YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

VİDEO VE SES KARIŞTIRICI SİSTEMLER

Elek. Müh. N. Tuncer BEYAZOĞLU

F.B.E. Elektrik Mühendisliği Anabilim Dalında
Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı : Prof. Dr. Halit PASTACI

İSTANBUL, 2000

Prof. Dr. Halit PASTACI

Prof. Dr. Galip Canseven

Yard. Doç. Dr. Aktül Kavas

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

B_i	Satır tamponu
$C_{x,y}$	Karıştırılmış alandaki (x, y) pikselinin üç boyutlu renk vektörü
$G(K)$	Kazanç fonksiyonu
H	Penaltı fonksiyonu
i	Karıştırılmamış alandaki satır
j	Karıştırılmış alandaki satır
K_e	Kodlanmış anahtar
K_p	Yalın metin anahtar
$K_{i,j}$	Korelasyon matrisi
N_i	i karıştırılmamış alan satırına karşılık gelen düğüm
N_j	j karıştırılmış alan satırına karşılık gelen düğüm
P	Satır karıştırma permütasyonu
P^{-1}	Satır düzeltme permütasyonu
S	Yerine koyma tablosu
S''	S yerine koyma tablosunun sırası değiştirilerek oluşturulan yeni tablo
v	Tampon seçme fonksiyonu
V_{cc}	Kart besleme gerilimi
V_{pp}	Kart programlama gerilimi

KISALTMA LİSTESİ

APL	Average Peak Level
ASIC	Application Specific Integrated Circuit
ATM	Automatic Teller Machine
ATR	Answer To Reset
BBS	Bulletin Board Service
BSkyB	British Sky Broadcasting
CBC	Cipher Block Chaining
CCD	Charged Coupled Device
DES	Data Encyption Standart
DDT	Delayed Data Transfer
DSS	Digital Satellite System
DVB	Digital Video Broadcasting
EBU	Europe Broadcasting Union
ECM	Electronic Counter Measure
EXOR	Exclusive Or
FIFO	First In First Out
FSZKT	Fiat-Shamir Zero Knowledge Test
IRD	Integrated Receiver Decoder
ISO	International Standards Organization
MAC	Multiplexed Analogue Component
NICAM	Near Instantaneously Companded Audio Multiplex
ORION	Oak Restricted Information and Operation Network
PCM	Pulse Coded Modulation
PIC	Programmable Integrated Circuit
PLL	Phase Locked Loop
PPV	Pay Per View
RSA	Rivest Shamir Adlemann
TSE	Thomson Consumer Electronics
UART	Universal Asynchronous Receiver Transmitter
VBI	Vertical Blanking Interval
VBL	Video Broadcast Log
VCL	VideoCrypt Log

ŞEKİL LİSTESİ

ÇİZELGE LİSTESİ

ÖNSÖZ

Bu çalışmayı hazırlarken bana yardımcı olan veya olmak isteyen arkadaşlarıma, her zaman yanımda olan dostlarıma ve bana maddi manevi her konuda destek olan aileme sonsuz teşekkürler.

ÖZET

Ücretli televizyon kanalları, yaptıkları yayınların sadece kendilerine bir abonelik ücreti ödeyen ve bir kod çözücü cihaz verilen televizyon izleyicileri tarafından seyredilebilmesini sağlamak için koşullu erişim sistemi kullanmaktadır.

Ücretli televizyonların koşullu erişim sistemi, tipik televizyon görüntüsü özelliklerine sahip bir alanın satırlarını yeniden düzenleyen görüntü işleme algoritmaları kullanılarak uygun bir şekilde kırılabilmektedir. Karıştırıcı sistem donanımı hakkında biraz bilgi sahibi olan bir kimse, abone akıllı kartında depolanmış olan kriptografik sırlar hakkında hiçbir bilgi sahibi olmaksızın karıştırılmış televizyon görüntüsünü gerçek zamanlı olarak yeniden kurabilmektedir.

Akıllı karttan kod çözme algoritmasını ve gizli anahtar verisini çıkartmak için mikroelektronik test etme teçhizatları kullanılabilmekte ve elde edilen bu bilgilerle uygun korsan akıllı kartlar ve kod çözücüler yapılabilmektedir.

Bir karıştırıcı sistemde kullanılmış olan erişim kontrol sisteminin, hack edilmeye karşı güvenli olması veya en azından hack edilmesinin çok masraflı olması gerekir. Bu yüzden bu karıştırıcı sistemde, iyi bir kriptografik sistemin kullanılması şarttır. Fakat bir karıştırıcı sistemde iyi bir kriptosistemin de gerekli olmasına rağmen, güvenliği sağlayan esas unsur kod çözücünün ve akıllı kartın teknolojisidir.

Anahtar kelimeler: Karıştırıcı, düzeltici, korsanlık, korsan

ABSTRACT

Pay-TV broadcasters employ conditional access system to ensure that only TV viewers who have payed a subscription fee and who have in return received a decoder box can watch the TV channel. The whole idea of an access control system is based on smart cards.

Pay-TV conditional access system that broadcasters used can be practically broken by image processing algorithms that rearrange the lines of a field based on statistical properies of typical TV images. With some knowledge about the limitations of the scrambling hardware one can reconstruct the scrambled TV image in real-time without knowledge of the cryptographic secret stored in the subscriber smart card.

Microelectronics testing equipment can be used to extract the decryption algorithm and secret key data from the smart card and with this knowledge compatible pirate smart cards and decoders can be manufactured.

The access control system used on a scrambling system has to be secure from hacking or at least not economical to hack. A good cryptographical system is essential. But it is not the element that ensures security. The technology of the decoder and the smart card is the one thing that ensures security.

Keywords: Scrambling, descrambling, piracy, pirate

1. GİRİŞ

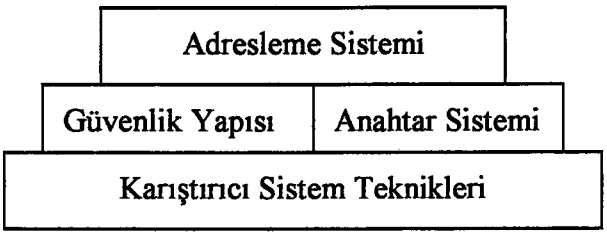
Avrupa'da, ücretli televizyon kanallarının kullanılmış olduğu analog ve dijital karıştırıcı sistemlerin tamamı hack edilmiştir. Bu hack işlemlerinin büyük bir kısmı sistemin erişim kontrol bölümünde gerçekleştirilmiştir. Karıştırıcı sistemlerin büyük bir kısmının kullanmış olduğu orijinal akıllı kart aynıdır. Sadece EEPROM'larındaki programlar biraz farklıdır. Bu yüzden, bir kartının nasıl hack edildiğini öğrenen bilgisayar korsanları diğer sistemleri de hack etmek için aynı bilgiyi kullanabilmektedir.

Video işleyici bir sistem, videoyu dijitalleştiren ve karıştıran bir sistemdir. Teorik olarak, dijital bir sistem çok güvenlidir. Fakat uygulamada, sistemin diğer bölgelerindeki kusurlardan dolayı bu sistem de hack edilebilmektedir. Dijital sistemlerin kullanılmasıyla korsanlığın sona ereceği kesinlikle yanlıştır. Bu çalışmada incelenmiş olan hack işlemlerinin tamamı bir zamanlar korsanlığa karşı güvenli olduğu düşünülen sistemlerde gerçekleştirilmiştir. Çünkü şu ana kadar değerli televizyon programlarını koruyan hiç bir karıştırıcı sistem uzun bir süre güvenli olarak kalamamıştır.

Bu çalışmada incelenmiş olan sistemlerin büyük bir kısmının, geçiş sistemleri olarak adlandırılması daha doğru olur. Çünkü bu sistemler, değişmez bir şekilde analog televizyon standartlarını baz almıştır ve dijital kodlama metotlarını sadece güvenliklerini sağlamak için kullanmıştır. Kodlama metodlarının büyük bir kısmı veri akışını korumayı amaçlamaktadır. Çünkü bu veri akışı, yetki verilmiş bir kart veya düzeltici tarafından videonun kodunun çözülmesini sağlamaktadır. Bu geçiş sistemlerinin erişim kontrol bölgelerinin tamamen dijital ve sıkı kodlama kullanıyor olmasına rağmen video, sadece dijital teknikler kullanılarak karıştırılmıştır.

2. KARIŞTIRICI SİSTEMLERDE KULLANILAN TEKNİKLER

Karıştırıcı sistem, görüntüyü seyredilemeyecek veya sesi duyulamayacak şekle çevirmek için kullanılan yöntemlerden çok daha fazlasının içeren karmaşık bir çalışma için kullanılan oldukça genel bir tabirdir [1]. Bir karıştırıcı sistem; adresleme sistemi, güvenlik yapısı ve karıştırıcı sistem teknikleri olmak üzere üç bölümden oluşur (Şekil 2.1).



Şekil 2.1 Bir karıştırıcı sistemin yapısının teorik bir modeli [1]

2.1 Karıştırıcı Sistemlerde Adresleme Unsuru

Karıştırıcı sistemlerde, adreslenebilir ve adreslenemez olmak üzere iki temel format vardır. Birkaç binin üzerinde abonesi olan ve oldukça değerli televizyon programları yayımlayan herhangi bir ücretli televizyon kanalı işletiminde, adreslenebilir bir karıştırıcı sistemin kullanılması gereklidir [1]. Bu sistem, televizyon yayınını seyredenlerin ve seyretmeyenlerin üzerinde televizyon kanalının bazı kontrollere sahip olmasını sağlar. Bu sistemin alternatifi adreslenemez bir karıştırıcı sistemdir [1]. Fakat bu sistemin kullanılması televizyon kanalının yapacağı en büyük hatadır. Çünkü, eğer televizyon kanalı abonenin kod çözücüsü üzerinde herhangi bir kontrole sahip değilse, o zaman bu abone abonelik süresi dolduktan sonra da televizyon programlarını seyredebilir. Ayrıca çalıntı kod çözücüler, televizyon kanalının bilgisi dışında başka kişiler tarafından yeniden kullanılabilir. Bu duruma telif hakları açısından bakarsak bu kod çözücüler, telif haklarıyla korunduğu bölgelerin dışına çıkarılabilirler. Bu durum, televizyon kanalı için yasal problemlere ilaveten güvenlik problemlerine de neden olmaktadır.

Adreslenemez sistem, havadan yayın yapan televizyon kanalları için kuruluş bakımından en hızlı ve en ucuz yöntemdir. Bu yöntem, Avrupa'da birkaç televizyon kanalı tarafından kullanılmıştır. Red Hot Dutch isimli ödemeli televizyon kanalı, yayına başlamalarından itibaren altı ay içerisinde daha güvenli bir sisteme geçmek üzere havadan yaptığı yayınında, adreslenemez bir sistem olan SAVE sistemini kullanmıştır [1]. Fakat yaptıkları planlar yolunda gitmemiş ve bu televizyon kanalı bilgisayar korsanları tarafından çökertilmiştir. Bu kanalın çökmesinde, kanalın yöneticilerinin büyük payı vardır.

Çünkü, bu ücretli televizyon kanalının kullanmış olduğu SAVE karıştırıcı sistemi yayına geçilmesinden en az beş yıl önce Avrupa'da geniş çapta korsan olarak izlenebiliyordu [1]. Bu yüzden, üzerinde kolayca değişiklik yapılabilen bu kod çözücülerin altyapısı mevcuttu. Bu değişiklik, sadece bir kristali değiştirmekten ibaretti. Kod çözücüde kullanılmış olan kristalin frekans değeri, piyasada mevcut olan bir değerdi. Bunun sonucu olarak, çalışmayan pek çok korsan SAVE sistemi kod çözücüsü, çok az bir masrafla tekrar çalışır duruma getirilebilmekteydi [1]. Red Hot Dutch kanalı için ana problem, mevcut olan bu korsan kod çözücü piyasası üzerinde hiçbir kontrole sahip olmamasıydı.

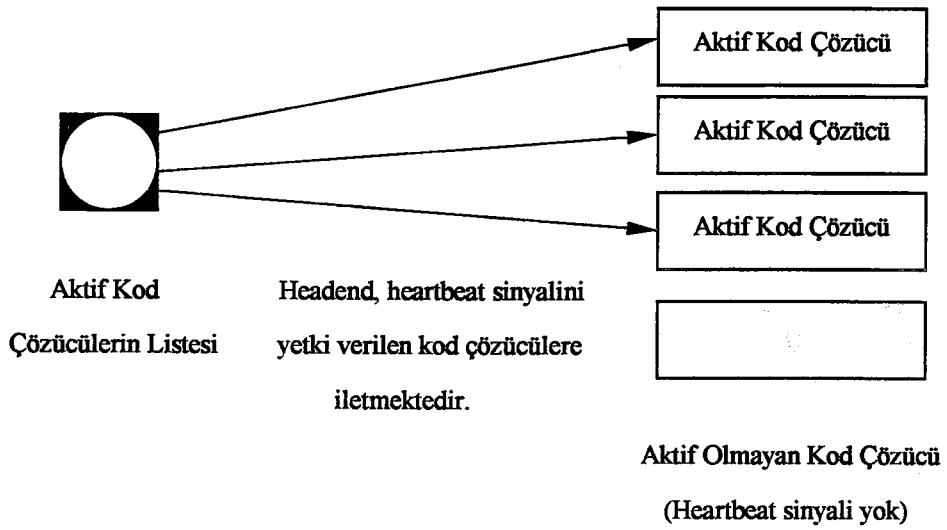
Eğer Red Hot Dutch kanalı, yayına başlamadan önce adreslenebilir bir sistem kullanmaya karar vermiş olsaydı durum bu olanlardan farklı olmayacaktı. Sistemi hack edilmesi muhtemelen daha uzun zaman alacaktı ve bu zaman aralığında, Red Hot Dutch kanalının bu hack işlemine elektronik karşı tedbir alma şansı olacaktı. Adreslenemez bir sistemde sinyali karıştırmada kullanılan tekniklerin güvenliği, televizyon kanalının çökertilmesini engelleyebilecek tek unsurdur [1].

2.1.1 Dahil etme ve hariç tutma prensibi

Bir karıştırıcı sistem, yetki verilen kod çözücüleri sisteme dahil ederek veya yetki verilmeyen kod çözücüleri sistemden hariç tutarak çalışmaktadır [1]. Bu, yüzeysel olarak bakıldığında mantıksız görünebilir. Çünkü, karıştırıcı bir sistemin bunların her ikisini de yapması gerektiği düşünülür. Fakat, bu konu daha detaylı incelendiğinde bu durum açık bir şekilde anlaşılmış olacaktır.

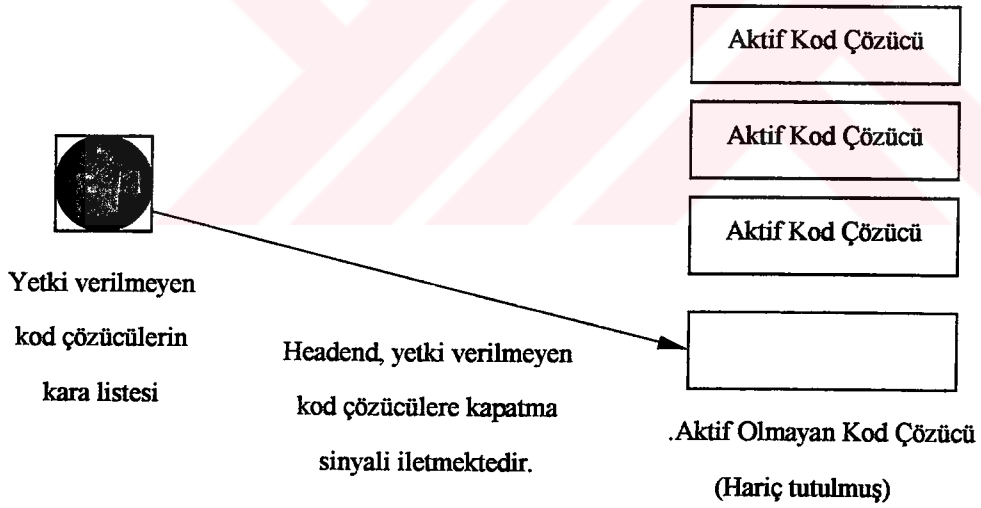
Dahil etme prensibiyle çalışan bir karıştırıcı sistemde, sadece bu kod çözücülere yetki verilmektedir ve kod çözücülere gönderilen heartbeat sinyali ile verilen bu yetkinin sürekliliği sağlanmaktadır [1]. Eğer heartbeat sinyali, kod çözücü tarafından alınmazsa kod çözücü çalışmayacaktır. Yetki verilen kod çözücülerin her birinin heartbeat sinyalini alması gerekli olduğu için bu tip bir sistem, yüksek bant genişlikli bir adresleme sistemi için çok uygundur.

Hariç tutma prensibi, dahil edilme prensibi için yukarıda anlatılanların tam tersidir. Yani yetki verilen bir kod çözücü, kapalı duruma getirme veya kesme sinyalini alıncaya kadar çalışmaya devam etmektedir. Kapatılmak istenen kod çözücülerin kimlik bilgileri kara liste (Blacklist) olarak isimlendirilen bir dizi ile gönderilmektedir. Bu kara liste, kapatılacak kod çözücülerin sayısının fazlalığına bağlı olarak her birkaç saatte bir yeniden gönderilebilir [1]. Bant genişliği açısından bakılırsa bu yaklaşım, maliyetinin düşük olmasının yanısıra aktivasyon bilgileriyle bant genişliğini karmaşık bir hale sokmamaktadır.



Şekil 2.2 Dahil etme prensibinin çalışma şekline basit bir örnek [1]

Dahil Etme Prensibi'nin kullanımı, D2-MAC gibi yüksek bant genişliğine sahip olan karıştırıcı sistemler için çok uygundur. Bu prensibin en büyük güvenlik kusuru, bilgisayar korsanları tarafından headend'in gönderdiği heartbeat sinyalinin bir kopyasının yapılabilmesinin mümkün olmasıdır [1].



Şekil 2.3 Hariç tutma prensibinin çalışma şekline basit bir örnek [1]

Hariç Tutma Prensibi, bant genişliği açısından en ekonomik prensiptir. Burada sadece, yetki verilmeyen kod çözücülerin kimlik bilgilerinin iletilmesi gereklidir. Diğer kod çözücülerin hepsi, onlara adreslenecek olan kapatma sinyalini alıncaya kadar aktif kalacaklardır [1]. Bu prensibin güvenlik kusuru ise, bu kesme sinyalinin nasıl engelleneceğinin bulunabilmesinin mümkün olmasıdır.

2.1.2 Bant içi ve bant dışı adresleme

Bant İçi Adresleme'nin en basit tanımı, karıştırılmış olan sinyalin bant genişliğinde taşınan adresleme bilgisidir. Adresleme bilgisi için tipik bölge, Düşey Aralıktaki Test Sinyalleri ve teletekst bilgilerinin de bulunduğu Düşey Karartma Aralığı (VBI)'dır. Ayrıca, bu adreslemenin biçimi Sinyal İçi Adresleme'yi de kapsamaktadır. Piyasada mevcut olan karıştırıcı sistemlerin büyük bir kısmı bu adresleme biçimini kullanmaktadır. Adresleme bilgisi, video bant genişliğinin bir bölümü olduğu için bu adresleme biçiminin uydu üzerinden yayın yapan kanallarda kullanılması çok uygundur [1]. Piyasadaki en yeni sistemlerin büyük bir kısmının dijital sistem olması, kanalın bant genişliğini daha verimli kullanabilmesini sağlamıştır. Bu nedenle, Bant İçi Adresleme olarak ifade edilen adresleme tekniklerini kullanmaya yönelmişlerdir.

Bant Dışı Adresleme'nin tanımı, normal video kanalı bant genişliğinin dışında taşınan adresleme bilgisidir. Genellikle ayrı bir veri taşıyıcı, sinyal ile birlikte iletilmektedir. Bu tip bir adresleme, uydu üzerinden yayın yapmış olan FilmNet kanalının eski SATPAC sisteminde kullanılmıştır [1]. Günümüzde kullanım alanı, Jerrold Tri-Mode sistemi gibi kablolu yayın bazlı karıştırıcı sistemler ile sınırlıdır [1]. Bu adresleme biçimine verilebilecek en klasik örnek, FilmNet'in kullanmış olduğu SATPAC sistemidir. Bu sistem, uydu bazlı bir sistem olarak çalışmaya zorlanmış olan aslında kablolu yayın bazlı bir karıştırıcı sistemdir. Kod çözücülere yetki verme veri akışı, yeniden senkronize edici darbeler olarak bir alt taşıyıcı üzerinden iletilmiştir [1].

2.2 Karıştırıcı Sistemlerin Güvenlik Yapısı

Bir sistemin güvenlik yapısı, sistemin bilgisayar korsanları tarafından uğrayacağı saldırılardan nasıl korunabileceğini belirtmektedir. Güvenlik yapısının başlıca iki tipi vardır. Bunlar; Kod Çözücünün İçine Yerleştirilmiş Güvenli Mikrokontrolör ve Kod Çözücüden Ayrılabilir Güvenli Mikrokontrolör olarak adlandırılır [1]. Bu iki tip, birçok bakımdan düşünce farklılıklarını yansıtmaktadır. Mikrokontrolör, mikroçip üzerinde ROM, EPROM ve/veya EEPROM'a sahip olan bir mikroişlemci uyarlamasıdır. Mikrokontrolör kod çözücüdeki erişim kontrolünü, kontrol sinyallerinin işlemden geçirilmesini ve kanalları açmayı veya kapatmayı kontrol altında tutmaktadır.

2.2.1 Kod çözücünün içine yerleştirilmiş güvenli mikrokontrolör

Kod çözücünün içine yerleştirilmiş güvenli mikrokontrolör, kod çözücünün ana kontrolünün kod çözücünün kendi içindeki devre yapısına gömülü olduğu bir yapıdır. Sistemin bütün gizli sırları, kod çözücünün içinde tutulmaktadır. Bu, yetmişli yıllardan seksenlerin sonuna kadar yaygın olarak kullanılmış olan bir metottur [1]. Ayrıca, bu yapı en savunmasız yapıdır ve bünyesinde güvenli bir mikroçip olduğu düşüncesini baz almaktadır.

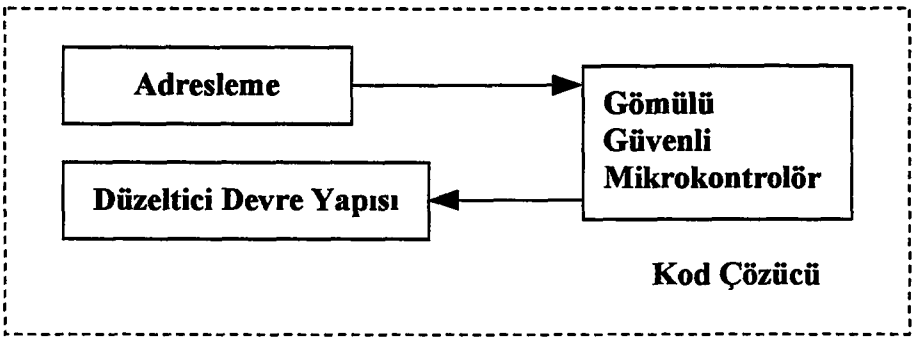
Karıştırıcı sistemlerde güvenlik kalıcı değildir. Bir mikroçipin, sadece birkaç aylık veya en iyi ihtimalle bir yıllık bir süre için güvenli olduğu düşünülebilir [1]. Yaygın olarak kullanılan bir mikroçipin güvenli kalma olasılığı, mikroçip konusunda uzmanlığa sahip olan ve kar amaçlı çalışan kişiler olduğu için çok zayıftır.

Bu tip güvenlik düşüncesi, karıştırıcı sistem tasarımlarına 1988 yılı sonuna kadar hakim olmuştur. Bu, FilmNet SATPAC sistemi, Jerrold Starcom sistemi, VideoCipher II sistemi ve Scientific Atlanta B-MAC sistemi gibi sistemlerin kod çözücü tasarımlarında görülmektedir [1]. Bu sistemlerin sahip olduğu tek ortak nokta, bilgisayar korsanları tarafından hack edilmiş olmalarıdır. Bu da, esas problemin içine yerleştirilmiş güvenli mikrokontrolör yapısında olduğunun örneklerle ispatıdır. Bu tür bir sistemde sürekli hack etme olayları yaşandığı zaman, bunlardan etkilenen bütün kod çözücülerin güvenlik seviyelerinin terfi edilmesi zor ve masraflıdır [1].

Ayrıca, kod çözücü tamamen abonenin kontrolü altındadır. Teorik olarak, abone kod çözücünün içini açabilir ve kod çözücüyü inceleyebilir. En kötü durum, abonenin kod çözücünün çalışma şeklinde değişiklik yapabilmesidir ve bu durum gerçekleştiğinde yapılabilecek çok az şey vardır.

Bu yaklaşımı ile tasarlanmış olan bir kod çözücü mimarisindeki ana problem, sistemin hack edildikten sonra geri kazanılmasının çok masraflı olmasıdır [1]. Eğer bu olay gerçekleşirse, her bir kod çözücünün televizyon kanalı tarafından değiştirilmesi gereklidir. Ayrıca, hack edilmiş olan bir kod çözücünün televizyon kanalı tarafından, havadan yapılan yayın ile gönderilecek olan sinyallerle güncellenebilmesi de mümkündür. Buradaki esas sorun, içine yerleştirilmiş güvenli mikrokontrolör mimarisine sahip bir kod çözücü hack edildiği zaman, artık bunun telafisinin olmamasıdır. Çünkü hack işlemini gerçekleştiren bilgisayar korsanı, abonelerin kod çözücülerine havadan yapılan yayın ile yüklenecek olan güncellemeleri izleyebilecek ve gerçekleştirmiş olduğu hack işlemini bu yeni duruma göre düzeltecektir.

Günümüzde, bu tip güvenlik mimarisini kullanan sistemlerin çoğunluğu kablo bazlı karıştırıcı sistemlerdir. Çünkü, kablo bazlı karıştırıcı sitemler yasalar ile daha iyi korunmaktadır. Fakat bu yasalar, bu kanalın uluslararası ortamda korsan olarak izlenmesini kapsamamaktadır. Küçük çaplı kablolu televizyon firmaları, sistem maliyetinin yüksek olması nedeniyle daha ucuz ve daha az güvenli güvenlik mimarilerine yönelmektedir.



Şekil 2.4 İçine yerleştirilmiş güvenli mikrokontrolör tasarımı [1]

Bu yaklaşım, seksenli senelerin ortalarından sonlarına doğru yaygın bir şekilde kullanılmıştır [1]. Herhangi bir hack edilme durumunda, her abonedeki kod çözücünün tamamen güncellenmesi gerektiği için, kod çözücü tasarımlarında büyük ölçüde gözden düşmüş bir yaklaşımdır. Çünkü abone sayısı milyonları bulan bir ödemeli televizyon kanalı için, bu çok masraflı bir işlemdir. Bununla beraber, Cablenet gibi birkaç bin aboneye sahip olan küçük çaplı televizyon kanalları için çok fazla bir mali risk getirmemektedir [1].

Bu tür bir yaklaşım, yasalar tarafından çok iyi korunan kablolu televizyon servisleri için çok daha uygundur. Fakat bu yaklaşım, uydudan yayın yapan televizyon servisleri için hiç uygun değildir. Çünkü, uydudan yayın yapan televizyon servislerinin yararlanabileceği koruyucu yasaların bulunmadığı bölgelerden, bu televizyon kanalları için tehlike gelmesi ihtimali yüksektir.

2.2.2 Kod çözücüden ayrılabilir güvenli mikrokontrolör

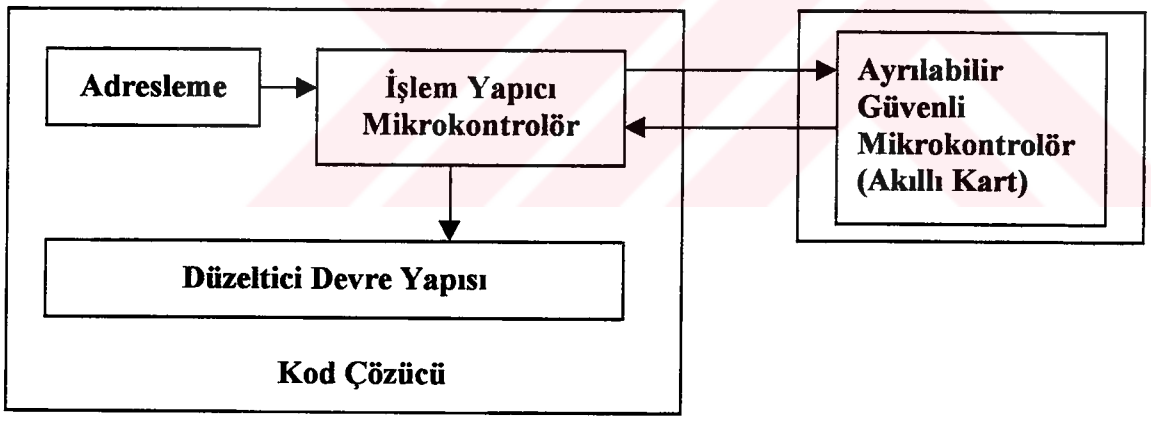
Ayrılabilir Güvenli Mikrokontrolör yapısı, İçine Yerleştirilmiş Güvenli Mikrokontrolör yapısı ile sahip oldukları ortak problemler çerçevesinde çalışılması için tasarlanmıştır. Bu yaklaşım, erişim kontrol mimarisindeki merkezi elemanının ayrılabilmesine ve çok düşük bir maliyetle güncellenmesine olanak tanır. Bahsedilmiş olan bu yapı, akıllı kart kavramıdır.

Bu modelde, kod çözücünün içinde hiçbir gizli sistem bilgisi yer almamaktadır. Bu nedenle, bilgisayar korsanının kod çözücü üzerinde hack işlemi gerçekleştirmesi, ona hiçbir şey

kazandırmayacaktır. Çünkü hack edilmesi gerekli olan akıllı karttır. Bu modele göre, eğer akıllı kart hack edilirse, bu akıllı kart çok düşük bir maliyetle yenisiyle değiştirilebilecektir.

Bu model kağıt üzerinde çok iyi çalışmaktadır. Fakat bu, gerçeklikle paralel gitmemektedir. Çünkü milyonlarca aboneye sahip olan bir ödemeli televizyon kanalının, abonelerindeki bütün akıllı kartları yenisi ile değiştirmesinin maliyeti on milyonlarca doları bulacaktır. Ayrıca, eğer akıllı kart hack edilirse yeni akıllı kartın bundan daha güvenli olması gerekir ve doğal olarak bunun maliyeti eskisinden daha fazla olacaktır. Bu yüksek maliyetten dolayı, her birkaç ayda bir akıllı kartı güncellemek hiç ekonomik değildir.

Sonuç olarak, bu yeni akıllı kart da büyük bir ihtimalle dört ila altı ay içersinde hack edilecektir [1]. Örneğin, başlangıçta VideoCrypt sisteminde akıllı kartın her üç ila altı ay içerisinde yenisi ile değiştirilmesi düşünülmekteydi [1]. Böyle bir zaman aralığında, akıllı kartı hack etmek bu korsan kod çözücü piyasası için çok zor olacaktı. Ancak, bu güncelleme işleminin maliyeti daha önceden yapılmış olan bütün kar hesaplarını altüst etmişti. BSkyB kanalı, her bir abonesindeki akıllı kartı on altı ila on sekiz ay arasında güncellemeyi denemiştir [1]. Fakat, bu yeni akıllı kart da abonelere dağıtılmaya başlandığı ayın ikinci haftası sonunda tamamen hack edilmişti.



Şekil 2.5 Ayrılabilir güvenli mikrokontrolör tasarımı [1]

Günümüzde, en yeni tasarımların büyük bir kısmında bu yaklaşım kullanılmıştır [1]. Teorik olarak, kod çözücü sisteminde akıllı kart kullanımı sistemin güncelleme maliyetini düşürmektedir. Bu durumda, akıllı kartın maliyetinin düşük olmasının da etkisi vardır. Bu akıllı kartlı tasarım, günümüzde de en güvenli tasarım olarak kabul edilmektedir.

Ayrılabilir Güvenli Mikrokontrolör teorisi ortaya çıktığından beri, içinde kullanıldığı uygulamaların çoğu kez kusurlu olduğu ortadadır. Bu kusurlar, çoğunlukla ekonomik nedenler yüzünden ortaya çıkmaktadır ve bu kusurlar yüzünden sistemin hack edilmesi

kaçınılmaz bir son haline gelmektedir.

2.2.3 Anahtar sistemleri

Birçok ödemeli televizyon kanalı, anahtarlarını düzenli olarak değiştirmemektedir. Bu yüzden bu kanallar, genellikle feci bir şekilde hack edilmektedir. Bilgisayar korsanları, bir kanalın anahtar sistemi aynı kaldığı zaman bu kanalın içine sızmaktadır. Televizyon kanalı sahipleri, bu durumu tam olarak anlamamaktadırlar. Onlar, sistemlerine o an kimse sızmadığı için altı ay sonra da hiç kimsenin sisteme sızmayacağını düşünmektedir. Fakat gerçek şudur ki, hiçbir sistem gelecek zaman içinde altı aylık bir zaman içinde kimsenin içeriye sızmayacağının garantisini veremez [1].

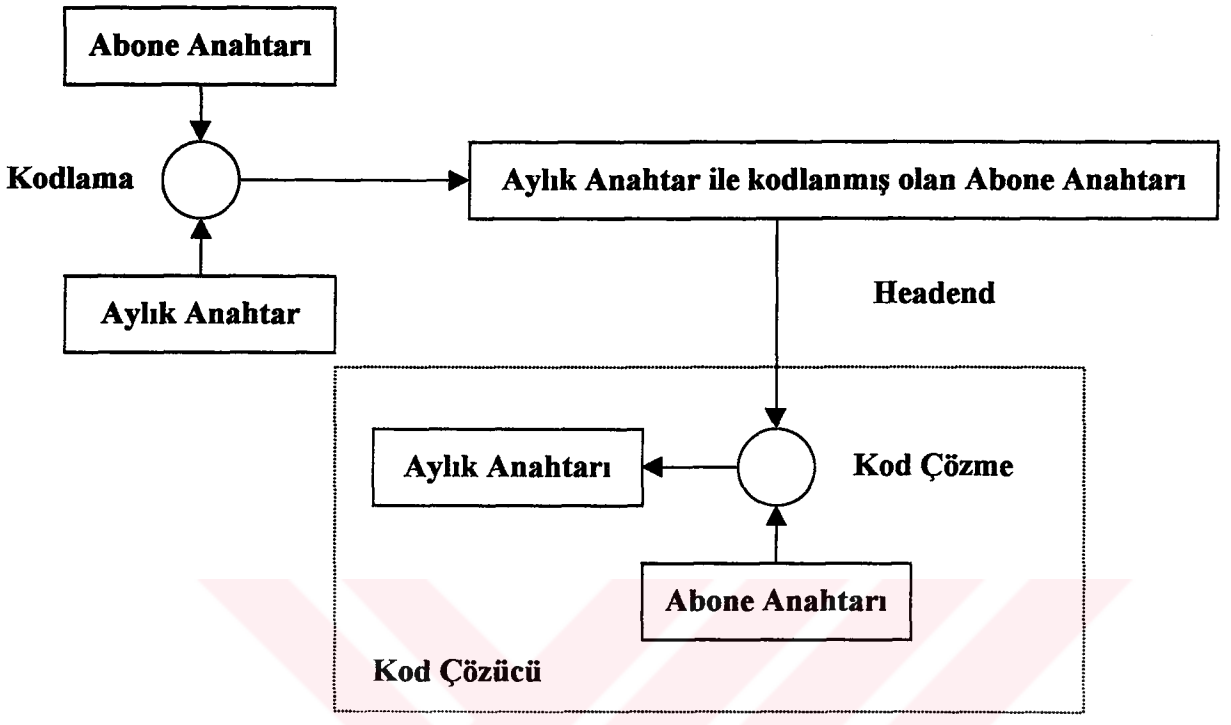
Klasik anahtar sistemine Hiyerarşik Anahtar Sistemi adı verilmektedir [1]. İçermiş olduğu anahtarların sayısı bakımından bu, sistemlerin en karışığıdır. Ayrıca bu anahtar sistemi, seksenli yıllarda kullanılmış olan İçine Yerleştirilmiş Güvenli Mikrokontrolör sistemleri ile benzerlikler gösterir.

Bu tip bir anahtar sisteminde kod çözücülerin her biri, teorik olarak hiçbir zaman bilinmediği kabul edilen kendisine özel gizli bir anahtara sahiptir. Yetki verilmiş olan kod çözücülerin tümüne hey ay, her bir kod çözücünün kendisine özel olan anahtarı ile ayrı ayrı kodlanmış olan bir aylık anahtar gönderilir. Bu aylık anahtarın kodu, yetki verilmiş olan bütün kod çözücülerde çözülür ve daha sonra bu aylık anahtar, oturum anahtarının kodunu çözmek için kullanılır. Bu oturum anahtarı, bir televizyon programından diğerine geçilince veya her birkaç saniyede bir düzenli olarak değiştirilebilir.

Bu tip bir anahtar sistemi, yüksek bant genişlikli karıştırıcı sistemler için çok uygundur. Uygulamada bu anahtar sisteminin, yaygın olarak Dahil Etme Prensipli sistemlerde kullanıldığı görülmektedir [1]. Diğer erişim kontrolü veri trafiğine ilaveten sürekli olarak, yetki verilmiş olan kod çözücülerin listesi abonelerdeki kod çözücülere iletilmelidir.

Hiyerarşik Anahtar Sistemi formunun alternatifi, televizyon kanalının kodunu çözmek için gerekli olan bütün algoritmaları ve verileri içeren ve sadece yetki verildiği zaman bu işi yapan kod çözücü veya akıllı karttır. İletilecek olan veriler açısından ele alındığında, bu sistemin maliyeti diğer sistemden daha düşüktür. Havadan abonelerdeki kod çözücülere gönderilen sadece, açma ve kapatma verileridir. Havadan hiçbir anahtarın iletilmesi gerekmemektedir. Bunun yerine havadan sürekli olarak, yetki verilmeyen kod çözücülerin listesi iletilmektedir. Bu tip bir sisteme verilebilecek en iyi örnek VideoCrypt sistemidir.

Tamamen hiyerarşik yapıya dayalı bir karıştırıcı sistem bulmak çok zordur. Bu sistemlerin çoğu, anahtar güncellemeye imkan tanıyan bazı kalıplar entegre etmeye yönelmektedir. Bu tip bir sisteme verilebilecek en iyi örnek EuroCrypt-M sistemidir.



Şekil 2.6 Anahtar protokolünün basit bir örneği [1]

Yönetim Anahtarı, kullanıcıların her bir düzeyi kontrol eden anahtara erişimini sağlayan bir Anahtar Hiyerarşi temeline dayanır. İşletme Anahtarı, en düşük düzeyde yer alır ve bu anahtar, her birkaç saniyede bir sürekli değişmektedir. Kontrol Sözcüğü, EuroCrypt gibi bir karıştırıcı sistemde Yönetim Anahtarı ve İşletme Anahtarı'na karşılık gelir [1].

Hack işlemlerinin büyük bir kısmının sadece İşletme Anahtarına erişimi vardır. Bu nedenle, bu anahtarı Kontrol Sözcüğü'nün kodunu çözmede kullanabilirler. Fakat, İşletme Anahtarı değiştirilirse Kontrol Sözcüğü'nün kodu çözülemeyecektir.

Yönetim Anahtarı, yeni İşletme Anahtarını kodlamak için kullanılır. Böylece, Yönetim Anahtarının hack edilmesinin fazla bir önemi yoktur. EuroCrypt karıştırıcı sistemini kullanan yeni televizyon kanallarının büyük bir kısmı, bu tür elektronik karşı tedbirlere başvurmaktadır.

Birçok sistem, kullandıkları anahtarları düzenli olarak değiştirmemektedir. Bunun temel sebebi, sistem kullanımı ve erişim kontrolü veya hangi kod çözücülerin sinyalin kodunu çözmesine izin verilmiş olması gerektiğini belirleyen yetki verme rutinidir.

Kod çözücü veya akıllı kart, sinyalin kodunu çözmek için gerekli olan anahtar/algoritma kombinasyonuna sahip olabilir. Fakat, tam olarak yetki verilinceye kadar sinyalin kodunu çözemez. Elbette bu durum, kod çözücü veya akıllı kart hack edilinceye kadar geçerlidir.

Kod çözücüde veya akıllı kartta, geçerli anahtar setini ve algoritmayı saklama yaklaşımının tehlikeli bir durum olduğu, VideoCrypt ve EuroCrypt karıştırıcı sistemlerinin hack edilmesiyle kanıtlanmıştır. Eğer bir sistem, düzenli olarak anahtar/algoritma güncellemesi yapılmaksızın sinyalin kodunun çözülmesine izin veren yetki verme erişim kontrol katına dayalıysa, bir hack işleminin gerçekleşmesi de kaçınılmazdır. Eğer bir bilgisayar korsanı, erişim kontrol katının müdahalesi olmaksızın anahtar/algoritma kombinasyonu fonksiyonunu gerçekleştirebilirse, ancak akıllı kartların tamamının değiştirilmesi veya kod çözücülerin yenilenmesi ile bu problem çözülebilir.

D2-MAC ve EuroCrypt-M karıştırıcı sistemlerini kullanan bazı televizyon kanallarının anahtar değiştirme işlemleri arasında geçen sürenin uzunluğu bilgisayar korsanlarının kafasını karıştırmıştır [1]. Bu konu üzerine çok sayıda teori mevcuttur. Bazı kimseler, televizyon kanallarının düzenli güncelleme yerine daha seyrek güncelleme yapılmasının nedenini, televizyon kanalının korsanlığı önlemekten ziyade mevcut abonelerinin elindeki akıllı kartlarının problemsiz olarak çalışmasını sağlamakla daha fazla ilgilenmesine bağlamaktadır. Fakat, gerçek durum bundan daha karmaşıktır.

Bir hack olayından etkilenmiş bir kanalda, Yönetim Anahtarının hala tehlike altında olduğunun kanal idaresi tarafından bilindiği bir gerçektir. Yani, bilgisayar korsanlarının havadan gelen yeni anahtarları da izleyebileceği bilinmektedir. Yeni Yönetim Anahtarına sahip olmayan sıradan bir korsan kod çözücü veya akıllı kart, havadan gelen sinyalleri alamaz ve kullanım dışı kalır. Daha sonra bilgisayar korsanları, korsan kod çözücü veya akıllı kart kullanıcılarına bir ücret karşılığı yeni anahtarı vererek güncelleme işlemini yapar. Televizyon kanalı sahipleri, anahtar değişimi yapmakla bilgisayar korsanlarına para kazandıracaklarının farkında oldukları için anahtar değiştirme yoluna gitmemektedirler.

2.3 Video Karıştırıcı Analog Teknikler

Aslında belli başlı birkaç video karıştırıcı analog teknik mevcuttur. İmalatçılar, aslında aynı karıştırıcı tekniği kullanmalarına rağmen kendi karıştırıcı sistemlerinin diğer imalatçıların kullandığı sistemlerden tamamen farklı olduğunu iddia etmektedirler. Sistemlerdeki bu fark, genellikle kullanmış oldukları erişim kontrol yapısının farklı olmasından kaynaklanmaktadır.

Bir imalatçının karıştırıcı sisteminde kullanmış olduğu karıştırıcı teknik hack edilirse, aynı tekniği kullanan başka bir imalatçıya ait başka bir sisteme de bu hack işlemi uygulanabilmektedir.

Analog tekniklerin büyük bir bölümü, uydu üzerinden yayın yapılan sistemlerde artık kullanılmamaktadır. Bunun nedeni, uydu üzerinden yayın yapılan sistemlerin diğer sistemlerden daha fazla hack edilmeye müsait olmasıdır. Geniş bir alanda yayınına ulaşılabilen bir sisteme, bilgisayar korsanlarından gelebilecek tehlike daha fazla olmaktadır. Çünkü birçok bilgisayar korsanı aynı problem üzerinde çalışmakta ve ortak çalışma ile bu problemi daha çabuk aşmaktadırlar.

Analog karıştırıcı tekniklere dayalı bir sistemde, bu tekniğin hack edilmesi durumunda yapılacak hiçbir şey yoktur. Buna rağmen, bu analog teknikler veya bu tekniklerin varyantları hala kablolu sistemlerde kullanılmaktadır. Bunun sebebi, kısmen mali ve kısmen de teknolojik yetersizliklerdir.

Uydu bazlı sistemlerde gerçekleştirilen hack işlemleri, baseband bazlı teknikler ile gerçekleştirilmektedir [1]. Kablolu sistemlerde ise baseband tekniklerinden çok RF bazlı karıştırıcı tekniklerin kullanıldığı görülmektedir. RF katında uygulanabilen bu teknikler, imalat masraflarını düşürmek için kullanılmaktadır [1].

Bilgisayar korsanlarına göre, baseband karıştırıcı bir sistemi hack etmedeki durum ile aynı koşullara sahip olan kablolu bir karıştırıcı sistemi hack etmek, kaçınılmaz bir mali başarısızlıktır. Çünkü RF bazlı bir sistemi hack edebilmek için yapılacak olan korsan kod çözücüde, bir RF katının olması gereklidir. Buna verilebilecek en iyi örnek, Kapılı Senkronizasyon Bastırma (Gated Synch Suppression)'nın kablo bazlı varyantıdır [1].

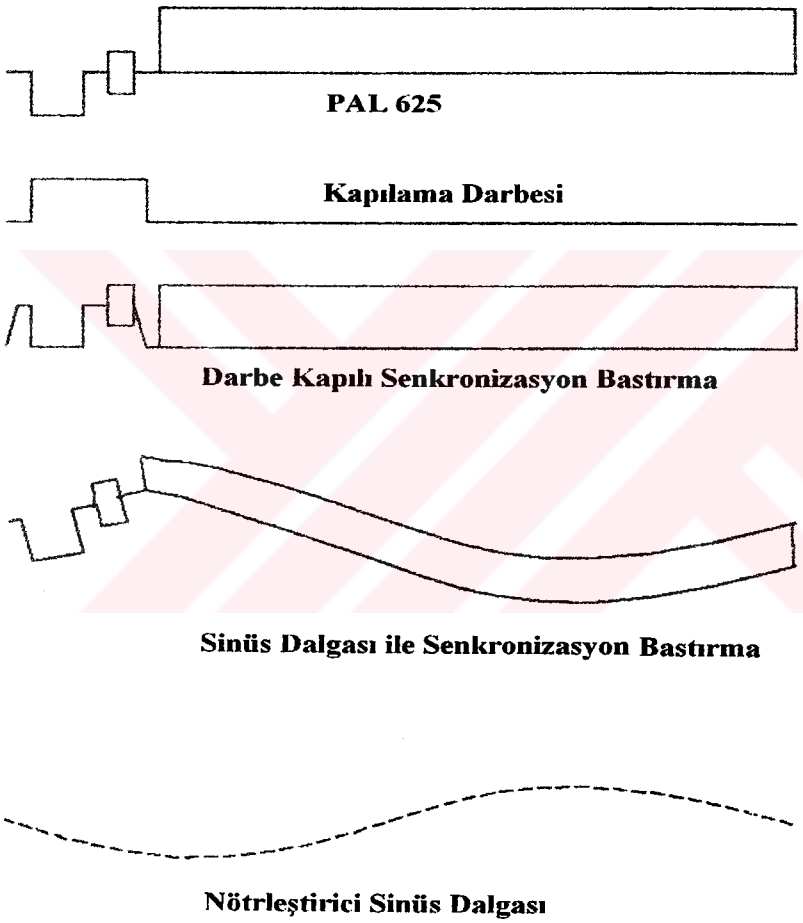
Bir baseband sistemde Kapılı Senkronizasyon Bastırma'nın anlamı, senkronizasyon darbeleri ve yatay karartma aralığının (horizontal blanking interval) geri kalan kısmının, satırın aktif video bölgesinin içine gerilimle kaydırılmasıdır. RF bazlı uygulamalarda, darbelerin gerçek genliği değişmektedir [1].

Baseband karıştırıcı bir sistemin hack edilmesi, senkronizasyon darbesinin gerilim ile asıl düzeyine geri kaydırılması gerektiği anlamına gelmektedir. Kablolu bazlı (RF) bir karıştırıcı sistemin hack edilmesi ise, RF sinyalinin yatay karartma bölgesinin doğru miktarda kuvvetlendirilmesi gerektiği anlamına gelmektedir. Bu yüzden, RF hack işleminde bir RF katına ve doğru zamanlamayı ve doğru kuvvetlendirme düzeyini saptamak için bazı devrelere ihtiyaç vardır. Bilgisayar korsanları, orijinal bir kod çözücünün çalışma tarzını değiştirerek

kullanmayı, korsan bir kod çözücü yaparak kullanmaktan daha basit bulmaktadır [1].

2.3.1 Senkronizasyon kullanan karıştırıcı sistemler

Senkronizasyon kullanan bir karıştırıcı sistem, sinyaldeki senkronizasyon darbelerine engel olur [1]. Böyle bir sistemin amacı, televizyon alıcısının görüntüyü kilitlemesine engel olmaktır. Tekniklerin çoğunun, dijital video teknikleri ile karşılaştırıldığı zaman oldukça ilkel oldukları, fakat buna rağmen yinede etkili oldukları görülmektedir. Daha da önemlisi, bazı uygulamalar için maliyeti oldukça düşüktür. Bu yüzden, bu metotları baz alan sistemlerin kullanımının küçük çaplı kablolu sistemler ile sınırlı olduğu görülmektedir.



Şekil 2.7 Senkronizasyon bastırma biçimleri [1]

Senkronizasyon kullanan bir sistemin zayıflığı, renk patlamasını tek başına bırakmaya eğilimli olmasıdır [1]. Renk patlaması, videoya göre gerilimle kaydırılmış olduğu sürece gerçek zamanlama aynı kalacaktır. Bu nedenle, bir senkronizasyon üretecini renk patlaması ile kilitleyerek bu sistemi hack etmek mümkündür [1]. Analog uydu televizyon sistemleri için

tasarlanmış olan eski korsan kod çözücülerin büyük bir kısmı bu kilitleme metodunu kullanmıştır.

Senkronizasyon bastırma, oldukça eski bir karıştırıcı tekniktir [1]. Bu yüzden nadiren kullanılmıştır. Yatay senkronizasyon darbesi veya yatay karartma alanı, sinyalin video bölgesine bastırılmıştır. Kabul edilen iki adet senkronizasyon bastırma formatı mevcuttur. Bunlar, darbe kapılı senkronizasyon bastırma ve sinüs dalgası senkronizasyon bastırma (Şekil 2.7) olarak adlandırılır [1].

2.3.1.1 Darbe kapılı senkronizasyon bastırma

Bir darbe kapılı senkronizasyon bastırma sistemi, düzeltme işlemi için karıştırılmış sinyal ile aynı fazda olan bir darbe trenine (pulse train) ihtiyaç duyar [1]. Bu darbe treni, yatay karartma aralığını veya doğru düzeylerin senkronizasyon darbelerini düzelten bir "pull down" devresini kontrol etmek için kullanılır [1].

Karıştırılmış sinyal için darbe treni veya düzeltme sinyali, genellikle FilmNet karıştırıcı sistemindeki gibi farklı bir alt taşıyıcı (subcarrier) üzerinden iletilir. FilmNet Matsushita SATPAC sisteminde bir bileşik senkronizasyon sinyali, 7.56 MHz'deki bir alt taşıyıcı üzerinden iletilmiştir [1]. Bu karıştırıcı sistemin kablolu televizyon uyarlamasında bileşik senkronizasyon sinyali, frekans modülasyonlu ses alt taşıyıcısı üzerinde genlik modülasyonludur [1].

2.3.1.2 Sinüs dalgası ile senkronizasyon bastırma

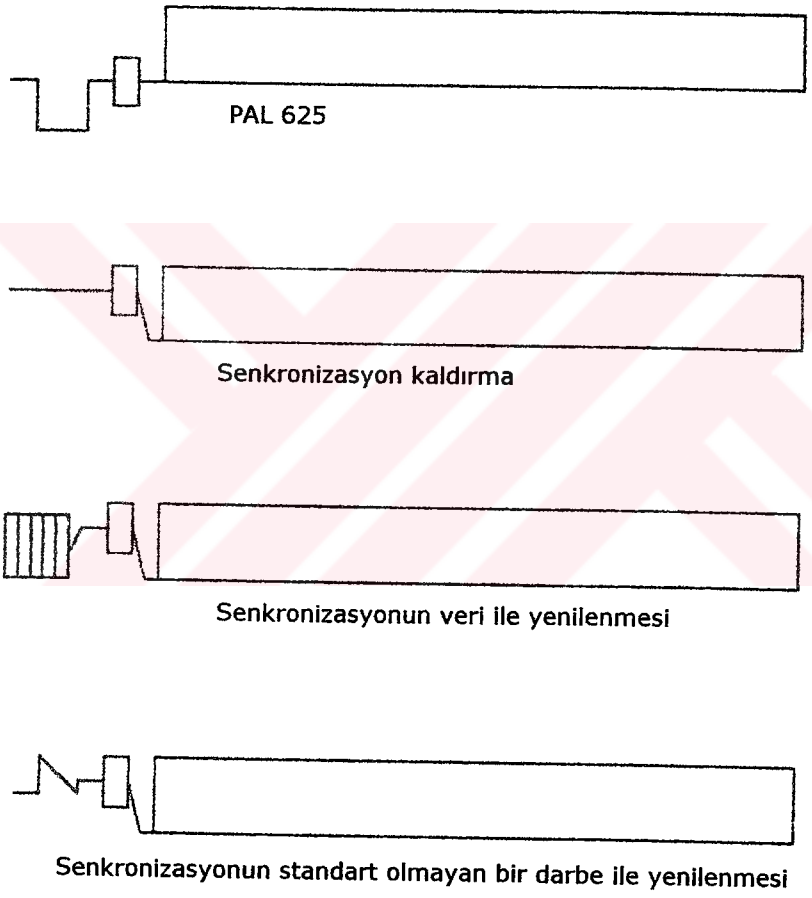
Sinüs dalgası ile senkronizasyon bastırma, senkronizasyon sinyallerini aktif video bölgesine bastırmak için bir sinüs dalgası kullanır [1]. Sinüs dalgasının frekansı, SAVE uydu televizyonu sisteminde olduğu gibi satır frekansına veya çeşitli satır frekanslarına yakın değerde olabilir. Daha yüksek frekansın, birçok satır frekansına yakın olmasının sebebi bir darbe frekansı yaratıyor olmasıdır. Ayrıca bu darbe frekansı, video ile karışmakta ve karıştırılma etkisini arttırmaktadır [1].

Sinüs dalgası ile karıştırılmış olan bir sinyalin düzeltilmesi, darbe kapılı sistemde olduğu gibi kolay değildir. Burada, sinüs dalgası sinyal ile iletilir veya iletilemez. Bazı kablolu sistemlerde düzeltme sinüs dalgası, FM ses alt taşıyıcısı üzerinde genlik modülasyonlu formatta iletilir. Bu düzeltme metodu, uydu sistemlerinde tam anlamıyla uygulanamaz. Uydu sistemlerinde kullanılan en yaygın metot, yenileme (regeneration) metodudur [1]. Sinüs dalgası, karıştırılmış olan video sinyalinden çıkarılmıştır ve bir faz kilitlemeli çevrime

yollanmıştır. Faz kilitlemeli çevrim, genellikle çok katlı yüksek sinüs dalgası frekanslarında çalışır. SAVE sisteminde engelleyici sinüs dalgasının frekansı, satır frekansının yaklaşık olarak altı katıdır (93.750 kHz). Düzelticideki faz kilitlemeli çevrim, sinüs dalgası frekansından 64 kat fazla bir frekansta (yaklaşık olarak 6.0 MHz) çalışır [1].

2.3.1.3 Senkronizasyon kaldırma ve yenileme

Bir video sinyalini karıştırmak için güvensiz bir metot tercih edilmişse, yatay veya düşey senkronizasyonun giderilmesi iyi sonuç verir [1]. Televizyon alıcısında senkronizasyon sinyali olmazsa televizyon görüntüyü kilitleyemez. Düzelticilerde görüntüyü kilitlemek için genellikle renk patlaması kullanılır. Renk patlamasının zamanlaması nadiren değişir [1].



Şekil 2.8 Senkronizasyon kaldırma ve yenileme [1]

Senkronizasyon darbelerinin dijital veri ile yenilenmesi, bu tip karıştırıcıların tesisinde yaygın olarak kullanılır (Şekil 2.8). Bu yöntem, OAK Orion sistemi ve LuxCrypt sisteminde kullanılmıştır. Dijital veri ve ses blokları, senkronizasyon darbelerinin yerine kullanılmıştır. OAK Orion sisteminde, veriden önce 2.5 MHz'lik bir senkronizasyon patlaması gönderilmiştir [1]. Bu, düzelticilerdeki senkronizasyon üreteçleri için bir kilitleme sağlar. Korsan düzelticiler

bu senkronizasyon patlamasını, tekkararlılar ve basit faz kilitlemeli çevrimler kullanarak senkronizasyon sinyallerini yeniden yaratmada kullanır. LuxCrypt sistemi, 5.792 MHz'lik bir senkronizasyon patlaması kullanmaktadır [1].

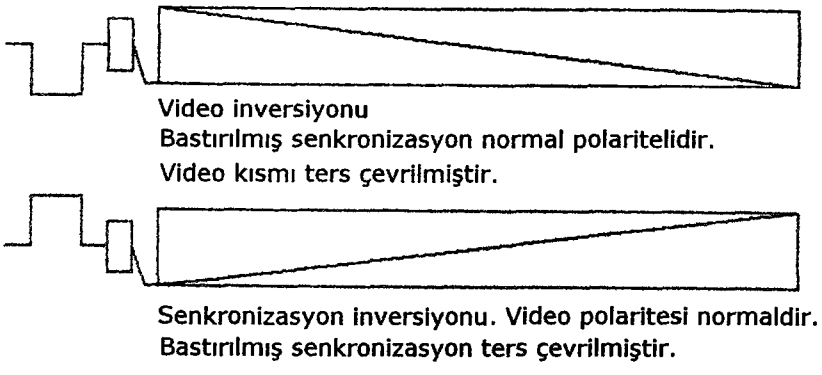
2.3.1.4 Senkronizasyon inversiyonu

Senkronizasyon inversiyonu, özellikle en kötü karıştırıcı sistem formudur. Korsan düzelticilerdeki polarite bulma devre yapılarının büyük bir kısmı, satırın tamamının ters çevrilmesi yönünde çalışır [1]. Senkronizasyon inversiyonu ile, sadece sinyalin karartma veya senkronizasyon kısmı ters çevrilmektedir (Şekil 2.9). Bu yöntem, optimal bir şekilde senkronizasyonun bastırılmış olduğu darbe kapılı sistemde kullanılabilir.

Polarite bulma devresi, yatay senkronizasyon darbesi ve yatay karartma arasındaki farkı bulduğunda, video polaritesi bu düzeyler ile tahmin edilir. FilmNet SATPAC karıştırıcı sistemi, korsan düzelticilerdeki bu zayıf noktayı kendi lehine kullanmıştır [1]. Bunu gerçekleştirmek için, yatay senkronizasyon darbesine bir tepe gerilimi ekleyerek korsan düzelticilerin videonun polaritesini yorumlayamamasını sağlamışlardır [1].

2.3.2 Video inversiyonu

Video inversiyonu (Şekil 2.9), en yaygın olarak kullanılan formdur. Bu inversiyon kapılı, sinüs bastırılmış veya normal sinyallere uygulanabilir [1]. Düzeltilmiş polariteler, birkaç milivolt farklılık gösterebileceği için uygulamalarda aldatıcı olabilmektedir. Bu, ya karıştırılmış videoya bir anahtar dahil edilmesi gerektiği ya da düzelticiye bir dengeleme potansiyometresi dahil edilmesi gerektiği anlamına gelmektedir [1].



Şekil 2.9 Video inversiyonu ve senkronizasyon inversiyonu [1]

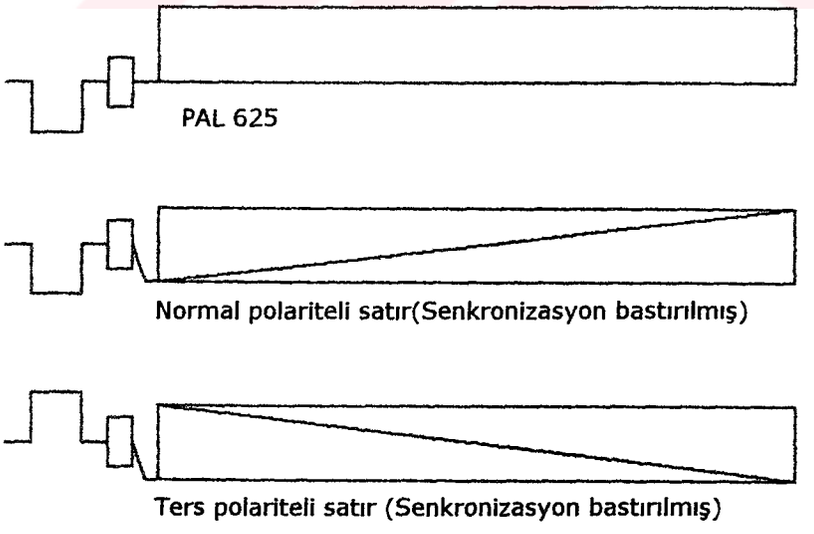
Bir anahtar, video ile ters çevrilmiş yatay karartma düzeyinin bir kısmının formunu alabilir. Karıştırılmış sinyalde, yatay karatma düzeyi yaklaşık olarak videonun yarısı kadar görülür.

Yaklaşık olarak 700 mV'luk video menzili ile bu yarım video noktası 350 mV olacaktır [1]. Bu, düzelticiye düzeltilmiş satırdaki bir referans düzeyi ile sağlanır. Bu anahtar modellenebilir ve normal polarite anahtarı ile karşılaştırılabilir. Bu karıştırıcı metot, uydu bazlı sistemlerde daha yaygındır. Bu metot, karadan yayın yapılan veya kablolu sistemler için uygun değildir.

2.3.2.1 Alan inversiyonu, satır inversiyonu ve ortalama tepe düzeyi inversiyonu

Alan inversiyonu, uygulanabilecek en basit metodlardan biridir. Bu yüzden, hack edilmesi de çok kolaydır. Alan senkronizasyonu içeren bir video alanının tamamı ters çevrilir. Bir sonraki alan, normal polaritededir. Diğer seri, örneğin 1 normal ve 3 ters çevrilmiş şeklinde birkaç flip-flop ve biraz kombinasyonel lojik ile elde edilebilir [1]. Bu, sadece video alanına veya alanın tamamına uygulanabilir. İnversiyonu noktası genellikle, düşey karartma aralığındaki alan senkronizasyonu başlangıcına veya sonuna ters yönde olan satırlardan birinin yarı uzaklığı mesafededir [1].

Satır inversiyonu (Şekil 2.10), anahtarlı ve anahtarsız olmak üzere iki ana formdan oluşur. Anahtarlı inversiyon, satır karartmada bir polarite sinyali içerir. Bu form, Oak ORION veya LuxCrypt gibi sistemlerde yaygın olarak kullanılmıştır. Bu, güvenliği en az olan formdur. Anahtarsız video inversiyonu, bundan çok daha güvenli bir formdur. Burada, video bilgisinin tam polaritesini gösteren bir sinyal yoktur. İnversiyon dizisi, ardışık veya yalancı rasgele dizi olabilir. Düzelticilere siyah düzeyini (black level) yerleştirmenin zor olmasından dolayı anahtarlı inversiyon daha yaygın olarak kullanılır [1].



Şekil 2.10 Satır inversiyonu [1]

Ortalama tepe düzeyi inversiyonu, etkili video inversiyon metodunun en güvenlilerinden

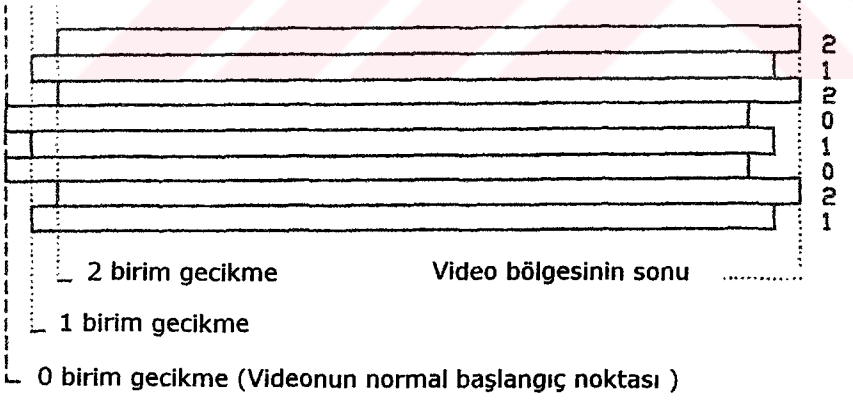
biridir. Videonun polaritesi, bir görüntüdeki siyah veya beyazın miktarına göre belirlenir [1]. Her bir resim (frame) örneklenir ve örneklerin gittikçe artan değeri, önceden ayarlanmış olan bir eşik değerini geçtiği zaman video ters çevrilir. Eşik değeri aşılıncaya kadar polarite değiştirilmez [1].

2.3.3 Video geciktirme

Karıştırıcıların video geciktirme formu birçok karıştırıcı sistemde kullanılmıştır. Canal Plus tarafından eskiden kullanılmış olan Discret sistemi, bu karıştırıcı formunu baz almıştır [1]. Ayrıca, Scientific Atlanta tarafından kullanılmış olan B-MAC sistemi de, gecikme artışı daha az olacak şekilde bu karıştırıcı metodu kullanmaktadır [1].

2.3.3.1 Sabit satır geciktirme ve değişken video geciktirme

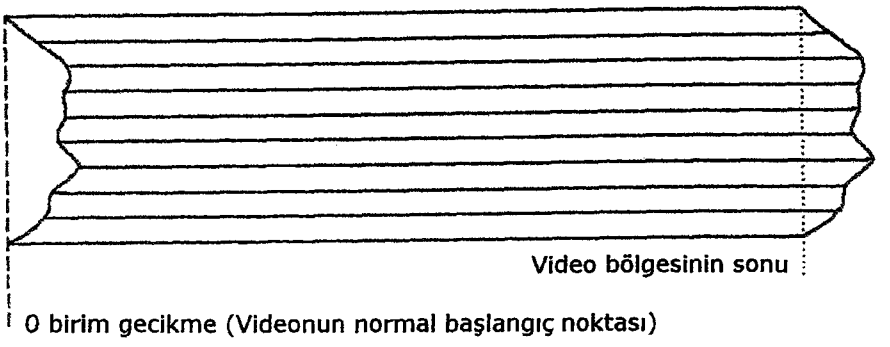
Sabit satır geciktirme formu, her satırdaki videoyu belli bir sayıdaki gecikme ile geciktirmektedir (Şekil 2.11). Discret sisteminde gecikmeler 0.902 ns ve 1804 ns'dir [1]. Gecikme işlemi, CCD'ler, cam (glass) gecikme satırları veya jiratör gecikme satırları ile gerçekleştirilir. Gecikme satırlarının uzunluğu bilinirse, sistem çok kolay hack edilir. Burada başvurulmuş olan sabit gecikme süresinde sadece üç gecikme durumu vardır. Sabit satır geciktirme kullanmış olan Discret sisteminin tasarımındaki temel kusur, piyasada bulunan elektronik bileşenler ile kullanmış olduğu gecikme birimlerinin emüle edilebilmesidir [1].



Şekil 2.11 Sabit satır geciktirme formu [1]

Değişken video geciktirmenin (Şekil 2.12) hack edilmesi biraz daha zordur. B-MAC sisteminde satırların video kısımları, veri bloğunun uzunluğu değiştirilerek geciktirilmektedir [1]. En küçük gecikme uzunluğunun ve gecikme birimlerinin maksimum sayısının doğrusunun bulunması zordur. Bu tip bir karıştırıcıyı, gecikme uzunluğunun değişimi daha büyük olduğu için başarılı bir biçimde hack etmek oldukça zordur. Videonun dijital olarak

genişletilmesi gerekli olduğu için bu tip karıştırıcı sistemlerde gecikme uzunluğunu bulunması çok zordur. Video elektroniğindeki gelişmeler sonucu, değişken geciktirmeli video karıştırıcıların güvenliği artık B-MAC sisteminin geliştirilmiş olduğu seksenli yıllardaki kadar iyi değildir [1].



Şekil 2.12 Değişken video geciktirme formu [1]

2.3.4 Video konumu modülasyonu

Video konumu modülasyonu, Macrovision PhaseKrypt sistemidir [1]. Bu, hack edilmesi en zor olan sistemlerden biridir. Çok güvenli bir video karıştırıcı metottur. Satırdaki videonun konumu modüle edilmiştir. Video bilgisinin kendisi, bununla birbirine uyması için biraz kısaltılmıştır. Her bir video alanının başlangıcındaki ve sonundaki gecikme kısmı, elektronik olarak uzatılmış olan video ile kaplanmıştır. Geciktirme süresi, doğru şekilde bulunabilmesi için çok küçüktür ve bunun sonucu olarak, sadece video yaklaşımıyla hack etmek aşırı derecede zordur [1].

Bu sistem, kablolu sistemler gibi küçük çaplı yayın yapan kanallar için gerçekten ideal bir sistemdir. Bununla birlikte, değerli televizyon programların iletildiği uydu bazlı sistemler için bu durum aynı değildir. Sistem, hack edilmeden kalması gereken erişim kontrol devre yapısına güvenmektedir. Geniş ölçekli bir uydu sisteminde erişim kontrol devre yapısının hack edilme ihtimali büyüktür [1].

2.4 Video Karıştırıcı Dijital Teknikler

Genellikle, dijitalleştirilmiş video sinyallerine kes ve ters çevir, kes ve yer değiştir, satır karıştırma teknikleri uygulanmaktadır [1]. Bu teknikleri kullanan sistemleri hack etmek genelde çok zordur ve çoğu durumda karıştırıcı işlemi gerçekten hack edilememektedir. Bu sistemlerin zayıf noktası, hemen hemen hiç değişmeyen kontrol devre yapısıdır. Günümüzde video elektroniğindeki ilerlemeler ve yapılması gereken işlemlerin maliyetinin düşmesi, dijital

sistemlerin video görüntüsünü hack etmeyi artık olanaklı kılmaktadır.

Piyasadaki sonuca ulaşan yeni sistemlerin çoğunluğu, aşağıda ana hatları verilmiş olan dijital video tekniklerinin birini veya birkaçını kullanmaktadır. En yaygın kullanılan karıştırıcı tekniği satır karıştırmadır (line shuffle). Kayan çubuk karıştırması (sliding bar shuffle) kullanmak daha ucuz bir seçenek olduğunda, tam alan karıştırmasına (full field shuffle) dayanan daha güvenli diğer versiyonları da ortaya çıkmıştır [1]. Tam alan karıştırma, bellek gerektiren bir seçenektir ve bu durum kod çözücü birim maliyetine yansımaktadır. Kod çözücünün yüksek maliyetinden dolayı, sıradan primli televizyon programları yayınlayan ödemeli televizyon kanallarından ziyade son derece değerli programlar yayınlayan kanallar hedeflenmektedir.

Bir dijital video bazlı sistemi video yoluyla hack edilip edilemeyeceğini belirleyen bir faktör, korsan bir dijital kod çözücü yaratılmasını engelleyen akıllı kartın ters mühendisliğinin (reverse-engineering) maliyetidir [1]. Dijital Sinyal İşlemci mikroçiplerinin maliyeti düştükten sonra, dijital tekniklere dayanan karıştırıcı sistemler giderek daha güvenilmez bir hale gelecektir. Şimdiden, Nagra sistemi (SECAM versiyonu) donanım bazlı olarak hack edilmiştir [1]. Bu sistem altı sene kullanılmıştır ve ciddi bir hack edilmeye maruz kalmadan kullanımına son verilmiştir.

Bir donanım bazlı hack etme işlemine karşı güvenlik koşulları bakımından satır kes ve yer değiştir (line cut and rotate) tekniği, satır karıştırmadan daha başarılıdır. Satır kesme ve yer değiştirme üzerinde yapılan donanım bazlı hack etme denemelerinde, korsan kod çözücünün her birkaç dakikada bir yeniden resetlenmesi gerekmektedir [1]. Çünkü, belirli bir rengin yüksek değerine sahip olan sahneler, işlem yapan devre yapısı için problem çıkarmaya eğilimlidir. Bu sistemler genelde karmaşıktır. Bölüm 6'da, dijital video sistemleri detaylı olarak incelenmiştir.

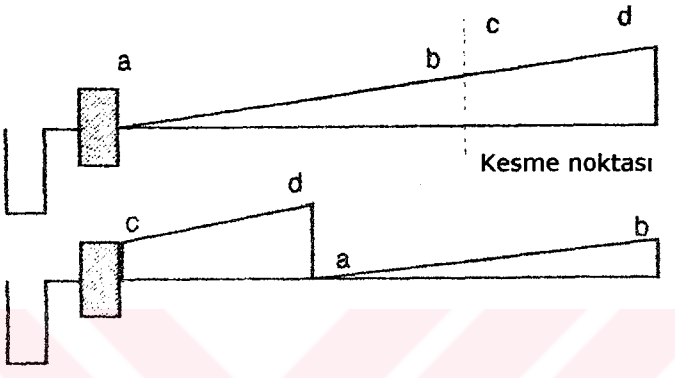
2.4.1 Satırı kesme ve ters çevirme tekniği

Dijitalleştirilmiş satır, belirli bir noktadan kesilir ve bu noktadan sonra gelen bütün veriler ters çevrilir [1]. Bu teknik, analog teknolojide başarılı olabilir. Fakat devrilme (tilt) gibi artık (residual) problemlere eğilim göstermektedir.

2.4.2 Satırı kesme ve yer değiştirme tekniği

Dijitalleştirilmiş satır, belirli bir noktadan kesilir ve bu iki parçanın yeri değiştirilir [1]. Bu şekilde, sondaki parça başa ve baştaki parça da sona geçer. Bu, oldukça güvenli bir metottur.

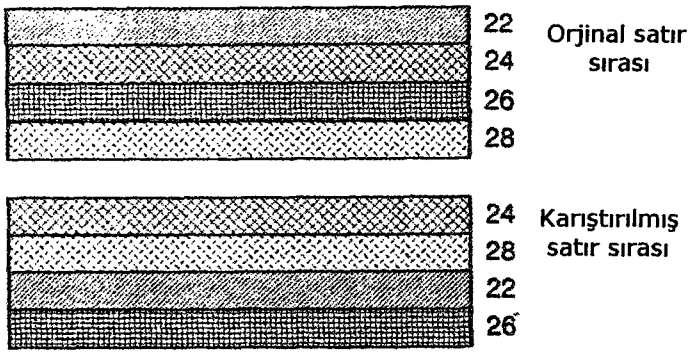
Fakat kesim noktaları, zayıflığı ve gürültüyü engellemek için gizlenmelidir. VideoCrypt sistemi, bu karıştırıcı formu Cryptovision sisteminde olduğu gibi aynen kullanmaktadır [1]. Kesme dizisi, havadan gönderilmekte olan kodlanmış formattaki bir çekirdek ile yapılandırılmış olan bir Yalancı Rasgele Sayı Üreteci tarafından üretilmektedir. VideoCrypt kod çözücüdeki yalancı rasgele sayı üretecinin parametrelerini saptamak için bazı araştırmalar mevcuttur [1]. Buradaki problem, karıştırılmış videodaki kesme noktalarını saptamanın genellikle çok zor olmasıdır. Yani, kesme noktalarını bulmaya ve diziyi yalancı rasgele sayı üreteci dizisine yeniden senkronize etmeye dayalı donanım bazlı hack işlemi, akıllı kart ile etkili bir şekilde uzlaşılmadığı zaman uygulanamaz [1].



Şekil 2.13 Satırı kesme ve kesilen parçaların yerlerini değiştirme [1]

2.4.3 Satır karıştırma tekniği

Bu sistem, tamamen dijital bir sistemdir. Her bir alandaki satırın gerçek konumu değiştirilmiştir (Şekil 2.14). Örneğin, onuncu satır yirminci satır olabilir. Satırların sırasının değişmesine rağmen bu satırların video bilgisi aynı kalmaktadır.



Şekil 2.14 Satır karıştırma tekniğine basit bir örnek [1]

Bu sistem, alan veya resim (frame) bazlı olarak uygulanabilir. Fakat, bu tip bir karıştırıcının alan veya resim bazlı olarak uygulanması bellek gerektirir. Bunun sonucunda, böyle bir

sistemin kod çözücüsü pahalı olacaktır. Bunun alternatifi, her bir alanda daha küçük bir satır bloğu kullanılması ve ilave güvenlik için her bir alandaki bloğu kaydırarak her bir alanda farklı bir satır bloğunun seçilmesinin sağlanmasıdır. Bu, maliyeti daha düşük olan bir seçenektir ve hemen hemen tam alan kaydırmadaki kadar güvenlik sağlamaktadır [1].

2.4.4 Sıkı kodlama tekniği

Bu dijital video tekniği en güvenli tekniktir. Örneklerin dijital verileri, DES veya RSA gibi bir algoritma kullanılarak kodlanır [1]. Sıkı (hard) kodlamalı tamamen dijital video sistemi kullanan pek çok ödemeli televizyon kanalı vardır. Bu tipteki bir sistem için verilebilecek en iyi örnek, Amerika'da kullanılmış olan DirecTv sistemidir [1]. Çünkü bu sistemin akıllı kart yaklaşımı üzerinde tamamen uzlaşılmıştır.

Sıkı kodlama kullanan sistemler, genellikle MPEG-2 standardı gibi dijital bir video protokolü kullanır ve kodlama ile bu videonun üzerini kaplar (overlay). Bu, sistem geliştirme süresinden tasarruf ettirir. Yani, demodülasyon devre yapısı herhangi bir yerden hazır olarak satın alınabilir. Üzerinde çalışılan kod çözücü yaklaşımı sadece güvenlik elektroniğidir. Avrupa'daki birkaç servis, birkaç yıl sonra bu tekniği kullanmaya başlayacaktır. Bu servisler, Dijital Video Yayıncılığı (DVB) teknik özelliklerini baz alacaktır [1]. Görünüşe göre, bu servislerin hepsi çok gizli tutulacak olan ortak bir karıştırma algoritması kullanacaktır. Koşullu erişim sistemi üreticileri, servislerin kendine özgü güvenlik kaplamalarını daha sonra verecektir [1].

2.5 Ses Karıştırıcı Teknikleri

Sesin karıştırılması, sadece düşük ücretli ödemeli televizyon kanalları için etkili bir önlem olabilir. Buradaki amaç, izleyicilere sesi karıştırıp göndererek videonun eğlence değerini ortadan kaldırmaktır [1]. Ses karıştırıcı teknikleri için en yeni tehlike, çoklu dil desteğine sahip altyazılı televizyon filmleridir.

Ses karıştırıcıların kullanımı, Avrupa'da fazla yaygın değildir. Bu teknik, kablolu sistemlerde kullanılırken, uydu bazlı sistemler sıkı video karıştırıcı teknikleri ile çalışmaya yönelmişlerdi. Ses karıştırıcılar uydu bazlı sistemlerde kullanıldığında, genelde sadece karıştırıcının bir erişim kodu biçimindeydi. Bunun sebeplerinden biri, senkronizasyon sinyalinin bulunmadığı durumlarda, Avrupa'daki birçok televizyon kanalı sesi otomatik olarak silmesidir [1]. Bu nedenle, senkronizasyon darbelerini bastıran veya beceriyle kullanan bir sisteme ses karıştırıcı eklemek gereğinden fazlasının yapılması gibi gözükmekteydi.

Uydudan yayın yapan, sıkı video karıştırıcı kullanan servislerin bazıları, ayrıca bir ses karıştırıcı içermektedir. En yaygın olarak kullanılan ses karıştırıcı tekniği, Spektrum İnversiyonu'dur [1]. Bu teknik, uygulama kolaylığından dolayı tercih edilmektedir. Avrupa'da, karıştırılmış videoya ilave olarak sıkı kodlanmış sesin kullanıldığı tek durum kısa bir süre kullanılmış olan FilmNet dijital ses sistemidir [1]. Bu, aynı zamanda kullanılmış olan tamamen uzlaşılmış olan video karıştırıcı analog sistem için ilave bir özelliktir.

Amerika'da VideoCipher-II karıştırıcı sistemi, Avrupa'daki sistemlerin tam tersi bir yol izlemiştir ve videoyu basit bir senkronizasyon yenileyen karıştırma ile korurken dijital ses karıştırmada DES bazlı kodlama kullanmıştır [1]. Genel eğilim, ses karıştırıcı analog metotlardan daha güvenli olan dijital ses karıştırıcılara geçmektir. D2-MAC EuroCrypt sistemi, bu eğilimin tipik bir örneğidir. Bu sistemde video, iki kez kes ve yer değiştir metodu ile sıkı kodlanmıştır ve ayrıca sese de sıkı kodlama uygulanmıştır [1]. D2-MAC EuroCrypt sistemini kullanan televizyon kanallarının birçoğu sesi kodlamamaktadır.

Dışarıdan bakılınca ses karıştırıcı dijital bir sistem güvenlik için iyi bir seçim gibi gözükmektedir. Aslında dijital sesin veri akışı veya sinyal, iletildiği zaman güvende olur ve genellikle imalatçılar, havadan iletilen veri akışını kodlamak için sistemin DES, RSA veya başka bir güvenli algoritmayı kullandığını iddia eder [1]. Bu, tabiki sahte bir güvenliktir. Ses karıştırıcı dijital bir sistemin hack edildiği nokta, yetki verme ve erişim kontrol kısmındadır. Bir bilgisayar korsanı, orijinal bir kod çözücüye saldıracaktır ve bunu bir korsan kod çözücü gibi çalıştırmayı deneyecektir. Çoğu zaman bu tür bir hack işlemi başarılı olur. Bu şekilde ilk defa FilmNet sistemi hack edilmiştir [1]. FilmNet sisteminde, donanımın ve yetki verme kısmının tamamının ters mühendisliği gereklidir. Bilgisayar korsanlarının yaptığı kod çözücü, kalite bakımından orijinal FilmNet kod çözücüsünden daha başarılıydı [1]

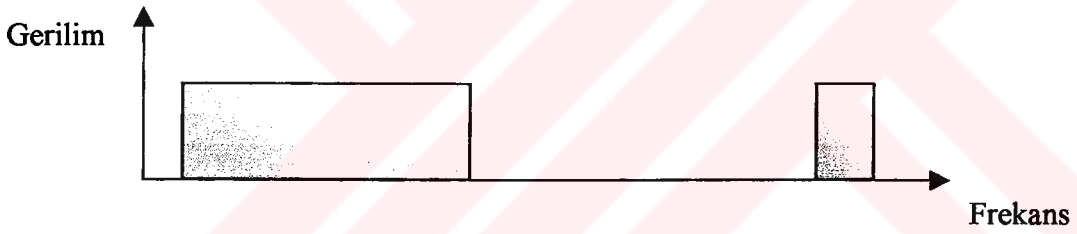
VideoCipher-II sistemi, bu modelin aynısını uygulamıştır. Yetki verme verisinin hack edilmesi mümkün olduğu için bu sistem de hack edilmiştir. FilmNet'in kullanmış olduğu ses karıştırıcı dijital sistemi, kod çözücünün tamamının ters mühendisliği mümkün olduğu için hack edilmiştir [1]. Tek sistem kullanan bir ortamın, uydu televizyonu endüstrisine verebileceği zararın iyi bir örneği VideoCipher II sistemidir. VideoCipher II sistemi, Amerika'nın uydu televizyonu endüstrisi ile bu endüstriden yararlanan birçok uydu bazlı kanalı gerçekten mahvetmiştir. Çünkü bu sistem hack edildiğinde bu durumdan bütün kanallar etkilenmişti [1]. VideoCipher II sisteminin, bu yüzden Avrupa'da pek tutulmadığı söylenebilir. Bu, belki de Avrupa'daki televizyon kanalların hiçbirinin VideoCipher-II sistemini kullanmamasının başlıca sebebidir.

Sabit bir algoritma ve değişebilir bir anahtar grubu kullanan herhangi bir dijital ses sistemi kullanıldığında, bir felaket ile karşılaşmak kaçınılmazdır. Bu tip bir sistemin güvenli olduğunu düşünmek imkansızdır. Sabitleşmiş bir yapısı olduğundan dolayı ters mühendisliği yapılabilir ve daha sonra da kopyalanabilir. Bundan sonra, anahtarları elde etmek için kullanılan kod çözücülerin kimliğini saptama ve bu kod çözücüleri kapatma görevi bu karıştırıcı sistemi kullanan televizyon kanalına aittir [1].

2.5.1 Ses karıştırıcı analog teknikler

2.5.1.1 Frekans modülasyonlu ses tekniği

Frekans modülasyonlu ses tekniğinde ses sinyali, satır frekansının üç veya dört katı olan bir frekans üzerinde frekans modülasyonlanmıştır (Şekil 2.15). Genellikle bu ses sinyali, 30 kHz ile 100 kHz arasında değişen bir menzilde taşıyıcı bir frekans üzerinde frekans modülasyonludur [1]. Amerika'da kullanılan sistemlerde yaygın olarak 62.5 kHz, 31.5 kHz, 40 kHz ve 63 kHz frekansları kullanılmaktadır [1]. Bu ses karıştırıcı teknik Amerika'da kullanılmaktayken, Avrupa'daki uydudan yayın yapan televizyon sisteminin hiçbirinde kullanılmıyordu [1].

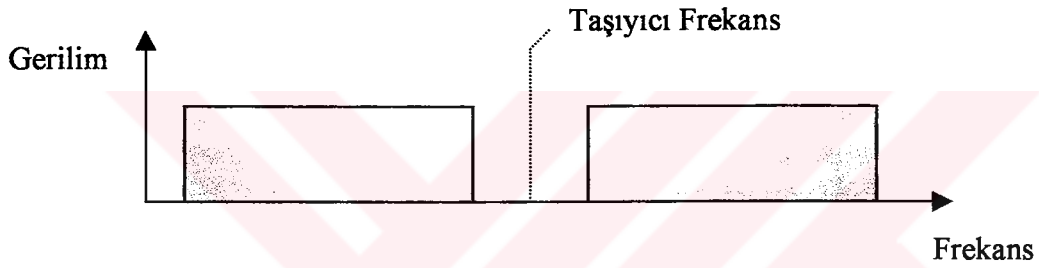


Şekil 2.15 Frekans modülasyonlu ses tekniği [1]

Bu şekilde karıştırılmış sesi düzeltmek için bir Faz Kilitlemeli Çevrim tipi bir devre gereklidir. Farklı tiplerde pek çok demodülatör mevcuttur. Fakat Faz Kilitlemeli Çevrim, bu düşük frekansa adapte edilmesi en kolay olanıdır. Bu uygulamalarda en yaygın olarak kullanılan iki Faz Kilitlemeli Çevrim entegre devresi NE565 ve 4046'dır [1]. 62.5 kHz'de çalışan NE565 için devre diyagramı Bölüm 3'te verilmiştir. Ses demodülatörlerinin cevap verme süresi, çoğu alıcıda yeterli olmadığı için Faz Kilitlemeli Çevrim demodülatöründen sonra bir amplifikatörün bulunması gereklidir. Düzeltici için ayrı bir demodülatör kullanılırsa çok daha iyi olmaktadır [1]. Birçok bakımdan bu teknik çok eskidir. Yeterli derecede güvenlik sağlamamaktadır. Bu ses karıştırma tekniği kullanıldığı zaman çoğunlukla, video da uygun bir güvenli karıştırıcı sistem ile karıştırılmıştır.

2.5.1.2 Spektrum inversiyonu tekniği

Spektrum inversiyonu tekniği, Discret karıştırıcı sistemi tarafından kullanılmaktadır. Ayrıca Nagra Syster sistemindeki ses de bu teknik kullanılarak karıştırılmaktadır. Aslında bu teknik, sese uygulanan tek yan bant (single sideband) tekniğidir ve yetmişli yılların sonunda, bazı basit telefon karıştırıcı sistemlerinde de kullanılmıştır [1]. Bu sistemin düzelticisi, bir önceki teknikle kıyaslanırsa biraz daha fazla karmaşıktır. Spektrumun yer değiştirdiği frekansın etrafında yer alan merkez frekansın yeniden yaratılması gerekmektedir (Şekil 2.16). Orijinal RITC Discret-I düzelticide 12.8 kHz'lik olan frekans, 8.0 MHz'lik bir kristal osilatörünün çıkışının 625 ile bölünmesiyle elde edilir [1]. Korsan Radio Plans tasarımında, 3.2768 MHz'te çalışan bir kristal kontrollü osilatörün çıkışı 512 ile bölünerek taşıyıcı frekans üretilmektedir. Bundan daha güzel bir metot, bir Faz Kilitlemeli Çevrimi düşey senkronizasyona faz kilitlemedir. Gerilim kontrollü osilatör-faz detektörü 256 böleni kullanılarak, gerilim kontrollü osilatörün çıkışı 12.8 kHz yapılır [1].



Şekil 2.16 Spektrum inversiyonu tekniği [1]

Spektrum inversiyonu tekniği için korsan ses düzelticinin merkezi, dengeli demodülatördür. Bu uygulama için en yaygın olarak kullanılan MC1496 entegre devresidir [1]. Bu tür ses karıştırıcılar için korsan kod çözücü tasarımındaki tek fark taşıyıcı frekans üretiminde bulunmaktadır. Bazı tasarımlar, osilatörün ve bölücünün tek bir mikroçip üzerinde bulunduğu 4060 entegre devresini kullanır. Diğerleri ise osilatör (genelikle 4069 entegre devresi) ve bölücü için ayrı birer mikroçip kullanır. Fakat en iyi çözüm, 4060 entegre devresinin kullanılmasıdır [1].

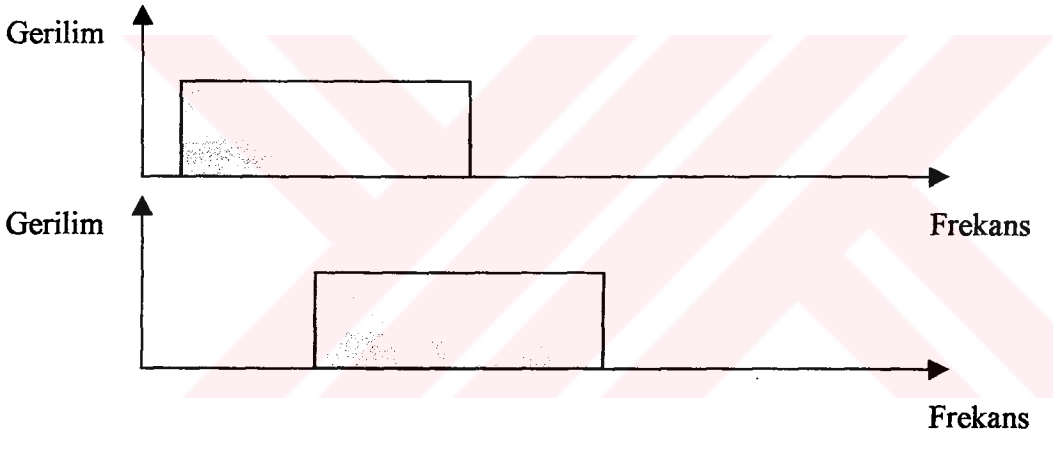
2.5.1.3 Diğer teknikler

Analog ses karıştırıcılarda kullanılan yayılmış (spread) spektrum inversiyonu tekniği birkaç taşıyıcı frekans kullandığı için, eğer bütün frekanslar bilinmiyorsa bu formun hack edilmesi zor olabilmektedir [1]. Bu tür ses karıştırıcı kullanan karıştırıcı sistemlerin büyük bir kısmı, taşıyıcı frekansı elde etmek için bir veya birden fazla kristal kullanır. Düzelticinin kendisi, kristal frekanslarının birinden video parazit taşıyıcısını elde eder. Ses inversiyon frekansı,

aynı zamanda o anda kullanılmakta özel bir taşıyıcı frekansına bağlanmıştır. SAVE sisteminde taşıyıcı frekans, genellikle bu video parazit taşıyıcısının altıda biri kadardır [1].

Bant spektrum inversiyonu ve rotasyonu tekniği, ses spektrumunun farklı bantlara filtre edildiği ve daha sonra bu bantların ters çevrildiği veya döndürüldüğü yerdir. Bu, önceki metotlardan çok daha güvenlidir. Ancak, bu metot daha fazla karmaşıktır ve daha karmaşık bir düzelticiye ihtiyaç duyar. Her bir banttaki ses, işlenmeden önce kusursuz bir şekilde sıkıştırılır. Bu sistem, telefon sistemlerinde kullanılan bazı ses karıştırıcılarında kullanılmıştır. Hack edilmesi diğerler tekniklerden daha zordur. En büyük dezavantajı, karıştırılmış sesin her şeye rağmen bazı bant döndürme kombinasyonlarında fark edilebilir olmasıdır [1].

Karıştırıcılarda kullanılan spektrum kaydırma tekniği ile ses spektrumu, frekansta ileri doğru kaydırılır (Şekil 2.17). Bu teknik, kağıt üzerinde basit gibi görünse de pratikte spektrum inversiyonundan daha karmaşıktır. Ayrıca, maliyeti yüksek olduğu için ses karıştırıcı tasarımlarında yaygın bir şekilde kullanılmamıştır [1].



Şekil 2.17 Spektrum kaydırma tekniği [1]

Tek (single) frekans kaydırma tekniği, SAVE sisteminin şu anda kullanılmayan BBC versiyonunda kullanılmış olan ses karıştırıcı sistem tipidir. Sesi kaydırmak için spektrumun tamamı yaklaşık 1 kHz'lik bir frekansta kaydırılır. Sinyali düzeltmek için, karıştırılmış olan bu spektrum 1 kHz ile geri kaydırılır. Bu genellikle yan bant modülasyon teknikleri ile elde edilmektedir. Bu konu, Elektor Electronics dergisinin Ekim 1991'de yayımlanmış olan sayısındaki bir makalede detaylı bir şekilde anlatılmıştır [1]. Ayrıca elektronik devre diyagramının tamamı ve baskılı devre kartının yerleşim planı bu makalede verilmiştir.

Çoklu frekans kaydırma tekniği, tek frekanslı kaydırmanın kullanımı çok güvenli bir tercih olmadığı için kullanılmıştır. Bu karıştırıcı formu genellikle bir çevrim yapan kaydırma ile

kullanılmıştır. Kaydırma frekansı, birkaç kristalden veya bir sintesayzırdan elde edilebilmektedir [1].

2.5.2 Ses karıştırıcı dijital teknikler

Ses karıştırıcı dijital bir sistemin donanım ile hack edilmesine çok nadir rastlanır. Bu durum sadece FilmNet sisteminin dijital ses sisteminde gerçekleşmiştir [1]. Çünkü dijital ses sisteminin erişim kontrol elemanının hack edilmesi çok kolaydı. Dijital ses sistemlerinin büyük bir kısmının yapısı karmaşık değildir. Bu yüzden bu sistemlerin güvenliği aldatıcıdır. Ses sinyalleri dijitalleştirilir ve sonra bir Yalancı Rasgele İkili (binary) Dizi Üretecinin çıkışı ile EXOR'lanır. Bu üreteç, her birkaç saniyede bir yeni bir başlangıç noktası ile yapılandırılır. Bu biçimde, bu üretecin çıkışı rasgele gibi görünür. Yeniden yapılandırma verisi anahtardır ve genellikle bu anahtar kriptografik algoritmalar ile çok sıkı korunur. Bu, çok basitleştirilmiş bir modeldir. Fakat donanım bakımından yapılabilen en kolay modeldir [1]. Yalancı Rasgele İkili (binary) Dizi Üreteci, uygulamaya özel entegre devrenin bir parçası olarak yapılabilmektedir ve dijital ses kod çözücüsünün devre yapısı, piyasada bulunan parçalarla gerçekleştirilebilir.

FilmNet sisteminin kullanmış olduğu yapı, çok yaygın olarak kullanılmıştır. Klasik devre yapısı, veriyi bir dizi veri akışına demodüle etmekte kullanılmıştır. Daha sonra bu veri akışı, onu işlemden geçiren ve sonra kodunu çözen klasik bir ASIC'i beslemektedir. Kodu çözülen veri, daha sonra dijital/analog konverteri beslemektedir. Bir ASIC'in kullanımı, kripto sistemlerin seçiminde tasarımcılara daha geniş olanaklar tanır. EXOR'lanmış Yalancı Rasgele Dizi Üretecinin en basit metotlarından biri olduğu halde, diğer daha karmaşık olan algoritmalar bu tasarıma dahil edilebilmektedir [1].

Dijital ses bloklarının işlenmesinde DES algoritması gibi eksiksiz bir kripto sistemi kullanılarak oluşturulan daha karmaşık bir çözüm, aslında iyi bir seçim değildir. Çünkü kod çözme işlemi, televizyondaki film müziğini ve videonun senkronizasyonunu etkilememek için yeterince hızlı olmalıdır [1]. Ayrıca, sesin ayarlanması da mümkün olmalıdır. Bu şekilde ses, videodan çok az önde olacaktır. Kodlama ve kod çözme işlemlerindeki doğal gecikmeler, film müziğini ve videoyu senkronizasyona geri getirir.

Dijitalleştirilmiş sesi kodlamak için DES algoritmasını kullanan bir sistem VideoCipher-II sistemidir. Bu sistem, donanım uygulamasındaki bir kusurdan dolayı hack edilmiştir. Fakat ses kripto sistemi hack edilememiştir [1]. Her şeye rağmen VideoCipher-II sistemi Avrupa'da fazla uzun ömürlü olmamıştır. Çünkü, doksanlı yıllarda geçerli bir sistem olabilmesi için teknoloji bakımından çok eskiydi [1].

Orion ve VideoCipher sistemlerinin her ikisi de sesi dijitalleştirmek için Darbe Kodlu Modülasyon (PCM) kullanmaktadır. Tekniklerden bir tanesi, dijitalleştirilmiş ses bilgisi bloklarının ters yönde iletilmesidir. Bu tür iletim, sıradan bilgisayar korsanlarını yenilgiye uğratmak için yeterince güvenlidir. Fakat bu teknik, tecrübeli bilgisayar korsanları tarafından hack edilebilmektedir [1]. Çünkü her bir bloğun başlangıcını ve sonunu düzelticilere tanıtmak için bir anahtar bulunmaktadır.

Dijital ses, bilinen bir veri standardına göre kodlanmıştır. Bir karıştırıcı sistemde kullanmak için yeni bir veri iletim standardının geliştirilmesi ve test edilmesi, tasarım ekibi için son derece geniş bir bütçe ayrılmadıkça imkansızdır. Dijital ses karıştırmada en yaygın kombinasyon Faz Kaydırmalı Anahtar (PSK: Phase Shift Keying) ve uygulamaya özel bir kripto sistem gibi iyi tesis edilmiş bir veri iletim formatıdır. Bu bakımdan, hack etme işinin ilk aşaması en kolay aşama olacaktır [1]. İlk aşama, kodlanmış verinin sinyalden çıkarılmasıdır. İkinci aşama ise, kripto sistemin hack edilmesidir. Dijital ses iletim formatını temiz veri ile test etmek en yaygın uygulamadır.

Dijital ses formatının birçok değişik tipi vardır. Bu incelemede sadece, Uyarlanabilir Delta Modülasyonu (Adaptive Delta Modulation) ve NICAM isimli dijital ses formatları yer verilmiştir. Bu sistemler günümüzde de Avrupa'daki karıştırıcı sistemlerde kullanılmaktadır. Uyarlanabilir Delta Modülasyonu, uydudan yayın yapan Scientific Atlanta isimli firmanın B-MAC sisteminde ve NICAM ise karadan yayın yapan kanallarda kullanılmıştır [1].

2.5.2.1 NICAM dijital ses karıştırıcı tekniği

NICAM tekniğinde analog ses sinyali dijitalleştirilir ve dijital formattayken sıkıştırılır. Daha sonra bu dijital bilgi, çoklanmış formatta iletilebilir. Böylece, mono kanallar veya stereo bir kanal bir görüntü üzerinden iletilebilir. Daha sonra, alıcı tarafında sinyal dijital olarak açılır ve analog haline geri çevrilir. Sesin sıkıştırıldıktan sonra açılmasının iki temel sebebi vardır. Bunlardan birincisi, iletmek için gerekli olan bit sayısının azaltılmasıdır. İkinci sebep ise, alınan sesteki aşırı sinyal-gürültü oranıdır. Analog ses, 32 kHz'lik bir oranda örneklenmiştir. Bu, 15 kHz'deki maksimum ses frekansının iki katının üzerindedir. İlk ses örneğinde 14 bit vardır. Bu 14 bitlik binary sözcük, dijital olarak 10 bite sıkıştırılmıştır [1].

NICAM sistemi, yetmişli yıllarda BBC televizyon kanalı tarafından geliştirilmiştir [1]. NICAM'ın İngiliz versiyonu, NICAM 728 olarak adlandırılır. Bu 728 sayısı, saniyede iletilen 728 kbit'lik oranı ifade eder. Yani, her milisaniyede 728 bitlik bir görüntü iletilmektedir. Bu bit oranının nerelerde kullanıldığı Çizelge 2.1'de gösterilmiştir.

Çizelge 2.1 NICAM 728 sisteminde kullanılmış olan 728 kbit/s'lik bit oranı [1]

Kullanıldığı Alan	Bit Oranı
8 bitlik Görüntü Sıra Sözcüğü (Frame Alignment Word)	8 kbit/s
5 bitlik Konrol Bilgisi (Control Information)	5 kbit/s
11 bitlik İlave Veri (Additional Data)	11 kbit/s
704 bitlik Ses, Parite ya da Veri (Sound, Parity or Data)	704 kbit/s
TOPLAM =	728 kbit/s

Sıkıştırma prosedüründeki birinci adım, dijital örnekleri her bir blokta 32 örnek olacak şekilde bloklara ayırmaktır. İkinci adım ise, 14 bitlik binary örnekleri 10 bitlik bir 2s Tamamlayıcı (complement) kod kullanarak, bloktaki en büyük örnek kelime büyüklüğü olarak tanımlanmış olan bir doğruluğa kodlamaktır [1].

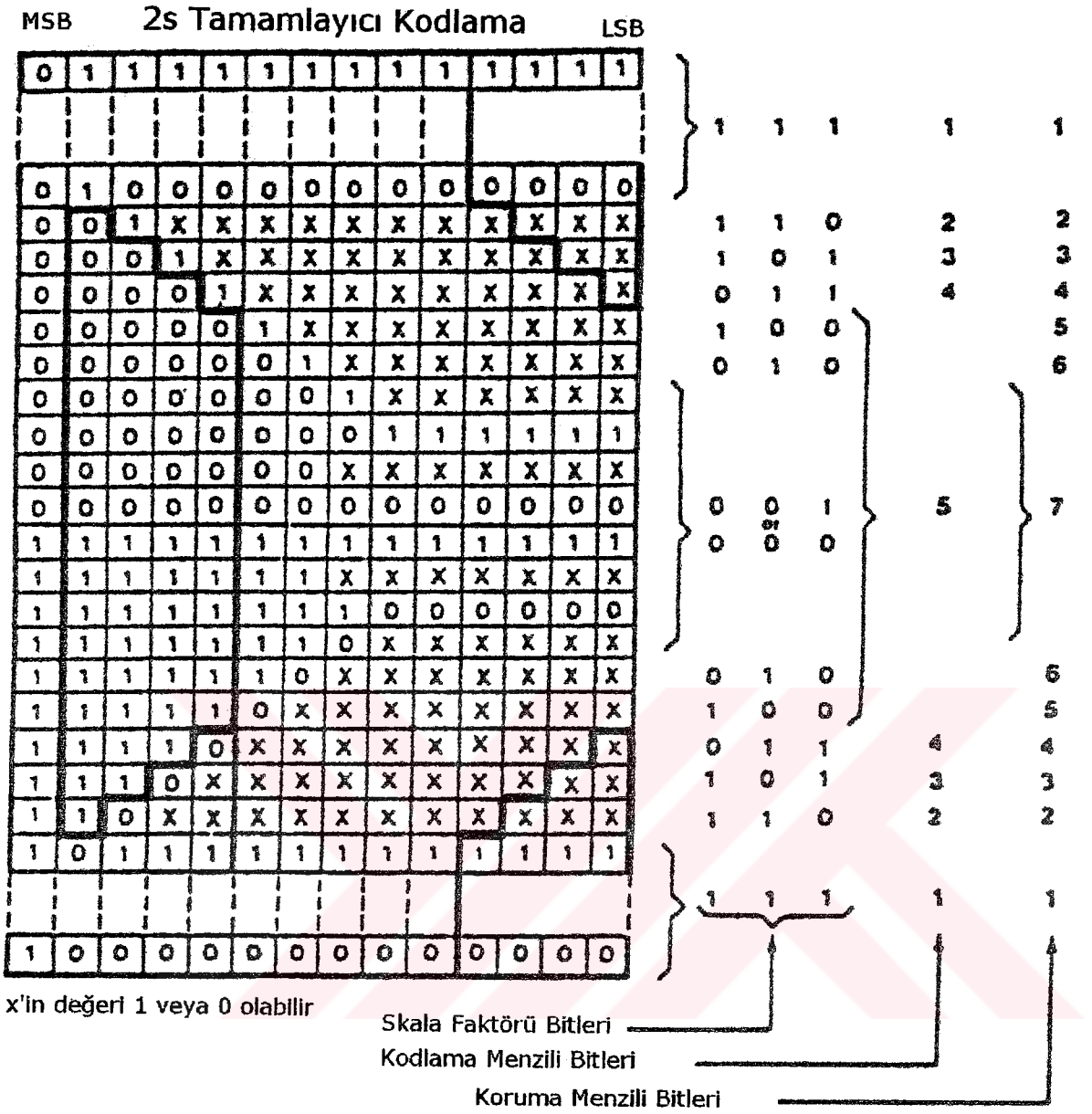
2s Tamamlayıcı kod, bir sayıyı göstermenin alternatif bir yoldur. Bu sayı, sadece 1 ve 0 kullanılarak gösterilir. Sayıdaki bir bit, sayının pozitif mi yoksa negatif mi olduğunu gösterir. Bu bit, sayının işaretidir. Bitlerin geri kalanı, sayının büyüklüğünü gösterir. Bu tipteki gösterime İşaretlenmiş Sayı Gösterimi (Signed Number Representation) adı verilir [1]. Bu sistemde pozitif sayılar, basit işaretlenmemiş ikili olarak gösterilir. Burada hiçbir değişiklik yoktur. Negatif bir sayı için bu durum değişir. Dönüştürülecek olan binary sayı bit bit ters çevrilir. Yani 1'ler 0 olur ve 0'lar da 1 olur. Ters çevrildikten sonra buna 1 eklenir. Bir negatif 2s Tamamlayıcı sayısının en soldaki (önemli) biti (MSB: Most Significant Bit) 1 olur [1]. Aşağıdaki örnek ile bu daha iyi anlaşılacaktır.

14 bitlik örnek, 2s Tamamlayıcı formata dönüştürülür ve sonra, Çizelge 2.2'de verilmiş olan tabloya göre işlem yapılır. 14 bit genişliğindeki 2s Tamamlayıcı sözcüğünün her birinin çıkan 4 biti, son 10 bitlik sözcükten çıkarılmıştır [1].

Örnek: -7 sayısını 2s Tamamlayıcıda göstermek için 0111 (+7 sayısı 0111'e karşılık gelir) ters çevrilir. Böylece 1000 elde edilir. Buna 1 eklenir ve son değer olarak 1001'i bulunur. Böylece, 2s Tamamlayıcı kod cinsinden -7 sayısının 1001'e eşit olduğu görülür [1].

Üçüncü adımda, bir Skala Katsayısı üretilmiştir. Skala katsayısı alıcıya, hangi derecede sıkıştırma kullanıldığını bildirmektedir. Skala katsayısı sözcüğü üç bit genişliğindedir [1].

Çizelge 2.2 NICAM ses karıştırıcısının sıkıştırma tablosu [1]



Kodlama Menzili, Skala Katsayısı ile tanımlanmıştır. Burada beş kodlama menzili vardır (Çizelge 2.3). Bu menziller, 1'in maksimum genliğine bağlıdır.

Çizelge 2.3 Kodlama menzillerinin karşılık geldiği skala katsayıları [1]

Kodlama Menzili	Skala Katsayısı
1. Menzil	1 - 0.5
2. Menzil	0.5 - 0.25
3. Menzil	0.25 - 0.125
4. Menzil	0.125 - 0.0625
5. Menzil	0.0625 - 0

Çizelge 2.3'te görüldüğü gibi, eğer örneklerin bloğu 1. kodlama menzilinde ise, en sağdaki (önemsiz) dört bit atılmıştır. 2. menzil için, en sağdaki üç bit ikinci en soldaki bit olacak şekilde atılmıştır. Her bir durumda, örnekteki bitlerin sayısı her zaman 10'dur. Bu yolla, 14 bitlik örnekler önce 2s Tamamlayıcıya ve sonra da 10 bitlik bir sıkıştırışmış örneğe kodlanır. Alıcı için bir başka bilgi seviyesi, koruma menzili tarafından sağlanır. Ayrıca bu, Skala Katsayısıyla da bağlantılıdır. Bu bağlantı, Çizelge 2.4'te gösterilmiştir.

Çizelge 2.4 Kodlama ve koruma menzili ile skala katsayılarının bağlantısı [1]

Kodlama Menzilleri	Koruma Menzilleri	Skala Katsayıları		
		r1	r2	r3
1	1	1	1	1
2	2	1	1	0
3	3	1	0	1
4	4	0	1	1
5	5	1	0	0
5	6	0	1	0
5	7	0	0	1
5	7	0	0	0

Her bir örneğe bir parite biti eklenmiştir. Bu, en soldaki altı bit kontrol edilerek sağlanmıştır. NICAM görüntüsündeki ses ve parite bitleri, 728 bitin sadece 704 bitinden oluşmaktadır (Şekil 2.18). Geriye kalan bitlerin 8 biti Görüntü Sıralama Sözcüğü, 5 biti Kontrol Bilgisi ve 11 biti İlave Veri tarafından kullanılmaktadır. Görüntü Sıralama Sözcüğü, her bir görüntünün başlangıcında iletilen 01001110 şeklindeki 8 bitlik bir sözcüktür. Görevi, alıcı ile veri akışının senkronizasyonunu sağlamaktır [1].

Kontrol Bilgisi, 5 bitlik bir blok şeklinde iletilir. c_0 olarak adlandırılan birinci bit, görüntü bayrak (frame flag) bitidir. Bu bit, ilk sekiz görüntü için yüksektir ve sonraki sekiz görüntü için düşüktür. Sonraki üç bit olan c_1, c_2, c_3 ses bloğunun içeriğinin nasıl uygulanacağını tanıtmaktadır. Bu bitler için kullanılan en uygun tabir, uygulama kontrol bitleri tabiridir (Çizelge 2.5). Alıcının daha ilerdeki işlemlerindeki ihtiyacını göstermek için kullanılır. Bu bit, alıcının kod çözücü devre yapısındaki anahtarlamayı yapması için kullanılmaktadır. Eğer bu bit yüksek ise ve alıcı gerekli olan kod çözücü devre yapısına sahip değil ise, ses çıkışı kapalı konuma gelir. Beşinci bit olan c_4 biti, yedek ses anahtarlama bayrak bitidir. Bu bit, frekans modülasyonlu alt taşıyıcı NICAM ile aynı kanalı taşıdığı zaman yüksek olur [1].

Çizelge 2.5 Uygulama kontrol bitleri tablosu [1]

Veri			Ses Bloklarının İncelenmesi
c1	c2	c3	
0	0	0	Stereo sinyal. Değişimli örnekler.
0	1	0	M1 ve M2 isimli İki Mono kanal. Değişimli görüntüler.
1	0	0	Bir Mono ses, bir veri kanalı. Değişimli görüntüler.
1	1	0	704 bitlik bir veri kanalı

Burada on bir ilave veri biti vardır. Bu bitlerin işlevi tanımlanmamıştır. Bu bitler, servis tanımlayıcı olarak veya diğer verileri iletmek için kolaylıkla kullanılabilir.

NICAM iletmek için kullanılan modülasyon formatı, Diferansiyel olarak Kodlanmış Dörtlük Faz Kaydırmalı Anahtarlama (DEQPSK: Differentially Encoded Quadrature Phase Shift Keying) olarak adlandırılır [1]. Veriyi iletmek için gerekli olan bant genişliğini azalttığı için mükemmel bir modülasyon sistemidir. Her bir faz değişimi, 1 bit çiftini veya verinin iki bitini temsil eder. Çizelge 2.6'da, taşıyıcı fazın kalan durumu (rest state) verilmiştir. Bu durumlar, birbirlerinden doksan derece ayrıdır. Taşıyıcı faz, bir bit çifti tarafından önceden belirlenmiş olan miktar ile fazı değiştirilinceye kadar bu durumlardan birinde kalır. Her 1 bit çifti tarafından neden olunan faz değişimi Çizelge 2.6'da gösterilmiştir.

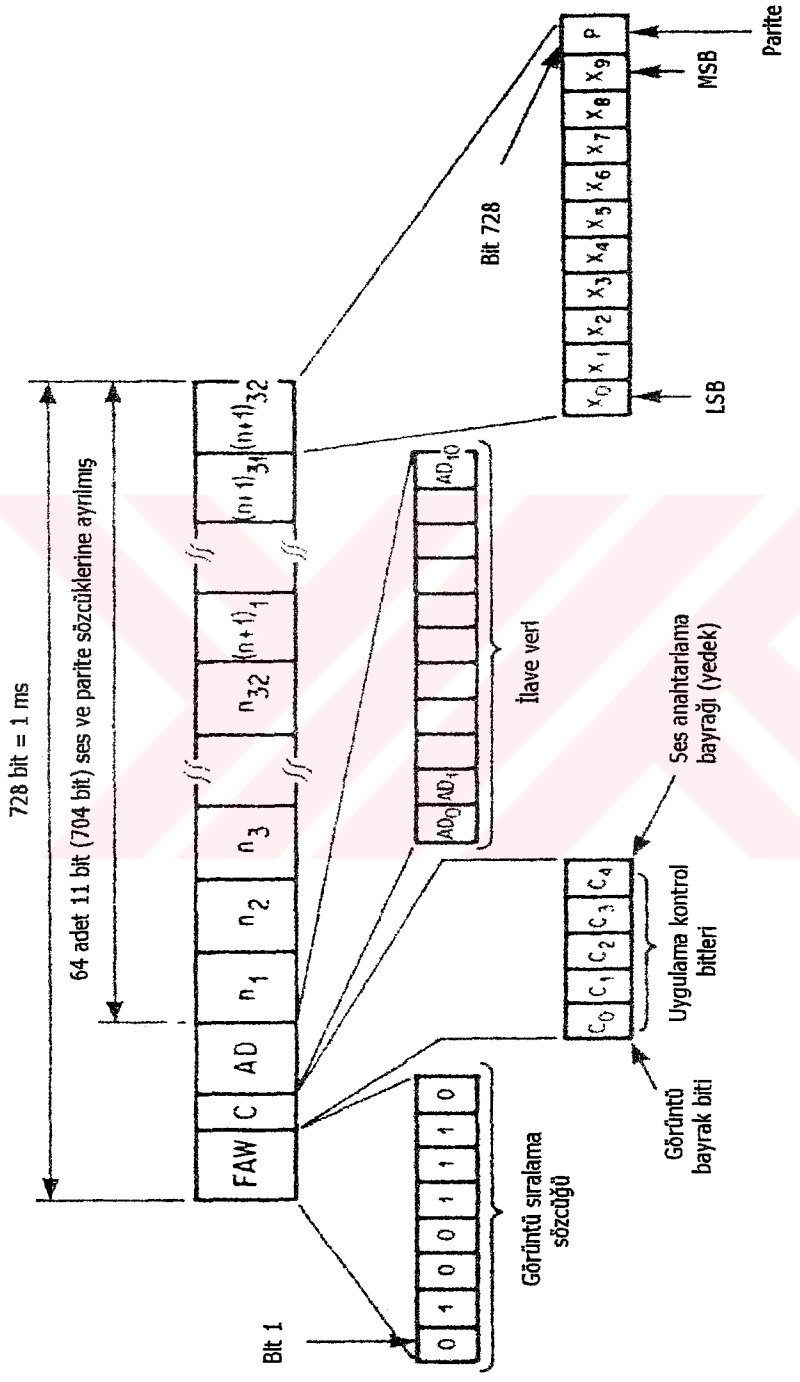
Çizelge 2.6 Faz değişimine karşılık gelen bit çiftleri [1]

1 Bit Çifti		Derece Cinsinden Faz Değişimi
A	B	
0	0	0°
0	1	-90°
1	0	-270°
1	1	-180°

Kalan durumdaki taşıyıcı ile bir 10 bit çifti, -270 derecelik bir faz değişimine neden olur. Bu, taşıyıcı fazı 4. kalan durumuna yerleştirir. Bir başka 11 bit çifti uygulamak, 2. kalan duruma göre -180 derecelik bir faz kaymasına neden olur. Bir başka 01 bit çifti uygulamak, 3. kalan duruma göre -90 derecelik bir faz kaymasına neden olur. Negatif kaymanın saat yelkovanı yönünde olması sıradan bir durum değildir. Modülasyon formatı karmaşık değildir. Bir bit çifti, taşıyıcının fazını doğrudan doğruya bir önceki faz ile karşılaştırarak yeniden elde edilir.

728 bitlik görüntü bit çiftlerine dönüştürülmeden önce veri akışı, spektrum şekillendirme amacı için karıştırılır. Bu, verinin gürültü gibi görünmesi ve böylece videoda veya diğer ses taşıyıcılarında minimum parazite neden olması için yapılır [1]. Bir yalancı rasgele dizi üreteci,

veri akışı ile EXOR'lanır. Yalancı rasgele dizi üreteci, dokuz katlı bir tiptir. Başlangıç durumuna getirme sözcüğü 111111111'dir [1]. Görüntü Sıra Sözcüğü karıştırılmamıştır. Karıştırılmış olan birinci bit Görüntü Sıra Sözcüğünden hemen sonra gelen bittir ve karıştırılmış olan sonuncu bit, Görüntü Sıra Sözcüğünden hemen önce gelen bittir. Görüntünün düzeltilmesinin, alıcıda gerçekleşmesi gereklidir [1].



Şekil 2.18 NICAM dijital ses karıştırıcısının 728 bitlik yapısı [1]

Bilgi dijital formatta ise kodlamak çok kolaydır. En kolay metot, Görüntü Sıra Sözcüğünü kodlamaktır. Bu, geçerli Görüntü Sıra Sözcüğüne sahip olmayan bir NICAM düzelticisinin görüntüyü çözmemesini sağlar. NICAM dijital sinyali, gürültünün azaltılması amacıyla bir Yalancı Rasgele Sayı Üreteci ile EXOR'lanmıştır. Yalancı Rasgele Sayı Üreteci, sabit bir çekirdeğe yapıya sahiptir. Eğer değişken bir çekirdek kullanılmış ise basit ama etkili bir kodlama sistemi sonuca varabilir. Kodlama sistemi için anahtarlar, düzelticilerin içinde tutulabilir veya NICAM sinyalindeki kullanılmamış olan bitlerde düzelticilere iletilebilir [1].

NICAM formatı, bir uydu televizyonu uygulamasına kolaylıkla adapte edilebilir. Bu standartta gerçekleştirilen ilk ve en belirgin değişiklik taşıyıcı frekanstır. İngiltere'de kullanılmış olan NICAM 728 için taşıyıcı frekans 6.552 MHz'dir. Bu frekans, saniyede 728 kbit olarak iletilen bit oranını 9 ile çarparak elde edilmiştir. Bu bit oranı 10 ile çarpılarak 7.28 MHz'lik bir taşıyıcı frekans elde edilir. İngiltere'de havadan yayın yapan sistemlerdeki NICAM taşıyıcı bant genişliği 700 kHz'dir. Bu değişikliğin en iyi tarafı, normal bir NICAM demodülatörüne yapılması gereken değişikliğin sadece taşıyıcı kristal frekansı ve girişteki bant geçiren filtre olmasıdır [1].

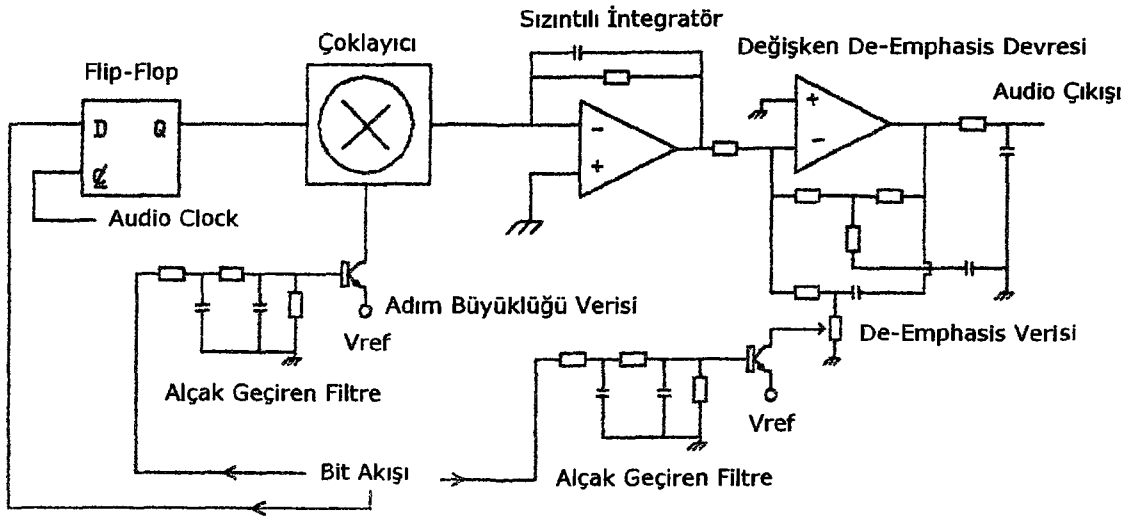
2.5.2.2 Uyarlanabilir delta modülasyonu tekniği

Uyarlanabilir Delta Modülasyonu formatı, Dolby Laboratories tarafından geliştirilmiştir. Scientific Atlantic firmasının B-MAC sisteminde kullanılmıştır. Günümüzde bu sistem, AFRTS ve SIS Racing ödemeli televizyon kanalları tarafından kullanılmaktadır [1].

Delta, matematikte değişimi göstermek için kullanılır. Bir delta modülasyonu sisteminde delta, değişikliğin yönünü göstermektedir [1]. Delta, pozitif veya negatif olabilir. Burada, sıradan delta modülasyonu sistemleri ile bağlantılı olan bir dezavantaj vardır. Ses sinyalinin genliği, nicelendirici adım büyüklüğünden (Analog/dijital dönüştürücünün dijital çıkışındaki bir bit değişimini gerçekleştirmek için gerekli olan minimum voltaj değişimi) biraz daha büyük değiştiği zaman bir aşırı yüklenme meydana gelir. Uyarlanabilir Delta Modülasyonu, değişken bir adım büyüklüğü ve değişken bir ön vurgu (pre-emphasis) kullanarak bu problemin üstesinden gelir [1].

Kodlayıcıda ses girişi sürekli olarak izlenmektedir. Böylece, en iyi adım büyüklüğü ve ön vurgu seçilebilmektedir. Uyarlanabilir Delta Modülasyonu, 200 ve 300 kbit/s arasında bir bit akışı üretmektedir. Adım büyüklüğü ve ön vurgu verisi, daha düşük bir bit oranında iletilmektedir [1]. Böylece, kod çözücü tasarımı basitleşmektedir.

Adım büyüklüğü ve ön vurgu verisinin daha yavaş bit oranları, basit bir alçak geçiren filtre ile filtrelenebilmelerine olanak tanır. Şekil 2.19'da gösterilmiş olan Uyarlanabilir Delta Modülasyonu kod çözücüsünün basitleştirilmiş devre şemasında, kod çözme işlemi açıkça belirtilmiştir.



Şekil 2.19 Uyarlanabilir delta modülatörünün basitleştirilmiş devre şeması [1]

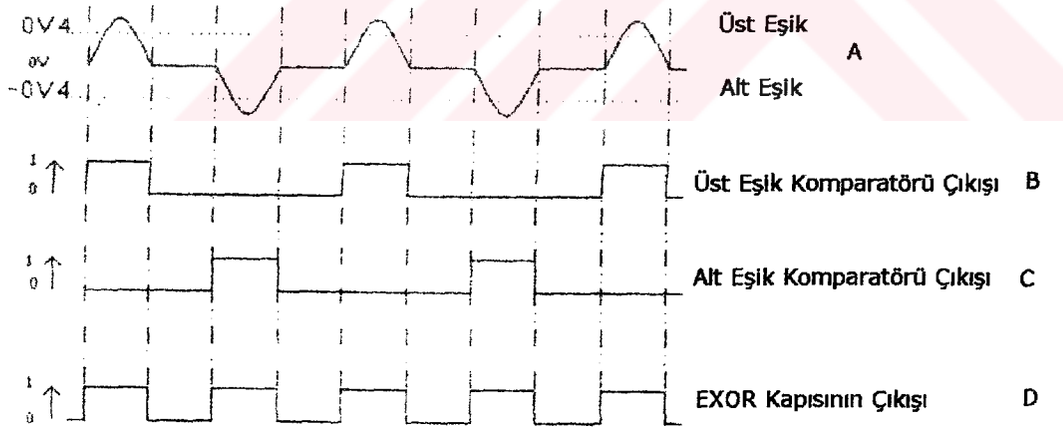
Dijital ses verisi bir flip-flop'u beslemektedir. Bu flip-flop, ses clock frekansı ile tetiklenir. Flip-flop'un çıkışı ya 1 ya da 0 olur. Bu çıkış, bir çarpıcıyı (multiplier) besler. Çarpıcı, iki voltajın sonucunu oluşturmak için kullanılan analog bir devredir. Çarpım katsayısı, adım büyüklüğü verisi ile belirlenir. Çarpıcının çıkışı sızdıran bir integratörü besler. Aslında çarpıcının çıkışı, ayrık voltaj noktalarının bir kümesidir. Sızıntılı integratör, daha düzgün bir sinyal vermek için bu voltaj noktalarını birleştirir. Daha sonra bu sızıntılı integratör çıkışı, değişken de-emphasis devresini besler. Sonra bu bileşke ses kuvvetlendirilir ve modülatörü veya ses çıkışını besler.

Uyarlanabilir Delta Modülasyonu kod çözücüsü, NE5420 mikroçipi olarak mevcuttur. Bu, stereo bir kod çözücüdür ve Scientific Atlanta firması tarafından üretilmiş olan B-MAC düzelticilerinde kullanılmıştır [1]. Bu düzelticilerde dijital ses, Uyarlanabilir Delta Modülasyonu formatına dönüştürülmeden önce kodlanmalıdır. B-MAC sisteminde kullanılmış olan kodlama sistemi DES algoritmasının biraz değişik biçimidir. Ayrıca bu, DES algoritmasından daha güvenlidir. Bu sistemdeki sesi, henüz hack edememiştir. Bunun yerine, erişim kontrol yazılımı hack edilmiştir [1].

2.5.2.3 Duobinary kodlama tekniği

Duobinary kodlama tekniği, oldukça kolay bir veri kodlama metodu olduğu için karmaşık olmayan kod çözücü tasarımlarına izin vermektedir. D-MAC ve D2-MAC sistemlerinde kullanılmıştır [1]. Bu sistem, veriyi bir üç seviyeli dalga biçiminin seviyesi ile taşıyan bir baseband sistemidir. Bu analog benzeri görünüş, MAC sinyalinin resetlenmesi ile beraber uydu televizyonu iletimi için frekans modülasyonlu olabileceği anlamına gelmektedir. D-MAC sisteminin dezavantajı, satırın video kısmının frekans modülasyonlu olmasını ve veri kısmının 2-4 PSK (Phase Shift Keying) modülasyonlu olmasını gerektirmesidir. Yani, iki demodülatör gereklidir ve kodlayıcı devre yapısı aşırı derecede karışıktır. D-MAC sisteminde, her bir satırın sesinde ve veri paketinde 209 veri biti vardır. D2-MAC sisteminde ise her bir satırın paketinde 105 bit vardır [1].

Bir duobinary kodlayıcı üç aşama olarak kabul edilebilir. Tüm işlem, dijital ve ses tekniklerinin bir birleşimidir. Birinci aşama, bit akışını ön kodlamadır (pre-code). Bit akışı ters çevrilmiştir. Bit akışındaki her bir bit, daha sonra bir önceki bit ile hemen EXOR'lanır. Daha sonra, yeni bit akışı bir seviye kaydırıcıyı besler. Bu, bir +1 ve -1 bit akışı oluşturur. İkinci aşama, kodlayıcının görevi olan kodlama kısmıdır. Ön kodlanmış bit akışı bir bitlik gecikmeye maruz bırakılmıştır ve lineer olarak kendisine eklenmiştir. Bileşke sinyal, genlik sınırlı olduğu için maksimum video seviyesini aşamaz.

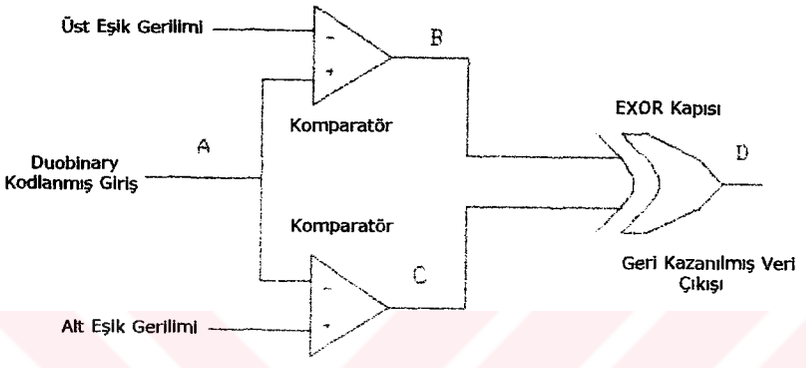


Şekil 2.20 Duobinary kod çözücüyü besleyen dalga biçimleri [1]

Üçüncü aşama ise, alçak geçiren filtrelemedir. Bu, eğer bit akışı harmonikler üretmiyorsa gereklidir. Alçak geçiren filtreleme için diğer bir sebep, D2-MAC ses ve veri paketi için gerekli olan bant genişliğini yaklaşık olarak 5.026 MHz'e düşürmektir [1]. D-MAC sisteminde filtre, D-MAC sesini ve veri paketinin bant genişliğini yaklaşık olarak 10.5 MHz'e

sınırlar. Binary kodlanmış sinyalin seviyeleri +0.4 V, 0 V ve -0.4 V'tur. Lojik 1, +0.4 V ve -0.4 V ile gösterilmektedir (Şekil 2.20). Lojik 0 ise 0 V ile gösterilmektedir [1].

Binary kod çözücünün çalışma şekli aşırı derecede basittir. Teorik olarak iki komparatör, bir EXOR kapısı ve bir invertörden oluşur (Şekil 2.21). Binary sinyal, bu iki komparatörü beslemektedir. Kompararörün bir tanesi sinyali üst seviyede kırpar (slice). Diğer komparatör ise sinyali, alt kırpma seviyesinde kırpar. Bu komparatörlerin çıkışı, EXOR kapısını besler. EXOR kapısının çıkışı ise invertör kapı ile ters çevrilir ve orijinal bit akışı yenilenir [1]. Veri kırpıcı genellikle, ayrık devre yapısı olmaktan ziyade tümleşik devre olarak mevcuttur.

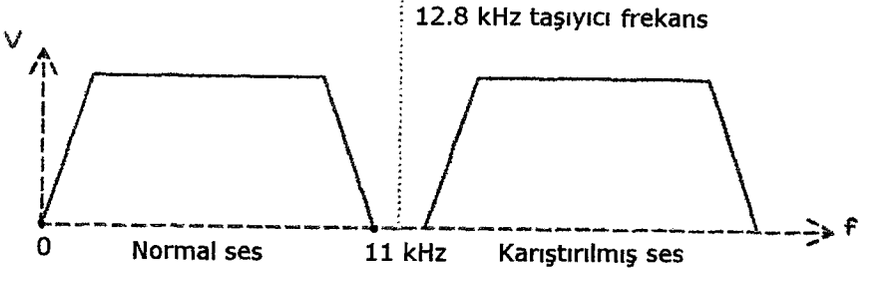


Şekil 2.21 Duobinary kod çözücü devre yapısı [1]

2.6 Karıştırıcı Sistemlerin İncelenmesi

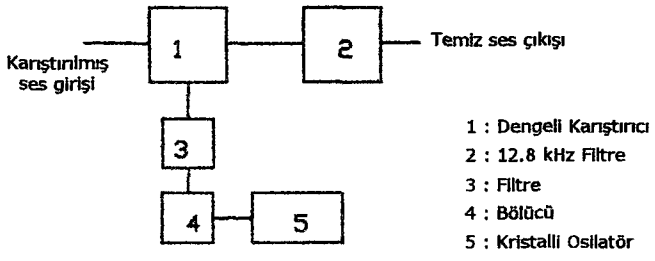
2.6.1 RITC Discret-I sistemi

RITC Discret-I sisteminin kullanmış olduğu video karıştırıcı yöntemi, video satır geciktirmesidir. Her bir satırdaki video bilgisi 0 ns, 902 ns veya 0.1804 ns gecikme sürelerinden biri ile geciktirilmektedir [1]. Bu gecikme süreleri, yalancı rasgele bazda uygulandığından karıştırılmış video düzenli bir biçim almaktadır.



Şekil 2.22 Spektrum inversiyonu ile sesin karıştırılması [1]

Bu sisteminin kullanmış olduğu ses karıştırıcı yöntemi ise spektrum inversiyonudur. Sesin spektrumu, yaklaşık 12.8 kHz'lik bir taşıyıcı frekans ile ters çevrilmektedir (Şekil 2.22). Bu taşıyıcı frekans, orijinal düzelticilerdeki sistem clock'undan elde edilmektedir [1].



Şekil 2.23 Radio Plans ses düzelticisinin blok diyagramı [1]

Bu sistemi kullanan kanallar, Canal Plus (Fransa) ve MMDS/Cable'dır [1]. Canal Plus, 1984 yılının Kasım ayında Discret-I karıştırıcı sistemini kullanarak yayına başlamıştır. Bu sistem ilk çıktığında, hack edilemez olduğu ilan edilmişti. İlk bakışta, bu sistemin güvenli olduğuna inanmak için iyi bir sebep vardı. Çünkü orijinal düzelicilerde, piyasada bulunmayan kendine özgü entegre devreler kullanılmıştı ve mikroişlemci kontrollüydü. Abonelerin düzelticileri, kanal tarafından havadan gönderilen sinyaller ile açılabilmekte veya kapatılabilmekteydi.

Fransız Radio Plans dergisinin Aralık 1984 sayısında, Canal Plus için bir korsan düzelticinin nasıl yapılacağını anlatan bir makale yayımlanmıştı (Şekil 2.23). Doğal olarak Canal Plus, bu durumdan memnun olmadı. Bu dergiye karşı yasal dava açtılar ve başarılı oldular. Mahkeme tarafından dergiye el kondu. Mahkeme tarafından, Radio Plans dergisindeki tasarımın patent yasalarını ihlal etmediği, fakat insanları hırsızlığa teşvik ettiği kararı verildi. Fakat bu makalenin yeteri kadar kopyası piyasaya sürülmüştü ve isteyen herkes bunu temin edebilmekteydi. Bu problem, bir Fransız gazetesinin bu makaleyi tekrar yayınlamasıyla daha çok artmıştı. Fransa'da artık bu durum çok farklıdır. İzinsiz olarak yayımlama çok ciddi bir suçtur. Tabiki bu durum problemi sınırlamakta fakat ortadan kaldıramamaktadır [1].

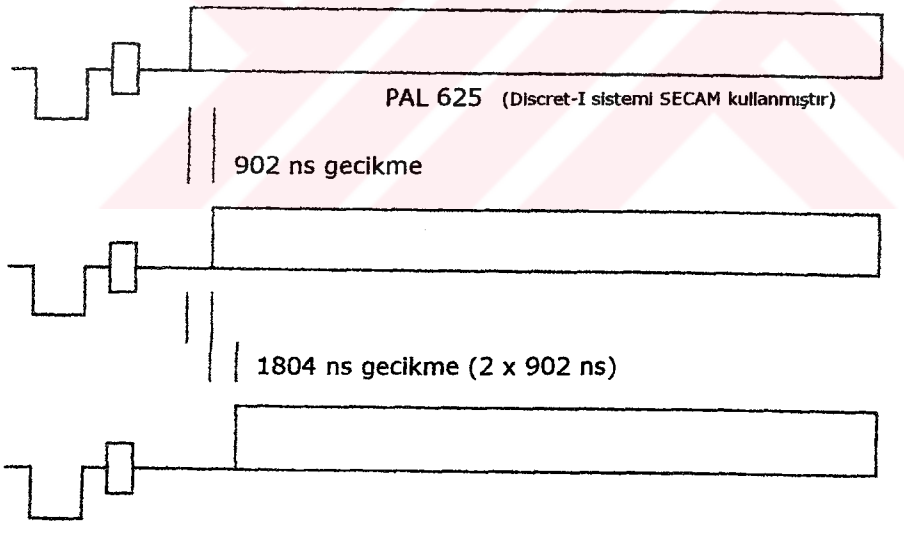
Canal Plus, Discret sistemini kullanmaya karar vermeden önce bu sistem piyasada mevcuttu. İlk başta bu sistem, TV5 kanalının Tunus bağlantılarında kullanılmaktaydı. Bu uygulama için kullanıldığı zamanlarda korsanlık çok azdı. Çünkü, gerekli uydu yakalama teçhizatına sahip olan çok az sayıda bilgisayar korsanı vardı. Canal Plus, karasal yayın yaptığı için sinyal birçok bilgisayar korsanı tarafından elde edilebilir olmuştu [1].

Discret sistemi, iki özelliğe sahip olan bir sistemdir. Hem videoyu hem de sesi

karıştırmaktadır. Discret sisteminden önceki sistemlerin büyük bir kısmı senkronizasyon darbelerine ve ara sıra da sese tesir etmekteydi. Discret sistemi, aslında videoyu belirli bir işleme tabi tutmaktadır. Bu, her şeyden önce bir baseband karıştırıcı sistemidir [1]. RF sinyali demodüle edilmeli ve düzeltilmeden önce bileşik video ve ses sinyaline dönüştürülmelidir.

SCART soketinin ortaya çıkmasından sonra, düzelticilerin televizyon bağlantısının daha etkili bir şekilde yapılması sağlanmıştır. Fransız yasalarına göre, bütün renkli televizyonlarda bir SCART soketinin bulunması zorunludur. RF tipi ve baseband tipi olmak üzere iki tip düzeltici imal edilmiştir. RF tipi düzelticiler, kendi alıcı cihazına (tuner) ve demodülatörüne sahiptir. SCART soketli televizyonlar ile kullanmak için tasarlanmıştır. Baseband düzelticiler, televizyondaki SCART konnektörüne direkt olarak bağlanmaktadır. Televizyonun alıcı cihaz/demodülatör devresi, düzelticiye bileşik video ve ses sinyalini sağlar. Düzeltici bu sinyalleri düzeltir ve temiz video ve ses sinyallerini televizyona geri verir [1].

Discret sistemindeki video karıştırıcı, satır geciktirmesi olarak adlandırılır. Her bir satırın aktif video kısmı, yalancı rasgele olarak 0 ns, 902 ns veya 1804 ns gecikme sürelerinden biri ile geciktirilmiştir (Şekil 2.24). Bu tip karıştırıcı, ekranda videonun çok düzenli bir şekilde görünmesini sağlar. Görüntünün eğlence değeri tamamen yok edilmemiştir.

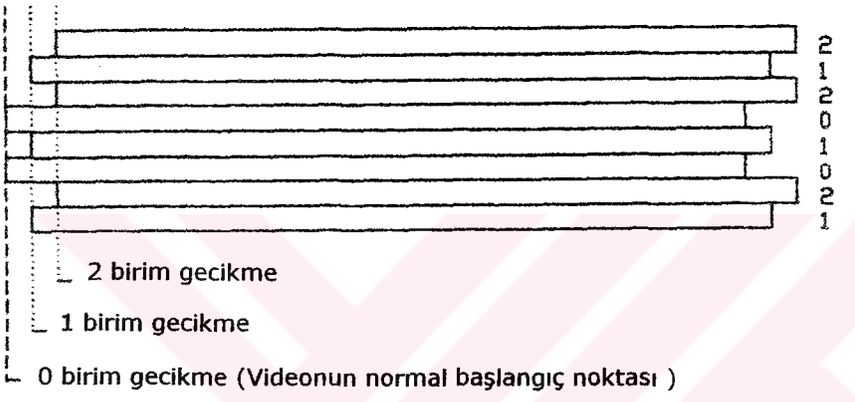


Şekil 2.24 Satırlardaki aktif video kısmını geciktirerek video karıştırma [1]

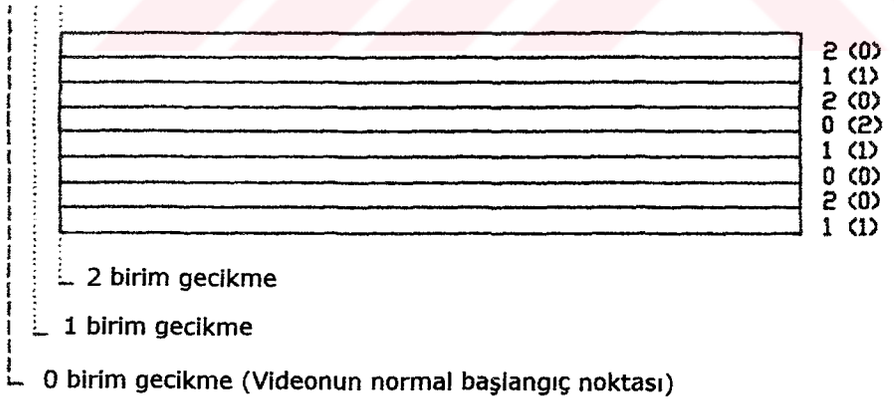
Discret sistemindeki ses karıştırıcı, spektrum inversiyonudur. Ses spektrumu, bir taşıyıcı frekans etrafında ters çevrilmiştir. Bu, sesin robot sesi gibi duyulmasını sağlamıştır. Karıştırılmış Discret sistemindeki sesin eksikliği, görüntünün eğlence değerini yok etmiştir.

Gecikmelerin sırası rasgele değil, yalancı rasgeledir. Yani gecikme sırası, altı alandan sonra tekrarlanmaktadır. Abone için gerekli olan orijinal düzelticide bir geçiş sayısı yazılmalıdır. Aboneliğin ilk ayında, herhangi bir sayı çalışabilir. Bundan sonra, abonenin kendi geçiş sayısı sadece kendi düzelticisinde çalışır. Radio Plans tasarımında bu karmaşıklık bulunmamaktadır. Radio Plans devresinin basitliği, Canal Plus'ın buna karşı koymasını kolaylaştırmıştır [1].

Aktif videonun başlangıcına siyah düzeyinden gelen artış tespit edilmiştir. Aktif videonun nereden başladığını kontrol etmek için bir zaman slotu (time slot) kullanılmıştır. Burada üç slot kullanılmıştır. Eğer aktif video birinci slotta başlamışsa, o zaman video geciktirilmemiştir. Eğer aktif video ikinci slotta başlamışsa, video 902 ns ile geciktirilmiştir. Eğer aktif video üçüncü slotta başlamışsa, video 1804 ns ile geciktirilmiştir (Şekil 2.25).



Şekil 2.25a Satır geciktirilmesi ile karıştırılmış video [1]



Şekil 2.25b Karıştırılmış videonun Radio Plans tasarımı düzeltici ile düzeltilmesi [1]

Radio Plans tasarımı düzeltici, Şekil 2.25a'da gösterilmiş olan satır geciktirilmesi ile karıştırılmış olan video satırlarına Şekil 2.25b'de parantez içinde verilmiş olan gecikme birimlerini ekleyerek gerçek sıralarına koymakta ve böylece ekrandaki görüntüyü düzeltmektedir. Ayrıca, bütün satırların iki birim geciktirilmiş olduğu da görülmektedir.

Radio Plans tasarımı, videonun bütün satırlarının 1804 ns gecikmeye sahip olmasını sağlamıştır. Prensip olarak bu, basit bir işlemdi. Eğer video geciktirilmemişse, o zaman 1804 ns'lik bir gecikmenin içinden geçirilmektedir. Eğer video 902 ns ile geciktirilmişse, o zaman video 902 ns'lik bir gecikmenin içinden geçirilmektedir. Eğer video 1804 ns ile geciktirilmişse, o zaman hiçbir gecikmeye maruz bırakılmadan geçirilmektedir.

Sinyal düzelticideki asıl problem, video geciktirmede sinyalin yeridir. Buna basit bir çözüm bulunmuştur. Bir süreksiz renk geliştirici (colour transient improver) entegre devresi olan TDA4560 kullanılmıştır. Bu entegre devre, 888 ns'lik bir gecikme sağlayabilecek bir jiratör gecikme satırına sahiptir [1]. Bu tasarımda, bu entegre devreden iki adet kullanılmıştır. Fakat bu entegre devrenin temin edilmesi çok zor olduğu için bunun yerine cam gecikme satırları (glass delay lines) ve LC gecikme satırları denenmiştir [1].

Radio Plans tasarımının çalışma metodu, hack edilmesini kolaylaştırmıştır. Canal Plus, siyah düzeyinden başka bir düzeyi gecikme alanı içine enjekte etmiştir [1]. Bu, video bulucu devresinin başlangıcını, videonun geciktirilmemiş olduğunu düşünmesini sağlayarak aldatmıştır. Canal Plus'ın bu konudaki uzmanlığı artarken, bilgisayar korsanlarının uzmanlığı da artmıştır. Bilgisayar korsanları, sabit düzey modifikasyonunun üstesinden gelmiştir. Sinyalin düzeyi gecikme alanına enjekte edildiğinde, bunu tespit etmek için bir komparatör devre kullanılmıştır [1]. Daha sonra bir lojik EXOR kapısı, bunun siyah, gri veya beyaz gibi değişmez bir düzey olup olmadığını kontrol etmek için kullanılmıştır. Bir düzeyin yanı sıra parazit patlamasının (noise burst) eklenmesi, karşılaştırıcı devresini aldatmıştır.

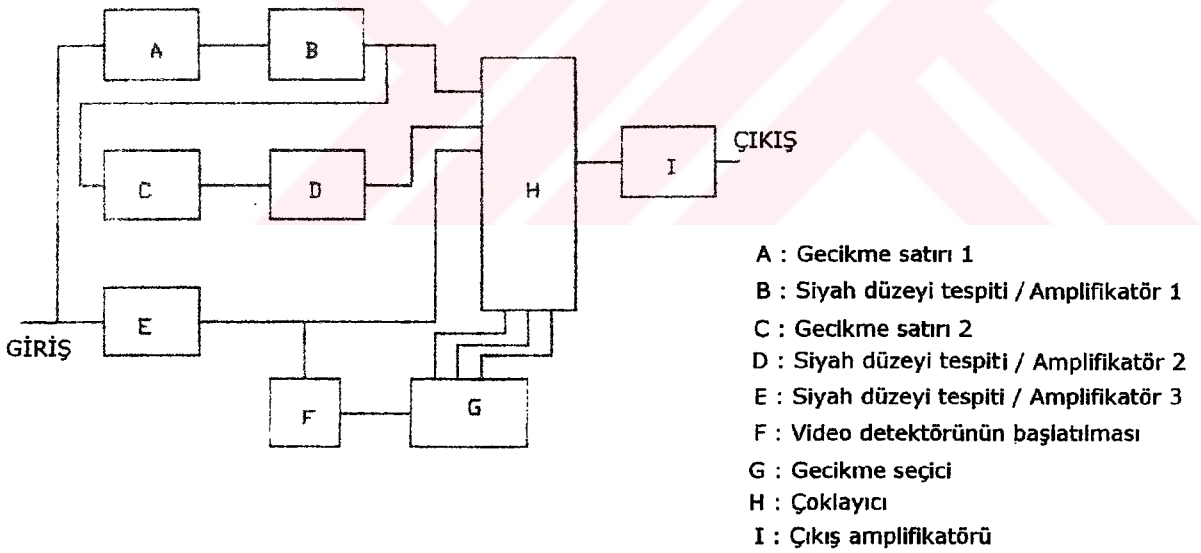
Bazı bilgisayar korsanları Radio Plans tasarımından hareket ederek mikroişlemci tabanlı düzelticileri geliştirdiler [1]. Bu düzelticiler, altı alan sırasının başlangıcını ve sonunu tespit etmiştir. Bu sıra her ay değiştiği zaman, bu mikroişlemci yeni sırayı öğrenebiliyordu. Şu an kullanımda olan korsan düzelticilerin çoğunun bu formatı kullanmaktadır. Buna paralel olarak, bu düzelticilerin şu an çok sınırlı çalışma ömrü vardır.

Mikroişlemci tabanlı düzelticilerin çoğunu başarıya ulaştıran elektronik karşı tedbirlerden biri Sahte Bayrak (False Flag)'tır [1]. Bu basit olarak şu şekilde açıklanabilir. Bir Discret sinyalinde bir sıranın sonu, anlaşılır bir şekilde bayraklanmıştır. Düzelticiler bunu, öğrenme rutinlerini başlatmak veya kilitlemek için kullanmıştır. Sıradan koşullar altında bu sıra, altı alan uzunluğundadır [1]. Bu yüzden, her altı alanda bir sıra bayrağı bulunmak zorundadır. Sıra bayrağının sonunda bulunan bir sahte bayrak, burada bulunmaması gerektiği zamanlarda bulunur. Bu, korsan düzelticilere gerekli olmadığı halde rutini başlatmalarına yol açmaktadır.

Ayrıca, sıra uzunluğu da değiştirilmektedir.

Korsan düzelticilerde video sinyali üç tampon amplifikatörün, iki gecikme satırının ve bir çoklayıcının içinden geçmektedir (Şekil 2.26). Lojik devre yapısının yüzeysel bilgisi, senkronizasyon sinyallerini ve renk patlamasını korumak için kullanılmaktadır. Ayrıca video sinyali, video detektörünün başlangıcını beslemektedir. Bu devre, video bilgisinin başlangıcındaki siyah düzeyindeki artışı tespit etmektedir. Bu devrenin çıkışı, gecikme detektörü adı verilen lojik bir devreyi beslemektedir. Satır senkronizasyon darbesi tarafından tetiklenmiş bir dizi tekkararlı kullanarak videonun başladığı peryodun tayin edilmesiyle bu gecikme kontrol edilmektedir. Her bir tekkararlının peryodu 902 ns'dir. Bu devrenin çıkışı, çoklayıcıyı kontrol etmektedir.

Eğer bu sinyal sıfır gecikmeye sahipse, o zaman iki gecikme satırı tarafından beslenir. Eğer bu sinyal bir birim gecikmeye (902 ns) sahipse, o zaman bir gecikme satırı tarafından beslenir. Eğer bu sinyal iki birim gecikmeye sahipse, o zaman doğrudan doğruya çoklayıcı tarafından beslenir. Düzeltici, bütün satırların iki birimlik bir gecikmeye sahip olmasını sağlamaktadır. Bu, her bir görüntünün sol tarafındaki kenarda, genellikle çoğu televizyonda tarama sonunda kaybolan bir siyah satır meydana getirmektedir.



Şekil 2.26 Radio Plans video düzelticisinin blok diyagramı [1]

Radio Plans düzelticinin tasarımında bir zayıflık vardı. Bu zayıflık, sistemin siyah seviyesinden herbir satırdaki videonun başlangıcına kadar olan artışın tespit edilmesine dayalı olmasıydı. Eğer gecikme, siyah düzeyinden başka bir düzey ile yapılmışsa, Radio Plans düzeltici çalışmamaktaydı [1].

Discret-I sistemi, dijital bazlı bir sistemdir. Videoyu karıştırmak ve düzeltmek için videonun dijitalleştirilmesi gereklidir. Gecikmeler, dijital kaydırma yazmaçları (digital shift registers) kullanılarak dijitalleştirilmiş videoya tanıtılmaktadır.

Radio Plans tasarımındaki devre yapısındaki en yenilikçi örneklerden bir tanesi, her bir satırın ilk birkaç milisaniyesini dijitalleştirmek ve dijitalleştirilmiş olan bu bilgiyi bir gecikmeyi tespit etmek için kullanmaktır. Her bir satırdaki video kısmının ön başlangıcı, birkaç kere örneklenmektedir. Her bir örneğin genişliği, en küçük gecikme zamanına karşılık gelmektedir. Eğer bu bayt, siyah düzeyi için dönüştürülmüş eşdeğerine (genellikle 00000000 ikili kod) karşılık gelmezse video başlamaktadır. Bu, sekiz girişli bir NAND kapısı kullanılarak kontrol edilmektedir. Düzelticinin dijitalleştirilmiş videoyu clock out yapabilmesinin iki yolu vardır [1]. Discret-I düzelticisinde olduğu gibi, mevcut satır en çok geciktirilmiş satır ile uyumlu olması için geciktirilebilir veya bir sonraki satır peryodunda ne olacağı görülünceye kadar video geciktirilebilir ve sonra clock out yapılır ve doğru zamanda analog hale dönüştürülür. Yukarıdaki tespit etme metodu güvenli olduğu zaman, Discret düzelticilerin çoğunda yaygın olarak kullanılmamıştır.

Discret sistemi, yapısal olarak güvenli bir sistem değildir ve geliştirilmiş yeni versiyonlarının büyük bir kısmı kısa bir süre içinde hack edilmiştir [1]. En yaygın yeni versiyonu, gecikmelerin sırasını değiştirmek ve gecikmeleri siyah olmayan düzeyler ile yapmaktır. Bu sistemin karşı karşıya kalmış olduğu ana problem, korsan düzelticilerin gecikme sırasının doğrusunu anlayabilir olmasıdır.

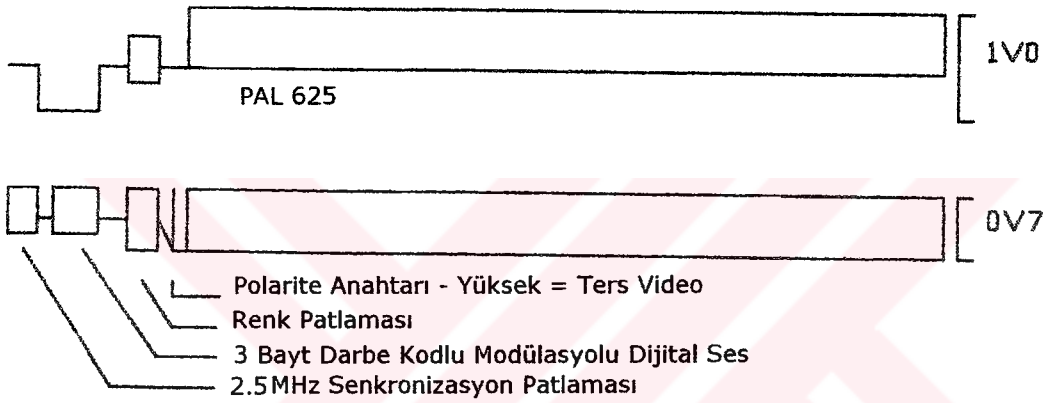
İrlanda'da Cablelink firması bu sistemi bir süre kullanmıştır. Daha sonra bu sistem beğenilmemiş ve güvenilmez bulunmuştur. Abonelerine vermiş oldukları düzelticiler, orijinal Fransız modelinin biraz değişiği olduğu açıkça görülmekteydi. Fransa'daki Canal Plus bu sistemi kullanmaktan vazgeçince, piyasada bir sürü ikinci el düzeltici mevcuttu [1]. Bu teçhizatların maliyetinin düşük olması, bu sistemi küçük sermayeli kablolu televizyon firmalar için cazip kılmaktaydı. Fakat bu sistemin kullanılması mantıklı değildi. Çünkü bu sistem hakkında bilgisayar korsanlarının bilgisi ve uzmanlığı mevcuttu.

Discret kod çözücüsünün en tehlikeli noktası, kritik adresleme verisinin kod çözücünün içinde bulunan ve kolayca okunabilecek olan bir EEPROM içinde tutulmasıdır. EEPROM'u okumak için gerekli olan bütün programlar, ilgili internet sitelerinden ve BBS'lerden kolayca elde edilebilmektedir. Bu EEPROM'u okumak, gerçekten zor bir iş değildi. Korunmamış kritik veri kusuru, seksenli yılların başlarında tasarlanmış olan sistemlerde çok yaygındır. Bu

EEPROM'un içeriği kopyalandığı zaman, orijinal kod çözücüleri bu veri ile yeniden programlayarak bir dizi klonlanmış kod çözücü yaratılması mümkündü [1].

2.6.2 OAK Orion sistemi

OAK Orion sisteminin kullanmış olduğu video karıştırıcı yöntemi yatay ve düşey senkronizasyon yenileme, rasgele veya dizisel alan veya satır inversiyonudur [1]. Alışılagelmiş olan yatay ve düşey senkronizasyon darbeleri, karıştırılmış videodan çıkarılmış ve 2.5 MHz'lik patlamalarla (burst) yenilenmiştir (Şekil 2.27). Her bir satırdaki video, tersine çevrilmiş veya normal polaritede olabilir. Her bir satırdaki videonun başlangıcından hemen önce yerleştirilmiş olan bir darbe, videonun polaritesini göstermektedir. İnversiyon; satır, alan veya görüntü bazında gerçekleşebilir [1].



Şekil 2.27 Oak Orion karıştırıcı sistemi [1]

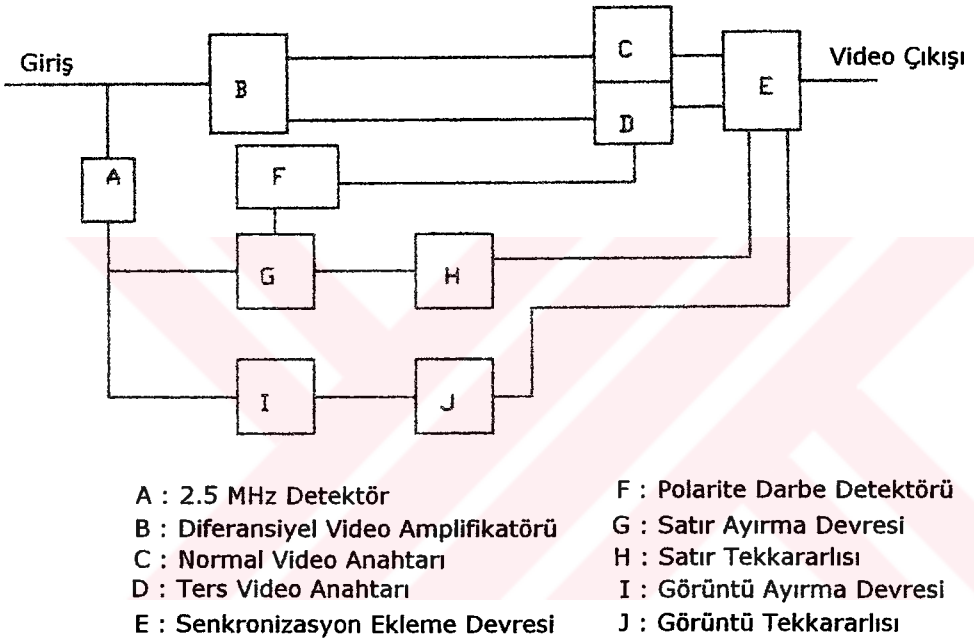
Bu sistemde kullanılmış olan ses karıştırıcı yöntem ise kodlama özelliğine sahip olan dijital ses karıştırıcıdır. Ses, dijitalleştirilmiş ve sıkıştırılmıştır. Daha sonra bu dijital ses örnekleri, normalde olmaları gereken yer olan yatay silme aralığının içine konmuştur [1].

OAK Orion karıştırıcı sistemi, pek çok bilgisayar korsanının düşünebileceğinden çok daha güvenliydi. Bu sistemi Avrupa'da kullanmış olan tek uydu servisi Sky Channel (1982-1987) isimli televizyon kanalıydı [1]. Sky, gerçek anlamda bir ödemeli kanal (pay-tv) olmadığı için bu uygulamada minimum güvenlik düzeyi kullanılmıştır. Mono ve stereo alt taşıyıcıları sinyalle birlikte iletildiğinden dalga biçimi üzerindeki ses özelliği Sky Channel tarafından kullanılmamıştır.

Bu sistemde, altı farklı inversiyon modu kullanılabilmektedir. Tek satırlarda inversiyon, çift satırlarda inversiyon, bütün satırlar tersine çevrilmiş veya hiçbir satır tersine çevrilmemiş olarak adlandırılan bu dört video inversiyon modundan seçilen bir tanesi, her bir alan boyunca

kullanılabilmektedir. Bu tercih için kontrol dizisi yirmi ikinci satırda bulunur. OAK Orion sisteminin orijinal patent (Nr: US 4353088) teknik özelliklerine göre bundan başka ayrıca iki tercihe de sahiptir [1]. Her bir satırdaki dijital paketin voltaj düzeyi kaydırılmış olabilir veya alternatif olarak, bir sinüs dalgası kapısı ile yatay silme peryodundaki düzeyleri başka bir hale döndürmek için değiştirilebilmektedir.

Bu sistemin değişik biçimleri (varyantları) hala kullanılmaktadır [1]. Bununla birlikte, daha güvenli sistemler bu sistemin yerini almıştır. Seksenli yılların başında, bu sistemin sunmuş olduğu güvenlik dikkate değerdi. Fakat EPROM'unu değiştirerek bu sistemin hack edilebileceği gerçeği hayal kırıklığı yaratmıştır.



Şekil 2.28 Korsan Oak Orion düzelticilerinin blok diyagramı [1]

En basit korsan düzelticiler bile 2.5 MHz'lik senkronizasyon patlamasını tespit edebilmektedir ve birkaç tekkararlı kullanarak satır ve görüntü senkronizasyon sinyalini yeniden yaratmaktadır [1]. Sıradan bir korsan düzeltici (Şekil 2.28) şu bloklardan oluşmaktadır; tersine çevrilmiş video amplifikatörü, 2.5 MHz'lik senkronizasyon patlaması detektörü, Schmitt Trigger invertörü, satır senkronizasyon tekkararlıları (monostable), integratör, görüntü senkronizasyon tekkararlısı ve senkronizasyon ekleme devresi. 2.5 MHz'lik senkronizasyon patlamasını tespit etmek için birkaç devre kullanılabilmektedir. Bu devreler, bir diyot detektöründen 2.5 MHz'de çalışan bir video demodülatörü entegre devresine kadar çeşitlilik göstermektedir. Senkronizasyon ekleme devresi, CMOS anahtarlamalı bir tip veya transistörlü bir tip olabilir.

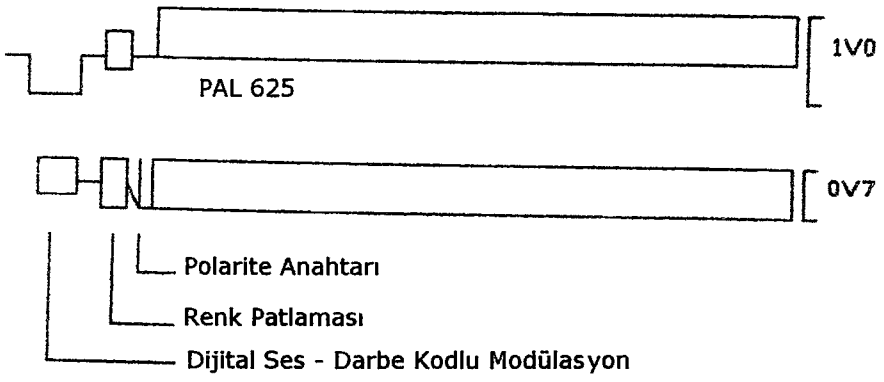
Her satır, video bilgisinden önce yer alan bir inversiyon bitine sahiptir. Eğer inversiyon özelliği her zaman kullanılmış olsaydı, o zaman korsan kod çözücüsünün bu biti örneklemesi ve pozitif ve negatif polariteli video arasında anahtarlama yapabilmesi için senkronizasyon ekleme devresinden önce bir çoklayıcı kullanması gerekirdi.

Bu sistem için bir düzeltici, Pink And Brown Book isimli kitapta yayımlanmıştır [1]. Bu, çok ayrıntılı bir sinyal düzeltici metodudur. Bu, geniş kapsamlı bir düzeltici veya senkronizasyon üretecidir. Ne yazık ki bu sistem artık Avrupa'daki uydu bağlantılarında kullanılmamaktadır. Kullanılmış olan korsan düzelticiler basit tasarımlara sahip olduğundan, Sky kanalı için sistemine başka bir güvenlik düzeyi sokarak bilgisayar korsanlarını engellemek çok kolaydı.

Avrupa'da, dijital ses karıştırıcının hack edildiğini gösteren bir bilgi bulunmamaktadır. Bu sonuçsuz olayın başlıca nedeni, karıştırılmamış bir ses alt taşıyıcısının mevcut olmasıydı. Elector Electronics dergisi, 1987 yılının başlarında Orion için bir video düzeltici tasarımı yayımlamıştı [1]. Sky, bu makale yayımlandıktan kısa bir süre sonra Orion karıştırıcı sistemini kullanmayı bıraktığından bu tasarım pek bir işe yaramamıştır.

2.6.3 LuxCrypt sistemi

LuxCrypt sisteminin kullanmış olduğu video karıştırıcı teknik yatay ve düşey senkronizasyon yenileme ve rasgele veya sırasal alan veya satır inversiyonudur [1]. Alışılagelmiş olan yatay ve düşey senkronizasyon darbeleri, karıştırılmış videodan çıkarılmış ve 5.72 MHz'lik patlamalarla yenilenmiştir. Her bir satırdaki video, tersine çevrilmiş veya normal polaritede olabilir [1]. İnversiyon; satır, alan veya görüntü bazında gerçekleşebilir.



Şekil 2.29 LuxCrypt karıştırıcı sistemi [1]

Bu sistemin kullanmış olduğu ses karıştırıcı tekniği ise dijital bir ses karıştırıcı tekniktir. Ses, dijitalleştirilmiş ve sıkıştırılmıştır. Daha sonra bu dijital ses örnekleri, normalde olmaları

gereken yer olan yatay silme aralığının içine konmuştur (Şekil 2.29). Dijital ses için, üç baytlık veri patlamasının sadece iki baytı kullanılmıştır. Diğer bayt ise senkronizasyon bilgisi ve satır polarite bilgisi için kullanılmıştır. Bu dijital ses özelliği sistemin patentinde bulunmasına rağmen, LuxCrypt karıştırıcı uygulamasında kullanılmamıştır [1].

Bu sistem, Orion sisteminin ilk baştaki haliyle bazı benzer özelliklere sahiptir. RTL4-V televizyon kanalında kullanılmış olan LuxCrypt sistemindeki temel farklılık, 2.5 MHz'lik senkronizasyon patlamasının olmamasıdır [1]. Bu durum, bir korsan Orion düzelticisinde bazı değişiklikler yapılmadan bu düzelticinin LuxCrypt sisteminde çalışmayacağı anlamına gelmektedir.

Video inversiyonu, sahnedeki (scene) beyaz veya siyah miktarına dayandırılabilmektedir. Bu inversiyon tipine Ortalama Tepe Düzeyi (APL: Average Peak Level) adı verilir. Bu inversiyonlar, üç saniye bazlı olarak gerçekleşir.

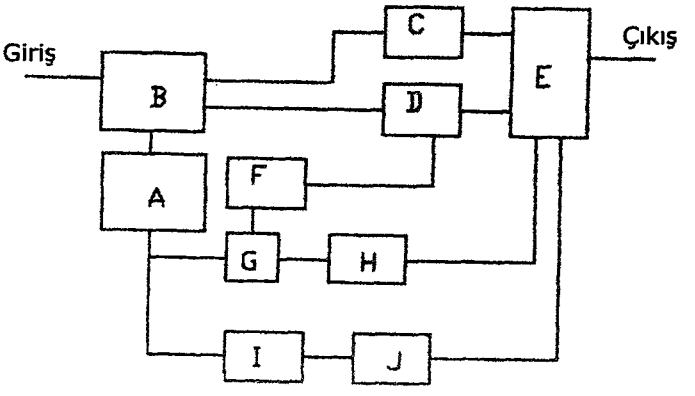
Ortalama Tepe Düzeyi inversiyonu, 1990 yılının Ocak ayında ortaya çıkmıştır [1]. Bilgisayar korsanları üzerindeki etkisi önemliydi. Ticari amaçlı bilgisayar korsanlarının büyük bir kısmı düzeltici tasarımlarını tamamlamışlardı ve Ortalama Tepe Düzeyi inversiyonu esasının var olduğu gerçeğinin farkında değillerdi. RTL4-V, sistemi terfi ettirdiği (upgrade) zaman bilgisayar korsanlarının büyük bir kısmı, tamamlamış oldukları düzelticileri müşterilerine göndermeye hazır hale gelmişti. Bu sistemin terfi işlemi, korsan düzelticilerin müşterilere teslim edilme tarihini birkaç ay ertelemiştir.

RTL4-V düzelticisi, rasgele bazlı bir polarite inversiyonu kullanmaktadır. Bunu saptamak için, satır bazından ziyade sadece alan bazında gerçekleşebilmekteydi. Buradaki amaç, basit tasarımlı kod çözücülerin çalışmasını engellemekti. RTL4-V korsan düzelticilerinin büyük bir kısmı orijinal düzelticinin birebir kopyası olduğu için bu durumdan etkilenmemiştir [1].

En basit korsan düzelticiler bile 5.72 MHz'lik senkronizasyon patlamasını tespit edebilmektedir ve satır ve görüntü senkronizasyon sinyallerini yeniden yaratmak için birkaç tekkararlı kullanmaktadır [1]. Diğer versiyonlar, herhangi bir satırdaki renk patlamasını tespit etmekte ve alan darbelerini tetiklemek için gerekli olan renk patlaması sayısını hesaplamaktadır.

Sıradan bir korsan düzeltici şu bloklardan oluşmaktadır (Şekil 2.30); 5.72 MHz'lik senkronizasyon patlaması detektörü, video amplifikatörü, Schmitt Trigger invertörleri, satır senkronizasyon tekkararlıları, integratör, görüntü senkronizasyon tekkararlısı ve senkronizasyon ekleme devresi. 5.72 MHz'lik senkronizasyon patlamasının tespiti için birkaç

devre kullanılabilir. Bu devreler, bir diyot detektöründen 5.72 MHz'de çalışan bir video demodülatörü entegre devresine kadar çeşitlilik göstermektedir [1]. Senkronizasyon yeniden ekleme devresi, CMOS anahtarlamalı bir tip veya transistörlü bir tip olabilir.



A : 5.72 MHz Detektör
B : Diferansiyel Video Amplifikatörü
C : Normal Video Kapısı
D : Ters Video Kapısı
E : Senkronizasyon Ekleyici
F : Polarite Detektörü
G : Satır Ayırıcı
H : Satır Tekkararlısı
I : Görüntü Ayırıcı
J : Alan Tekkararlısı

Şekil 2.30 Korsan LuxCrypt düzelticilerinin blok diyagramı [1]

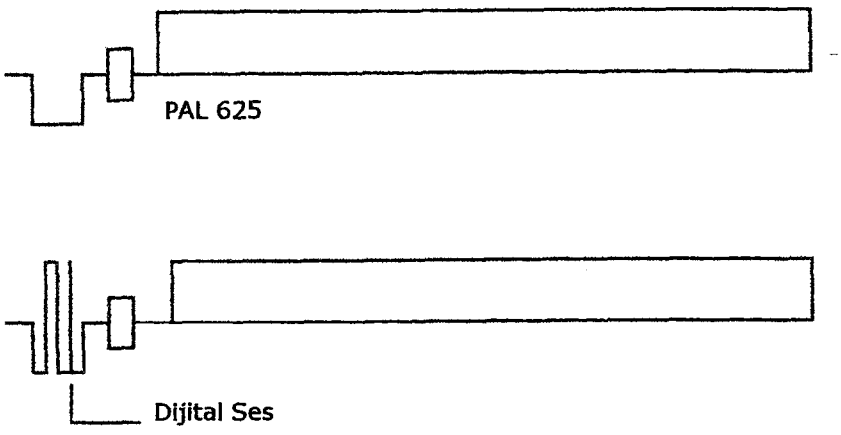
Korsan kod çözücülerin, LuxCrypt sisteminin inversiyon yapısını hack etmek için Düşey Aralıktaki Test Sinyallerindeki siyah düzeyi-beyaz düzeyi satırını örneklemesi gerekmektedir. Bu satırın durumu, alanın polaritesini göstermektedir. Daha sonra bu polarite örneği, senkronizasyon yeniden ekleme devresinden önce bulunan pozitif ve negatif polariteli video arasında anahtarlamayı sağlayan bir çoklayıcıyı kontrol etmek için kullanılmaktadır.

Satır bazlı bir inversiyonu kontrol etmek için kullanılan dijital bilginin bir baytı kullanılarak bu durumun üstesinden gelinebilmektedir. Bu seçeneğin RTL4-V uygulamasında kullanılıp kullanılmadığı bilinmediğinden dolayı bu mümkündü.

Görünüşe göre bu sistem, Ortalama Tepe Düzeyi inversiyonu kullandığından dolayı RTL4-V tarafından benimsenmiştir. Sonuç olarak, eski korsan düzeltici tasarımlarının bazıları çalışmadı. Fakat, XV2000 isimli korsan düzeltici tasarımının hala çalıştığı bilinmektedir [1].

2.6.4 EBU Sound In Synch sistemi

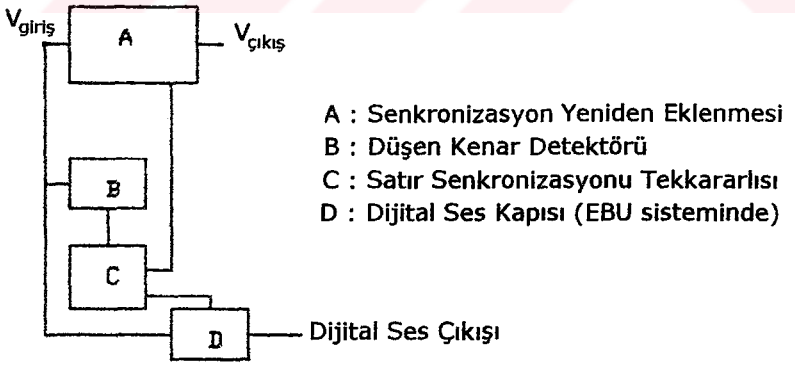
Avrupa Yayın Birliği (EBU)'nin kullandığı dijital sound in synch video karıştırıcı sistemindeki video aslında karıştırılmamıştır. Çünkü dijital ses, yatay silme aralığının içine konulmuştur ve televizyondaki senkronizasyon sıyırıcı bunu ayırt edememektedir [1]. Ekrandaki görüntü düzenli görünmektedir. Fakat bazı anlarda satır sürekliliği kaybolmaktadır.



Şekil 2.31 EBU sound in synch karıştırıcı sistemi [1]

Bu sistemin kullanmış olduğu ses karıştırıcı yöntemi kripto ile darbe kodlu modülasyonudur (Şekil 2.31). Bu sistemde ses, dijitalleştirilmiş ve sıkıştırılmıştır. Fakat bazı durumlarda ses kodlanmamıştır [1]. Fakat yinede bir dijital demodülatör gerekmektedir.

Bu karıştırıcı sistemi Avrupa Yayın Birliği (EBU) kullanmıştır. Bu sistem, uydu iletimi gücünü optimize etmek için tasarlanmıştır. Normal bir uydu iletiminde ses, 5 MHz ile 8 MHz arası menzildeki bir alt taşıyıcı üzerinde iletilmektedir [1]. Bu durum, mevcut gücün bir kısmını tüketmektedir. Bu sistem, sesi video dalga biçiminin içine yerleştirerek tasarruf etmektedir. Bu iletim formatı aslında sadece bir video dalga biçiminden oluşmaktadır. Bunun sonucu olarak, bir ses alt taşıyıcısı için kullanılması gereken güç video için kullanılabilecektir.

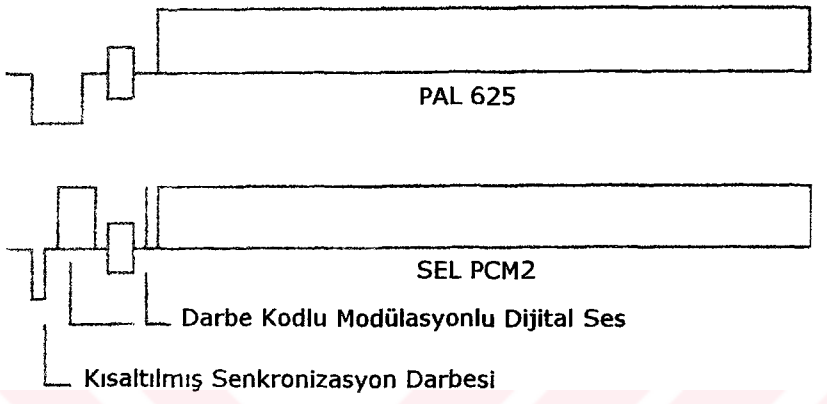


Şekil 2.32 Korsan sound in synch düzelticilerinin blok diyagramı [1]

Bu sistemde video çok kolay hack edilmiştir (Şekil 2.32). Sadece, karıştırılmış sinyaldeki yatay senkronizasyon darbesi alanını, uygun bir şekilde zamanlanmış yeni bir yatay senkronizasyon darbesi ile değiştirilmesi bu sistemi hack etmek için yeterli olmuştur [1].

2.6.5 Standard Electric Lorentz PCM2 sistemi

Bu sistemin kullanmış olduğu video karıştırıcı yöntemi, kısaltılmış yatay senkronizasyon darbesidir. Standart Electric Lorentz (SEL) sistemindeki video, gerçek anlamda karıştırılmamıştır [1]. Yatay senkronizasyon darbesi, 4.7 µs'den yaklaşık olarak 1 µs'ye kısaltılmıştır (Şekil 2.33). Bu durum, televizyondaki senkronizasyon devre yapısının satır kilitlemesini yapamamasına neden olmaktadır. Görüntü darbelerine dokunulmamıştır. Bunun sonucu olarak, görüntü düşey olarak kilitlenebilmekte fakat yatay olarak kilitlenememektedir.



Şekil 2.33 SEL PCM2 karıştırıcı sistemi [1]

Bu sistem, dijital ses karıştırıcı tekniğini kullanmıştır. Kısaltılmış yatay senkronizasyon darbesinin ardından bir ses paketi yerleştirilmiştir [1]. Diğer ses paketi ise, renk patlamasının ardından yerleştirilmiştir.

Standart Electric Lorentz PCM2 sisteminin EBU sisteminden iki temel farkı vardır. Birinci fark, dijital sesin satır karartma aralığında iki noktada yer almasıdır. Bir dijital ses paketi renk patlamasından önce, diğer paket ise renk patlamasından sonra yerleştirilmiştir. Bu sistem Avrupa'da kullanıldığında, bu ikinci paket çok nadir olarak kullanılmıştır [1]. İkinci fark ise, kısaltılmış bir satır senkronizasyon darbesinin kullanılmasıdır. Bu darbe, yaklaşık olarak 1 µs'ye kısaltılmıştır.

Standart Electric Lorentz PCM2 sisteminin video kısmının düzeltilmesi oldukça basittir. Korsan düzeltici, uygun şekilde boyutlandırılmış bir yatay senkronizasyon darbesini tetiklemek için kısaltılmış yatay senkronizasyon darbesini kullanmaktadır. Daha sonra bu yeni senkronizasyon darbesi, kısaltılmış senkronizasyon darbesinin yerine karıştırılmış dalga biçimine sokulmaktadır.

Standart bir senkronizasyon sıyırıcı (stripper) kullanılabilmektedir. Sıyrılmış olan senkronizasyon, 4.7 µs'lik bir darbe vermesi için ayarlanmış olan bir tekkararlıyı

beslemektedir. Ayrıca, dijital sesi demodülatöre kapılamak için kullanılmış olan birkaç kapılama tekkararlısını tetiklemek için 1 μs'lik senkronizasyon darbesi kullanılmıştır [1]. Dijital ses düzeyleri, siyah düzeyi ve beyaz düzeyi arasındadır. Bu, sinyalin düzeltilmeden önce çok iyi tespit edilmesinin gerekli olduğu anlamına gelmektedir. Eğer tespit devresi çok kötü tasarlanmışsa, senkronizasyon darbeleri bazen hasar görebilmektedir [1].

Günümüzde Standart Electric Lorentz PCM2 sistemi, EBU tarafından artık kullanılmamaktadır. Video karıştırıcının hack edilmiş olmasına rağmen bu sistemdeki dijital ses karıştırıcı hack edilememiştir [1].

2.6.6 SATPAC sistemi

Bu sistemin kullanmış olduğu video karıştırıcı yöntemler senkronizasyon kaydırma ve sırasal video alanı inversiyonudur. Ses karıştırıcı yöntem ise kripto ile modifiye edilmiş NICAM sistemidir [1].

SATPAC/Matsushita sistemi, ilk defa 01.09.1986 tarihinde FilmNet kanalı tarafından kullanılmıştır [1]. Bu zamana kadar bu kanal, Avrupa'da uydu üzerinden karıştırılmamış biçimde yayın yapan en popüler kanallardan biriydi. Karıştırıcı kullanıldıktan sonra bu sistem, Avrupa'daki bilgisayar korsanlarının başlıca hedefi durumuna geldi. FilmNet kanalının, Avrupa'daki korsan kod çözücü endüstrisini yaratan kanal olduğu söylenmektedir [1].

SATPAC sistemi, aslında kablolu televizyon kanalları için tasarlanmış olan bir karıştırıcı sistemin uydu yayıncılığında kullanıldığında neler olacağını gösteren en iyi örneklerden biridir. Bu sistem, bilgisayar korsanları tarafından tamamen hack edilmiştir.

FilmNet kanalı, ASTRA uydusu üzerinden bu karıştırıcı sistem ile yaptığı yayını durdurduğu zaman, Yunanistan'a yayın yapan diğer bir FilmNet kanalı bilgisayar korsanları tarafından hedef alınmıştı [1]. Bunun gibi birçok sistemin, eninde sonunda sistemde bazı değişiklikler yapmaya zorlandığı açıkça görülmektedir. Bu sistem hala Avrupa'nın her yerinde kablolu televizyon kanalları tarafından kullanılmaktadır.

SATPAC sistemi, Payview ve kablolu yayında kullanılmış olan Jerrold Tri-Mode sistemleri ile aynı kuşak olan eski bir sistemdir. SATPAC, bu sistemler gibi başlangıçta, senkronizasyon darbeleri ile karıştırmaya ve videoyu ters çevirmeye güvenmekteydi [1]. Analog video karıştırıcı sistemlerindeki korsanlık, FilmNet kanalını buna ilaveten bir ses şifreleme sistemi uygulamaya zorlamıştır. Bu, tamamen tehlikede olan ve değiştirilmesi gereken bir analog karıştırıcı kullanan bir sistem için yanlış bir davranıştır.

Seksenli yılların başlarındaki karıştırıcı sistem teknolojisi, video satırının senkronizasyon kısmıyla karıştırmaya ve yalancı rasgele bazda videoyu ters çevirmeye dayanmaktaydı. SATPAC, videonun polaritesi ve yatay karartma aralıklarının düzeyi ile videoyu karıştırmaktaydı.

FilmNet'in birinci düzeyi, 01.09.1986 tarihinden 23.03.1987 tarihine kadar kullanılmıştır [1]. Bu birinci düzeyi hack etmek aşırı derecede basitti ve bu yüzden, hızla büyüyen bir korsan düzeltici piyasası mevcuttu. 23.03.1987 tarihinde gerçekleştirilen terfi etme işlemi, bu korsan piyasayı çökertmiştir. Çünkü bu, her bir ardarda gelen alandaki videoyu ters çeviren çok kolay bir hack işlemiydi.

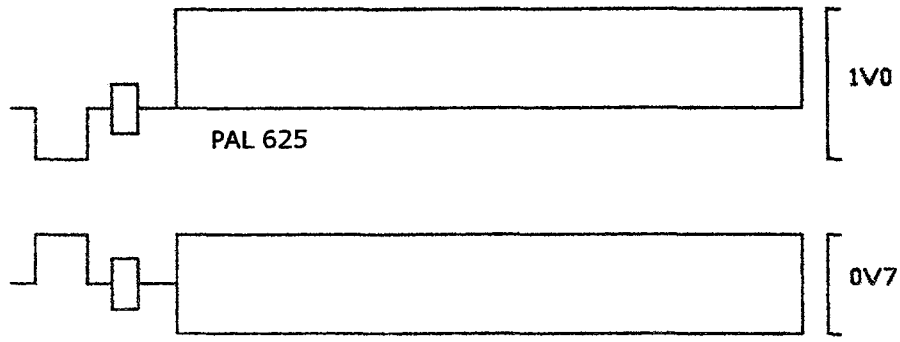
FilmNet sistemi, 24.12.1989 tarihinde tamamen terfi edilmiştir. Bu terfi etme işlemi birkaç gün içinde gerçekleşmiştir. FilmNet'in bu terfi işleminin etkisi, 1987 yılının Mart ayında gerçekleştirmiş olduğu terfi işleminden daha kısa sürmüştür [1]. Korsan düzelticilerin büyük bir kısmı, bu terfi işlemi sonunda etkisiz hale getirilememiştir. Etkilenmiş olan düzelticiler ise çok çabuk terfi edilmiştir ve FilmNet'in gerçekleştirmiş olduğu bu terfi işleminin ömrü sadece iki hafta olmuştur.

1990 yılı Ocak ayının sonunda FilmNet, bazı korsan düzeltici üreticileri için hiçte hoş olmayan etkilere sahip, iki alan sırası tekniğine geri döndü. Korsan düzeltici piyasası, düzeltici terfi işlemini dört alan sırasına göre gerçekleştirmişti. Bu yüzden, korsan düzelticiler FilmNet'in bu terfisinden sonra çalışmadı [1].

FilmNet, 1991 yılında dijital ses sistemini uygulamaya başladığında, mevcut korsan düzeltici piyasasına etkili bir şekilde saldırmıştı. Fakat bunun sonucunda umut ettiği etkiyi elde edemedi. Çünkü, bütün korsan düzeltici üreticilerini yok etmenin yerine sadece küçük firmaları yok etmiştir [1]. Büyük firmalar, dijital ses sistemini hack etme üzerine yoğunlaşmışlardı. Hi Tech isimli firma, gerçekten FilmNet'in dijital ses ASIC'ini ters mühendislikten geçirmişti ve bunu dikkatle inceledikten sonra yeni bir tane yaratmıştı. Hi Tech'in ASIC'i ve kod çözücüsü, orijinal FilmNet dijital ses kod çözücüsünden daha başarılı çalışmaktaydı [1].

FilmNet sinyalini düzeltmek için bilgisayar korsanları tarafından kullanılmış olan birkaç metot vardır. Bunların en yaygın olarak kullanılanları tetiklenmiş tekkararlı kullanarak senkronizasyonun yeniden birleştirmesi, bir faz kilitlemeli çevrim kullanarak senkronizasyonun yeniden birleştirmesi ve senkronizasyonun yeniden üretimidir [1]. Burada sadece, tetiklenmiş tekkararlı tasarımı incelenmektedir.

FilmNet'in kullanmış olduğu birinci düzey, ters çevrilmiş bir satır ve bastırılmış yatay karartma aralığıdır (Şekil 2.34). FilmNet sistemi için kompozit senkronizasyon sinyali, bir taşıyıcı üzerinde 7.56 MHz'de iletilmiştir [1]. Bu taşıyıcı, tipik bir TBA 120 entegre devresini baz alan bir FM demodülatörü ile demodüle edilmiştir. Bu sistemin kablolu televizyon versiyonunda bu taşıyıcı, FM ses alt taşıyıcısı üzerinde genlik modülasyonludur [1].



Şekil 2.34 FilmNet'in SATPAC sisteminde kullanmış olduğu birinci düzey [1]

Demodülasyondan sonra bu bileşik senkronizasyon sinyali, görüntü senkronizasyonuna (bir integratör kullanılarak) ve satır senkronizasyonuna ayrılmaktadır. İlk iki satır tekkararlısı, karıştırılmış videodaki senkronizasyon pozisyonu ile satır senkronizasyonunu aynı faza getirmektedir.

Karıştırılmış videodaki yatay senkronizasyon aralığını tespit etmek için bir gürültü (parazit) kapısı kullanılmıştır. Gürültü kapısının çıkışı, aynı faza getirilmiş olan satır senkronizasyonu ile AND'lenmiştir. Bu, doğru olarak zamanlanmış tetikleme satır senkronizasyonu darbesi sağlamaktadır [1].

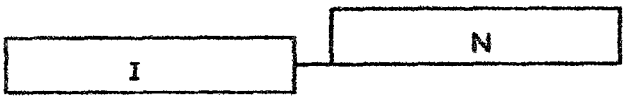
Bu tetikleme darbesi iki tekkararlıyı beslemektedir. Birinci tekkararlı, darbeyi 52 μs ile geciktirmektedir [1]. Daha sonra bu geciktirilmiş darbe, ikinci tekkararlıyı tetiklemek için kullanılmaktadır. Bu tekkararlı yaklaşık olarak, yatay karartma aralığının genişliği kadar bir darbe üretmektedir. Bu darbe, karıştırılmamış düzeye geri gelmek için karıştırılmış videodaki yatay karartma aralığını aşağı çekmek veya kaydırmak için kullanılmaktadır.

1) Terfi 1 (23.03.1987)

FilmNet'in alan bazlı ters çevrilmiş video seçeneğini ilk defa kullandığı durumdur. Video, her bir değişen alanda ters çevrilmiştir (Şekil 2.35). Korsan düzelticilerin büyük bir kısmında, FilmNet'in gerçekleştirdiği bu terfi yıkıcı olmuştur. Çünkü korsan düzelticilerin büyük bir

kısmının elektronik devre kartı ve devre yapısı, bu düşünce ile tasarlanmamıştı [1].

Bu terfiye bilgisayar korsanlarının cevabı, diferansiyel çıkışlı bir amplifikatörün ters çevrilmiş video ve normal video çıkışları arasında anahtarlama yapmak için bir çoklayıcı kullanımı olmuştur. Görüntü darbesi, bir flip-flop kullanılarak iki ile bölünmüştür. Yani, flip-flop'un çıkışı her alanda bir defa polarite değiştirmektedir [1]. Normal videodan ters çevrilmiş videoya gerçek dönüş, bir alanın doğru ucunda gerçekleşmemiştir. Yani, görüntü darbesinin flip-flop'u tetiklemek için kullanılmasından önce biraz geciktirilmesi gerekmekteydi.



I : Ters çevrilmiş video
N : Normal video

Düzey 2 : Birbiri ardından gelen alanın ters çevrilmesi
(İki alan sırası)

Şekil 2.35 FilmNet'in SATPAC sisteminde kullanmış olduğu ikinci düzey [1]

2) Terfi 2 (24.12.1989)

SATPAC sistemi, alan inversiyon sırasının birden fazla düzeyine sahiptir. Bilgisayar korsanlarının büyük bir kısmı, birbiri ardından gelen alan inversiyonunu üstesinden gelmeye çalışırken, birbiri ardından gelen alan inversiyonundan başka bir şey kullanılınca bunun üstesinden gelebilecek bir çözüm üretmeyi ihmal etmişlerdi [1].

I : Ters çevrilmiş video
N : Normal video

Düzey 3 : Dört alan sırası kullanılmıştır. Dördüncü alan normaldir.

Şekil 2.36 FilmNet'in SATPAC sisteminde kullanmış olduğu üçüncü düzey [1]

FilmNet, dört alan bazlı bir inversiyon sırası kullanarak bu zayıflıklarından istifade etti. Dördüncü alan normal polaritedir ve diğer üç alan ters çevrilmiş polaritedir (Şekil 2.36). Bu model, iki flip-flop ve bir AND kapısı kullanılarak yapılabilmekteydi. Birinci flip-flop, 50 Hz'lik alan frekansını 2 ile bölerek 25 Hz'lik bir kare dalga üretmektedir. İkinci flip-flop, 25 Hz'lik bir kare dalgayı 2 ile bölerek 12.5 Hz'lik bir kare dalga üretmektedir. 25 Hz'lik kare dalga ve 12.5 Hz'lik kare dalga, AND kapısı ile birleştirilmiştir. Bu, her dördüncü alanda yüksek (high) olacak bir sinyal üretmektedir [1]. Bunun yerine bir NAND kapısı da

kullanılabilirdi.

FilmNet, 1990 yılının Ocak ayının sonlarına doğru, iki alan sıralı inversiyona geri dönmüştür [1]. Bu terfinin amacı, bilgisayar korsanlarının kafasını karıştırmaktı ve hedefine ulaştı. Fakat bu sırada korsan düzeltici tasarımlarının büyük bir kısmında polarite tespit etme elemanları bu tasarımlara dahil etmişti. Bu, alan inversiyonun artık iyi bir tercih olmadığı anlamına gelmektedir.

3) Terfi 3 (Kasım 1990)

Korsan düzeltici tasarımlarının bazıları, yatay senkronizasyon darbesinin tepesi ve video polaritesi bulucu karartma düzeyi arasındaki voltaj farkının ölçülmesine dayanmaktadır [1]. Bu, FilmNet'in istifade edebileceği zayıf bir noktadır.

FilmNet kanalı, yatay senkronizasyon darbesinin tepesine düşük düzeyli bir yüksek frekans sinüs dalgası patlamasını eklemiştir. Sinüs dalgasının frekansı, yaklaşık olarak renk alt taşıyıcısınınki kadardır. Bunun iki sonucu vardı. Bu, renk patlamasını görüntüyü kilitlemek için kullanan düzelticileri bozguna uğratacaktı. Bu düzelticiler, birbirlerine göre doğru zamanlanmış iki renk patlaması görmekteydi. Ayrıca bu terfi, video polaritesini senkronizasyon tepesi düzeyi ile yatay karartma düzeyi ile karşılaştırarak saptayan düzelticileri de bozguna uğratmıştır [1].

Bu terfi, korsan düzeltici endüstrisinde geniş çaplı bir etkiye sahip olmuştur. Bu, bazı tecrübeli korsan üreticiler tarafından tahmin edilmişti ve bu yüzden bazı korsan düzelticiler bu durumdan çok az etkilenmişti. Eğer korsanların büyük bir kısmı da düzelticilerini daha sonra terfi edilmeye yönelik tasarlamış olsalardı, FilmNet'in gerçekleştirdiği bu terfi korsan düzelticilerin elektronik devre kartlarına sadece bir veya iki parça ilave etmekten ibaret olacaktı.

4) Terfi 4 (Aralık 1990)

FilmNet 1990 yılının Aralık ayında, yatay senkronizasyon darbesindeki patlamanın genliğini 1 Hz'lik çok düşük frekanslı bir dalga ile bu patlamayı genlik modülasyonlu yaparak değiştirmeye başlamıştır [1]. Senkronizasyon tepesi örnekleyici korsan düzelticilerin büyük bir kısmı, senkronizasyon tepesindeki patlamayı filtrelemek için kullandıkları komparatör devresinde tipik bir 100 pF'lık düşük değerli bir kondansatör kullanmıştı. Bu düşük frekans, 100 pF'lık kondansatör patlamayı filtreledikten sonra aynı kalacaktı. Bu patlamanın genliğindeki bu değişen düzey, gerçekte genlik normal polarite olduğu zaman bir sinyali ters

çevrilmiş polarite olarak yorumlayacağından dolayı komparatör için problem yaratacaktır [1].

5) Terfi 5 (Ocak 1991)

SATPAC sisteminin birinci düzeyi, bastırılmış senkronizasyon ve uygulanmamış inversiyondur. FilmNet, 1991 yılı Ocak ayında inversiyonu kullanmaya başladı. Bu girişim, korsan piyasasındaki en iyi birkaç korsan düzelticiyi etkisiz hale getirdi. Bu girişim, düzelticilerdeki düzeltme işleminin yapıldığı kısmı etkilemedi. Fakat, otomatik anahtarlama yapan devre yapısını oldukça etkiledi. Bu korsan düzelticilerin büyük bir kısmı, karıştırılmış video sinyalindeki ters çevrilmiş senkronizasyon darbelerini, düzelticiyi çalışma durumuna tetiklemek için kullanmıştır. Ters çevrilmiş senkronizasyon darbeleri olmadığı zaman korsan düzeltici, sinyali açık (anlaşılır) biçimde yorumlamıştır [1].

6) Terfi 6 (Mart 1991)

1991 yılının Mart ayında korsan düzelticiler, orijinal düzelticilerden daha karmaşık bir yapıya sahip hale gelmiştir [1]. Korsan düzeltici tasarımları, programlanabilir lojik düzenlerini ve diğer uygulamaya özel mikroçipleri baz almıştı. Bu tasarımların büyük bir kısmı, renk patlaması kilitleyicileriydi. Bu düzelticiler, eksiksiz bir yatay ve düşey senkronizasyon üretecini etkili bir şekilde senkronize etmek için karıştırılmış videodaki renk patlamasını kullanmışlardır.

1991 yılının Mart ayında, renk patlamalarının bir sırası düşey senkronizasyona yerleştirildi [1]. Bu uzun süreli patlamalar, renk patlaması kilitleyen düzelticilerin bazılarının patlama hesaplayan devre yapısını şaşırttı. Bunun sonucunda, patlama hesaplayan korsan düzelticiler düşey senkronizasyonu nereye konması gerektiğini görememiştir ve bunun sonucunda ekrandaki görüntü sağa sola doğru kaymaya başlamıştır. Piyasadaki düzelticilerin büyük bir kısmı kullanıcı tarafından tepeleme yapılabilmesini sağlayarak bu problemin üstesinden gelebilmiştir [1].

7) Terfi 7 (Mart 1991)

Bir önceki terfi işlemi piyasadaki en gelişmiş korsan düzelticileri hedef aldığı zaman, korsan düzeltici piyasasının büyük bir kısmı hala FilmNet tarafından iletilmekte olan 7.56 MHz'lik bileşke senkronizasyon taşıyıcısına dayanan tasarımlar kullanmaktaydı [1]. FilmNet'in bu piyasaya Double Glitch modifikasyonu ile karşılık vermiştir. Double Glitch modifikasyonu, her bir darbeye bitişik ikinci bir darbe yerleştirmiştir [1]. Bu, faz kilitlemeli çevrimlerin kilidini açmayı amaçlamaktaydı. Modifikasyonlar genellikle birinci darbenin bitiş

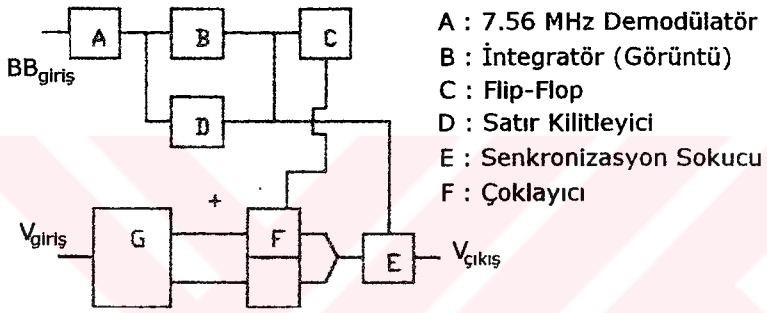
noktasından sonra darbe bulmayı engellemeyi kapsamaktaydı. Bu, bir tekkararlı ve bir çoklayıcı devre ile elde edilebilmekteydi.

8) Terfi 8 (Haziran 1991)

Bu terfi ile dijital ses kavramı ortaya çıkmıştır. ASTRA uydusunun fırlatılmasından sonra ortaya çıkan korsan düzeltici piyasası, bir yıl içinde ortadan kaybolmuştur. Sadece Hi Tech Extravision isimli firma, korsan bir dijital ses düzelticisini piyasaya çıkarabilmiştir [1].

9) Terfi 9 (Eylül 1992)

FilmNet, bütün korsanlık problemlerine bir çözüm olacağını umut ederek, ASTRA uydusu üzerinden PAL standardında yapmış olduğu yayınını keserek D2-MAC EuroCrypt-M sistemine geçmiştir [1].



Şekil 2.37 Tipik bir korsan SATPAC düzelticinin blok diyagramı [1]

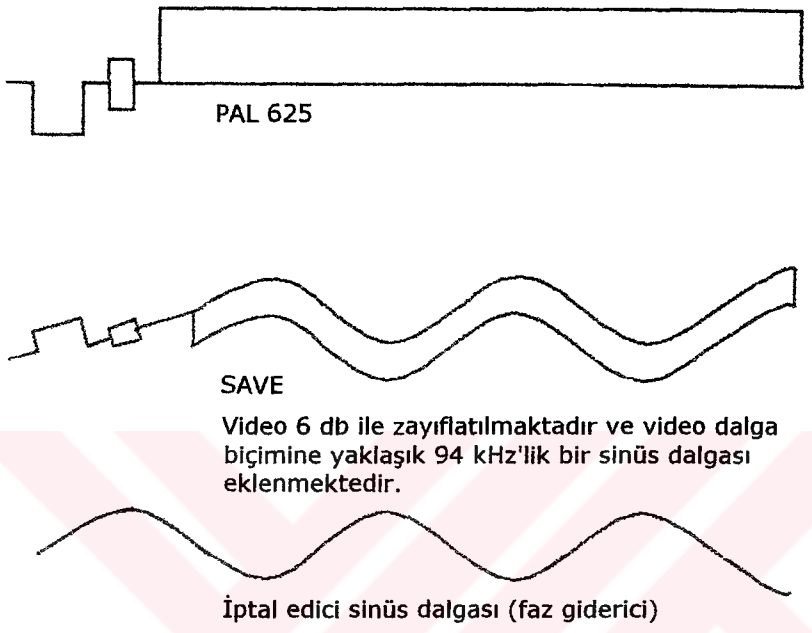
2.6.7 SAVE sistemi

SAVE sisteminin kullanmış olduğu video karıştırıcı yöntemleri sinüs dalgası ile karıştırma, video inversiyonu ve video genliğinin zayıflatılmasıdır. Karıştırılmış sinyaldeki video 3 dB (Avrupa'da 6 dB) ile zayıflatılmış, ters çevrilmiş ve karıştırıcı sinüs dalgası eklenmiştir [1]. Bu sinüs dalgasının frekansı, yatay raster frekansının yaklaşık olarak altı katıdır (15625 Hz x 6 = 93750 Hz).

Bu sistemin kullanmış olduğu ses karıştırıcı yöntemi, spektrum inversiyonudur. Karıştırıcı sinüs dalgası frekansından taşıyıcı frekans elde edilmiştir. Sinüs dalgasının frekansı, taşıyıcı frekansı üretmek için altı ile bölünmüştür [1].

MAAST sistemi, Telease isimli bir Amerikan firması tarafından geliştirilmiştir. Bu sistem Avrupa'da ise, şu an aktif olmayan Sat-Tel firması tarafından SAVE sistemi olarak üretilmiş ve satılmıştır [1]. Aslında bu sistem düşük güvenlikli bir sistemdir.

Bu sistem, video sinyalinin genliğini zayıflatır, videoyu ters çevirir ve videoya bir sinüs dalgası ekler (Şekil 2.38). Bu sinüs dalgasının frekansı, satır frekansının altıncı harmoniğine hemen hemen eşittir. Bu durum, karıştırıcı sinüs dalgasını filtreleme teşebbüslerini engellemeyi sağlar ve bunu karıştırılmış video ile ters fazda yaparak düzeltilmiş videoda örneklenmiş olan bir darbe (vuru) frekansı bırakır [1]. Bunun nedeni, satır frekansının altıncı harmoniğinin de filtre edilerek ayrılmış olmasıdır [1].



Şekil 2.38 SAVE sisteminin kullanmış olduğu sinüs dalgası ile karıştırma yöntemi [1]

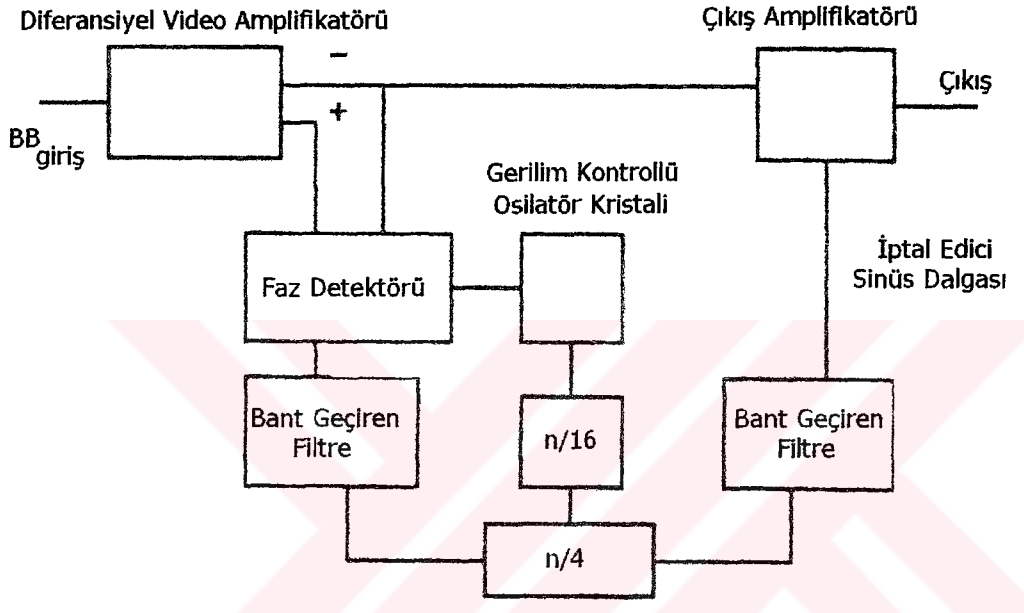
Video zayıflatmanın düzeyi farklılık gösterir. Amerikan versiyonu videoyu 3 dB ile zayıflatır. Avrupa versiyonu ise videoyu 6 dB ile zayıflatmaktadır. Bunun başlıca sebebi transponder bant genişliğinin farklı olmasıdır. Amerikan versiyonu tipik 36 MHz bant genişliğinde çalışmaktadır. Avrupa versiyonu ise 30 MHz bant genişliğinde çalışmaktadır [1].

Bu sistemin Amerika ve Avrupa'da kullanımı oldukça azaldığı sıralarda, şu an yayında olmayan İngiliz Premiere kanalı bu sistemi kullanmıştı. Intelsat uydusunda 27.5 derece batıdan iletilmiş olan BBC'nin hibrit formu, rasgele seçilmiş olan bir frekans kombinasyonu kullanmıştır [1]. Fakat bütün bunlar, bu sistemin hack edilmesini engellemek için yeterli olmamıştır.

En basit bir korsan düzeltici (Şekil 2.39), karıştırıcı sinüs dalgası frekansının 64 katı bir frekansta çalışan gerilim kontrollü bir osilatör kristali kullanır. Aslında bu, bir faz kilitlemeli çevrim devresidir. Gerilim kontrollü osilatör kristali, düzelticinin üretim maliyetini yükseltmektedir. Bu yüzden, bunun düşük maliyetli birçok alternatifi kullanılmıştır.

Avrupa'daki korsan düzeltici tasarımlarının en iyilerinden bir tanesi, 6.0 MHz'lik bir seramik rezonatör kullanmıştır [1].

SAVE sistemi, sesi karıştırma özelliğine sahiptir. Bu özellik, bunun Amerikan versiyonunda kullanılmıştır. Fakat Avrupa'da, stereo alt taşıyıcıların yaygın olarak kullanılmasından dolayı yaygın bir kullanım alanı yoktur. Standart bir ses karıştırıcıda ses spektrumu, nominal bir 15 kHz taşıyıcı etrafında yer değiştirmiştir. Genellikle yer değiştirme için kullanılmış olan taşıyıcı, karıştırıcı sinüs dalgası frekansının altıda biri kadardır ve faz kilitlemeli çevrimin çıkışını bölünmesiyle elde edilmiştir [1].



Şekil 2.39 Tipik bir korsan SAVE düzelticinin blok diyagramı [1]

BBC kanalının kullanmış olduğu SAVE ses karıştırıcı sisteminin özelliği daha karmaşıktı. İnversiyondan ziyade spektrum kaydırmayı baz almıştır [1]. Bundan dolayı, düzelticisi daha karmaşıktı. Spektrum Kaydırmalı karıştırıcı ve düzeltici için akla yatkın bir devre, Elektor Electronics dergisinin Ekim 1991 sayısında yayımlanmıştır [1].

Bu video karıştırıcının BBC formunda, karıştırıcı sinüs dalgası için birkaç frekans kullanılmıştır. Bu durum operatöre, frekanslar arasında geçiş yapabilme olanağı sağlamıştır. Genellikle bu geçiş, transponder video taşımadığı zamanlarda gerçekleşmektedir. Orijinal tek frekans sistemini kullanmış olan korsan düzelticilerin büyük bir kısmının tamamen terfi edilmeye ihtiyacı vardı. En yaygın olarak gerçekleştirilen terfi, yeni bir kristalin ve bir anahtarın kullanılmasıydı. Daha ucuz olan ve çok yönlü olarak kullanılan ise seramik rezonatörlerin kullanımıydı.

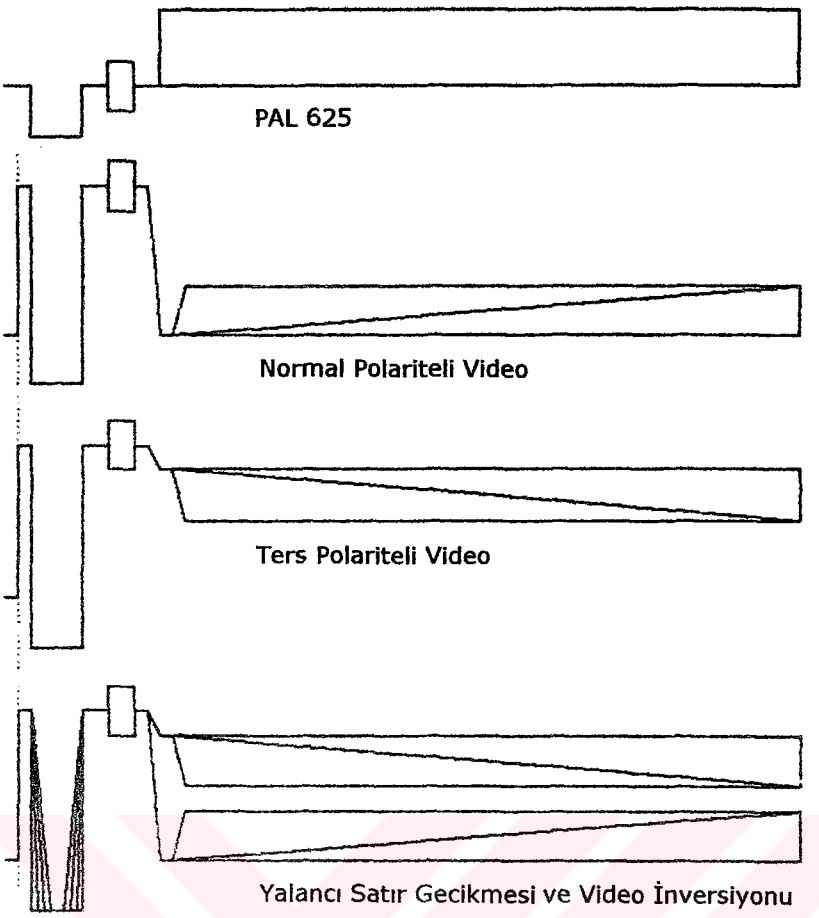
Avrupa'da bu sistemi en son kullanan kanal Red Hot Dutch isimli kanaldı [1]. Sistemin güvenli olmadığının farkındaydılar ve bu sistemi sadece geçici bir önlem olarak kullanma niyetindelerdi. Bu sistemin varyantlarında kullanılmış olan kristal frekansı, 8085 mikroçipinin sistem clock frekansıydı. Bu frekans 96 kHz'e bölündüğü için SAVE sisteminin gücünün avantajından faydalanamadı. Karıştırıcı sinüs dalgası frekansı, satır frekansının altıncı harmonik frekansıyla hemen hemen aynı olduğundan dolayı darbe frekansları üretilmekteydi. Önemli genlik darbe frekansları için 96 kHz'lik sinüs dalgası, 93.750 kHz'den çok uzaktaydı. Bu yüzden bazı korsanlar videoyu ters çevirerek seyredilebilir görüntüyü elde etmişlerdir [1].

2.6.8 PayView-III sistemi

PayView-III karıştırıcı sisteminin kullanmış olduğu video karıştırıcı yöntemler senkronizasyon modifikasyonu, yalancı satır gecikmesi ve video inversiyonudur [1]. Yatay karartma aralığı, beyaz seviyesi düzeyi üzerine yükseltilmiştir. Bu durum, televizyon alıcısının otomatik kazanç kontrolü devresini ve tespit devresini şaşırtmaktadır. Karıştırılmış video televizyonda gösterildiğinde, görüntü karanlık görünmektedir. Yatay senkronizasyon darbesi titretilmekte veya hızla kaydırılmaktadır. Bu durum karıştırılmış videoda yalancı satır gecikmesi etkisine neden olmaktadır (Şekil 2.40). Video satırı, sırasal veya rasgele yapıda ters çevrilebilmektedir. Bu sistemin kullanmış olduğu ses karıştırıcı teknik ise dijital ses karıştırıcıdır.

PayView-III sistemi, uydu üzerinde ilk defa artık yayında olmayan İspanyol Canal 10 kanalı için test edilmiştir [1]. Bu sistem, bu test yayının sonucunda kanalda kullanılmak için uygun görülmemiştir. Teleclub kanalı, 1988 yılında bu sistemi test etmiştir ve 1989 yılında bu sistemi kullanmıştır [1]. Fakat bu sistem, en basit formunda kullanılmıştır. Yani birbiri ardından gelen satır inversiyonu ve yalancı rasgele satır gecikmesi kullanılmamıştır. Bu düzey çok çabuk hack edilmiş ve korsan düzelticiler piyasaya sürülmüştür [1].

Bu sistemin bu en basit formunun hack edilmesi hiçte zor değildi. Rasgele satır inversiyonu, bu sistemde birden fazla problem olduğunu kanıtlamıştır. Yükseltilmiş yatay karartma kısmı, bazı uydu alıcı tiplerinde problemlere yol açmıştır. Bu alıcılarda meydana gelen başlıca problem, yetersiz bant genişliğiydi. Teleclub'ın uydu iletim formatı, 36 MHz'lik bir transponder bant genişliğini kullanmıştır. Bazı bilgisayar korsanları, ASTRA bant genişliğine (26 MHz) sahip alıcıları çok az değiştirerek sinyali yakalamayı denemişlerdi [1]. Bu, bastırılmış veya zayıflatılmış olarak görünen renk patlaması ile probleme yol açmıştı. Fakat Teleclub, bu problemin üstesinden gelmiştir.



Şekil 2.40 PayView-III sistemindeki yalancı satır gecikmesi ve video inversiyonu [1]

Bu sistem, video inversiyonunun hızlı bir formunu kullandığı zaman piyasadaki korsan düzelticilerin büyük bir kısmını işe yaramaz hale gelmiştir. Bu durumun diğerlerinden farkı, bu değişikliğin düzelticinin elektronik kartında gerçekleştirilmemiş olmasıydı. Teleclub'un Nagra Syster sistemine geçmesiyle, PayView sisteminin uydu iletiminde kullanımı sona ermiştir [1]. Fakat bu sistem Avrupa'daki bazı kablolu televizyon kanallarında hala kullanılmaktadır.

PayView sisteminin orijinal düzeyinin hack edilmesi çok kolaydır. En basit düzeltici tasarımı, beyaz seviyesi düzeyi üzerindeki yükselmenin tespit edilmesine dayalıdır. Burada sadece bir komparatör kullanılmıştır. Bu devre tasarımı, Yalancı Satır Gecikmesi Detektör devresi olarak Bölüm 3'te verilmiştir.

Beyaz seviyesi voltajı üzerindeki bu yükselme, bir grup tekkararlıyı tetiklemek için kullanılmıştır. Bu tekkararlılar, doğru olarak zamanlanmış senkronizasyon ve karartma düzeyi darbelerini üretmiştir. Bu darbeler, bir "pull down" devresini ve bir senkronizasyona yeniden sokucuyu kapılamak için kullanılmıştır. "pull down" devresi, renk patlamasını onun gerçek

voltaj düzeydeki eski yerine koymuştur. Senkronizasyona yeniden sokucu, karartma ve senkronizasyon darbelerini eski yerine koymuştur [1].

Senkronizasyona yeniden sokucu kullanımı, gerekli olan bir korumadır. Korsan düzelticilerin büyük bir kısmı yatay senkronizasyon darbesinin negatif giden geçişini kilitleme için kullandığı için yalancı satır gecikmesine geçişle birlikte saldırıya uğramışlardır. Beyaz seviyesinin üzerindeki yükselişi kilitleme noktası olarak kullanmak, bu terfi işlemini etkisiz hale getirmiştir [1].

Bu video inversiyonu, problemlere de neden olmuştur. Eski düzelticilerin büyük bir kısmı, alan bazlı sıra üreteçlerine sahiptir [1]. Bunların bir DIP anahtarıyla doğru sıra için ayarlanması gerekmekteydi. Bu düzelticileri etkisiz hale getirmek için yarım sıralar kullanılmıştır. Bunun sonucunda sıra üreteçleri işe yaramaz hale gelmiştir.

Gelişmiş düzelticilerin bazıları, video inversiyonunu tespit etmek için inversiyon anahtar tekniklerini kullanmışlardır. Bu metot, yükselen kenarı da kilitlemiştir. Fakat bu düzeltici, örnek slotu üreten satır frekansının birkaç katında çalışan bir sistem clock'una sahipti. Bu örnek, aktif videonun başlangıç kısmından alınmaktaydı.

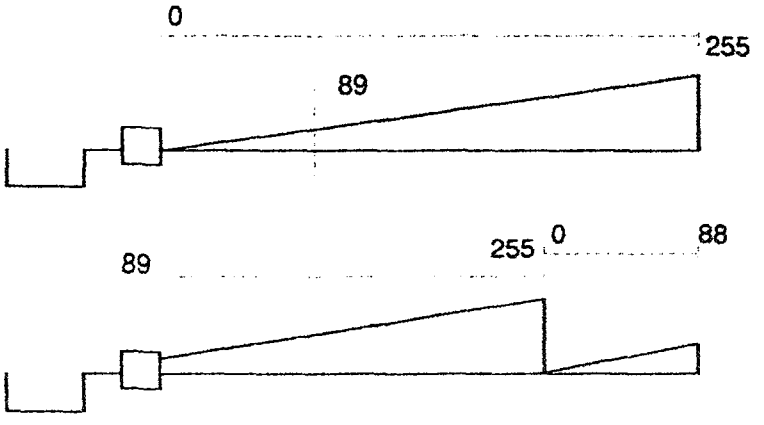
Sonuç olarak, bu sistemi gerçekten hack etmenin tek yolu mikrokontrolör bazlı bir düzeltici kullanmaktı. Teleclub'ın PayView sistemini kullanmayı bırakmasına yakın, mikrokontrolör bazlı kod çözücüler artık bir standart haline gelmişti. Bu yüzden terfi işlemi sadece, düzelticinin EPROM'unda bazı değişiklikler yapmaktan ibaret hale gelmiştir.

2.6.9 VideoCrypt sistemi

VideoCrypt sisteminin kullanmış olduğu video karıştırıcı yöntem, satırı kesme ve yer değiştirmedir [1]. Ses karıştırıcı yöntemi ise spektrum inversiyonudur. Bu sistem Sky Channel, The Adult Channel ve JSTV tarafından kullanılmıştır.

VideoCrypt sistemi, sadece videoyu karıştırmaktadır. Bu sistemde her bir video satırı, olası 256 kesme noktasından birinde kesilmektedir (Şekil 2.41). Daha sonra video bilgisinin, bu kesme noktasının etrafında yerleri değiştirilmektedir. PAL standartlı televizyon sisteminde 625 satır vardır [1]. Fakat bunun sadece yaklaşık 585 satırı video için kullanılmaktadır. Geriye kalan satırlar, test sinyalleri ve teletekst gibi video olmayan bilgiler için kullanılmaktadır. Yani bu sistemde, sadece 585 satırın karıştırılması gerekmektedir.

Her bir satırdaki kesme noktası bir bayt veya sekiz bit sözcük ile tanımlanabilmektedir. Kesme noktalarının gerçek sırası yalancı rasgeledir. Bu sıra, bir yalancı rasgele sayı üretecinden elde edilmektedir. Bu mikroçip, eğer sıra yeterince uzun çalışmaya bırakılınca tekrarlanacak bir sayı dizisi üretmektedir. Bu dizideki başlangıç noktası, havadan iletilmiş olan bir çekirdek tarafından belirlenmektedir. Bu çekirdek, her 2.5 saniyede bir değişmektedir.



Şekil 2.41 Kes ve yer değiştir tekniği ile video satırlarının karıştırılması [1]

Anahtarları ve havadan iletilen adresleme verilerini korumak için kullanılmış olan kodlama metodları, bu güne kadar mevcut olan sistemler arasında en ileri seviyede olanlardan bazılarıydı. Bu sistem, akıllı kartın doğruluğunu kanıtlamak için Fiat-Shamir Zero Knowledge Test'i kullanılmıştır [1]. Eski kod çözücülerdeki akıllı kart mikrokontrolör arabirimi programındaki bir hata, sistemin en etkili biçimde kullanılamayacağı anlamına gelmekteydi.

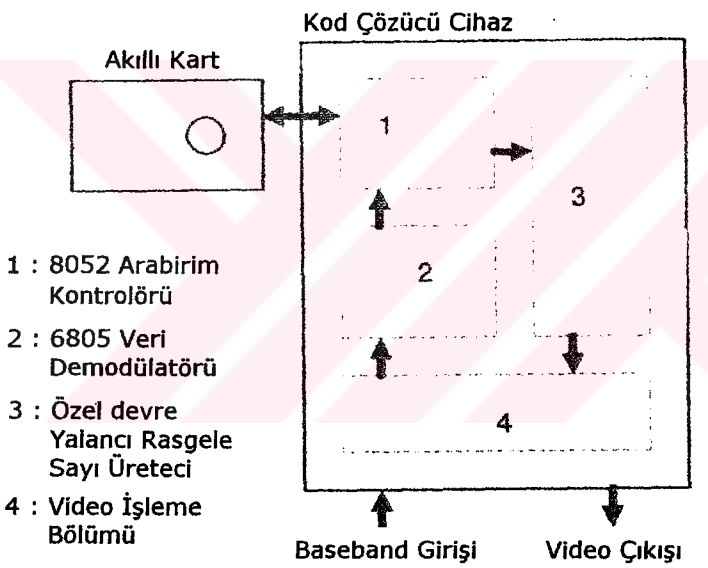
Kod çözücü, bir akıllı kart tarafından kontrol edilmektedir (Şekil 2.42). Her bir akıllı kartın kullanım peryodu en fazla üç ay olmalıdır [1]. Fakat Sky Channel, akıllı kartların dağıtım masrafı yüzünden, genellikle her bir kartın dağıtım süresini iki yıla uzatarak her bir kartı olabildiğince uzun bir süre kullanmaya çalışmıştır.

Akıllı kart, içine yerleştirilmiş olan bir devre yapısına sahip olduğu için ATM kartlarından farklıdır. ATM kartı, veriyi arkasındaki manyetik şeritte depolar. Akıllı kartlardaki bu içine yerleştirilmiş devre yapısı ise, çekirdeklerin ve havadan iletilen diğer verilerin kodunu çözmek için anahtarları depolamaktadır [1].

VideoCrypt sistemi, Thomson isimli bir Fransız şirketi tarafından geliştirilmiştir [1]. Bu sistem, dijital televizyon teknolojisini kullanmış olan en modern karıştırıcı sistemlerden biridir. Piyasadaki dijital olmayan karıştırıcı sistemlerin büyük bir kısmının eksikliği, videodaki senkronizasyon darbelerini etkilemeleridir [1].

VideoCrypt sistemi D-MAC sistemi ile kıyaslanınca teknolojisini yetersiz kalmaktadır. Çünkü D-MAC video karıştırıcı sistemi, çift kesme ve ters çevirme metodu kullanmaktadır [1]. Bu karıştırıcı sistem, krominansı (renkliliği) ve parlaklığı ayrı ayrı kesmekte ve ters çevirmektedir. Bu durum, D-MAC video karıştırıcı sisteminin VideoCrypt sisteminin iki katı güvenli olduğu anlamına gelmektedir.

Avrupa'daki teknik medya, VideoCrypt sisteminin güvenliğini inceleyen makaleler yayınlamıştı. Bu teknik medyada çıkan bazı makaleler, Avrupa'daki uydu iletişiminde sinyal güvenliği konusunda bilgili kişiler tarafından yazılmıştı ve bu kişiler VideoCrypt sisteminin hack edilebilir olduğunu belirtmişlerdi. Bu durum, Bölüm 6 ve Bölüm 7'de detaylı bir şekilde incelenmiştir. Bu sistemde gerçekleştirilmiş olan hack işlemleri; Versiyon 2 olarak tasarlanmış olan McCormac Hack işlemi, yazma voltajını sınırlayan hack işlemi, KENtucky Fried Chip Hack işlemi, Ho Lee Fook Hack işlemi, Phoenix Hack işlemi, 09 Ho Lee Fook Hack işlemi ve 10 Battery Card hack işlemidir [1].

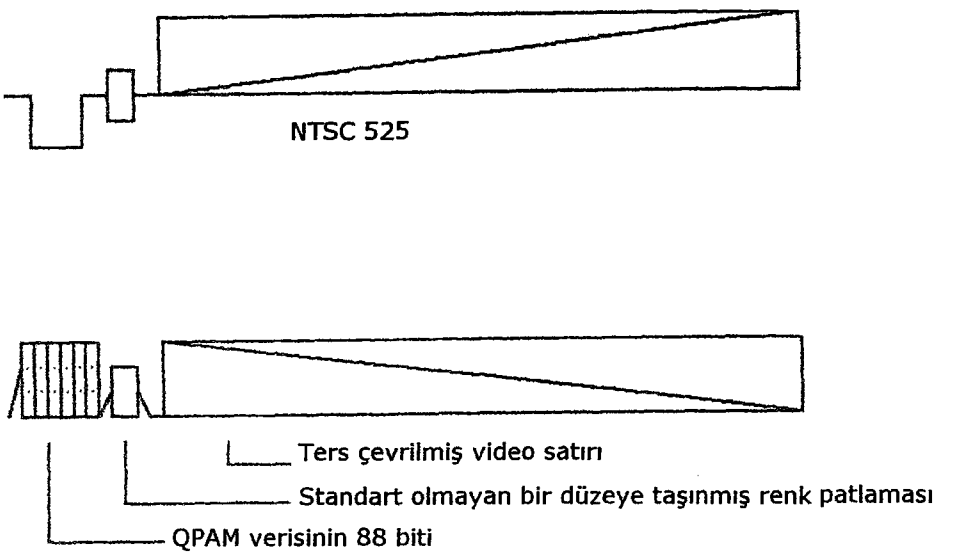


Şekil 2.42 VideoCrypt kod çözücüsünün blok diyagramı [1]

2.6.10 VideoCipher-II sistemi

VideoCipher II sisteminde kullanılmış olan video karıştırıcı yöntemleri yatay ve düşey senkronizasyon yenileme ve video inversiyonudur. Bu sistemde, yatay ve düşey senkronizasyon darbeleri çıkartılmış ve dijital veri ile yenilenmiştir [1]. Video ise ters çevrilmiştir (Şekil 2.43). Renk patlaması, standart olmayan bir voltaj düzeyine taşınmıştır. Bunun kullanılmasındaki başlıca sebep, renk patlamasını kullanarak videoyu kilitleyen bazı televizyon alıcılarını durdurmaktır [1].

Bu sistemde kullanılmış olan ses karıştırıcı yöntem ise DES ile kodlanmış olan dijital ses tekniğidir. Dijital ses, 14 bitlik paketler halinde iletilmiştir. Veriyi iletmek için dört düzeyli darbe genlik modülasyonu (Quad Level Pulse Amplitude Modulation) kullanılmıştır [1].



Şekil 2.43 VideoCipher-II sisteminde satır inversiyonu [1]

VideoCipher-II sistemi, belkide sinyal güvenliği tarihindeki en önemli karıştırıcı sistemdir. İlk denemesinde, video karıştırıcı için facto sistem olarak kabul edilen bir sisteme sahip olmayı hedeflemiştir. Kritik verinin kod çözücünün içinde tamamen korumasız olarak bırakılmasının dışında iyi bir karıştırıcı sistemdir. Seksenli senelerin başlarındaki teknolojiyi baz almıştır. Fakat, güvenlik yapısını iyileştirmek için hızla terfi edilmiş ve değişikliklere uğramıştır [1].

VideoCipher-II sistemi, dijitalleştirilmiş sese sıkı dijital kodlama teknikleri uygulamıştır. Daha sonra, kodlanmış olan dijital ses senkronizasyonun yerine video satırına sokulmuştur. VideoCipher-I sistemi, videoya ve ses dijital kodlama uygulamıştır. Fakat sadece stüdyolar ve şirketler arası video bağlantıları için kullanılmıştır [1]. Bu sistem, VideoCipher-II sisteminin hizmet vermek istediği geniş kitle için mali açıdan uygulanabilir bir özelliğe sahip değildir.

Veriyi kodlamak için kullanılmış olan dijital kodlama tekniği, DES algoritmasıdır. VideoCipher-II sisteminin kontrollü erişim kısmı, anahtarları ve program özelliklerini kodlamak için DES algoritması kullanmaktadır [1]. Aylık anahtar, her bir kod çözücünün kendisine özel olan anahtarıyla kodlanmıştır. Eğer abone, aylık ödemesini yapmamışsa, kod çözücünün yetkisini kaldırarak kullanım dışı bırakmak çok kolaydır. Kodlanmış olan aylık anahtarın iletimi, kod çözücünün kendisine özel olan anahtarı ile şifrelenmiş bir aylık anahtar içermemektedir. Her bir kod çözücüde, kendisine özel birkaç anahtar mevcuttur. Kod çözücü

tarafından bu aylık anahtarın kodu çözülmekte ve program özelliklerinin kodunu çözmek için kullanılmaktadır. Eğer kod çözücüye program için yetki verilmişse düzeltilmiş sinyali gösterebilmektedir. Fakat bu sistemin birkaç tehlikeli kusuru vardır ve bu kusurlar, korsanlığa yol açmıştır.

Her bir kod çözücü için yetki verici veri paketi, ayrı ayrı adreslenmektedir. Bu, kod çözücülerin kendisine özgü anahtarları veya adresi ile veri paketini kodlayarak elde edilmektedir. Bu anahtarın, birkaç alternatifiyle birlikte kod çözücünün içinde bulunduğu düşünülmektedir. Yetki verici bu veri paketi, 56 bitlik bir sıra maskesi (tier mask), bir servis kimlik bilgisi ve verilen servis kimlik bilgisi için bir aylık anahtar içermektedir. Sıra maskesi, bu servis tarafından mevcut olan olası 56 paketin bir veya daha fazlasına erişime izni vermektedir [1]. Her bir televizyon programı, benzer bir 56 bitlik sıra maskesiyle iletilmektedir. Bu sıra maskesi kod çözücüye hangi pakete ait olduğunu belirtmektedir. Eğer programın sıra maskesi, kod çözücünün içindekiyle uyuyorsa kod çözücü artık düzeltme işlemini yapabilecektir. Bu sistemde gerçekleştirilmiş olan hack işlemlerinden aşağıda bahsedilmiştir:

1) Musketeer Hack işlemi

Kontrol rutinleri EPROM'un içinde tutulmaktadır. Bu rutinler birbirinden ayrılmıştır ve analiz edilmiştir. VideoCipher-II sisteminde gerçekleşen en basit hack işlemi, sadece EPROM'daki rutinlerin değiştirilmesini gerektirmekteydi [1]. Bu hack işlemi, kullanıcının bir kanal için abone olarak bütün kanalları izleyebilmesine olanak tanımaktaydı. Değiştirilmiş rutinleriyle bu EPROM'lar Musketeer mikroçipleri olarak bilinmektedir. Bu hack işleminin esas aldığı mantık mükemmeldir.

Kod çözücü, bir sıra maskesine sahiptir. Bu, her bir kanal için bir bitin tutulduğu birkaç yazmaç (register) olarak ta düşünülebilir. Eğer kod çözücüye bir kanal için yetki verilmişse register yüksek olacak ve kod çözücü devre yapısına sinyali düzeltmesi için izin verilecektir. Eğer bu bit düşük ise, o zaman kod çözme işlemine engel olunacaktır.

Bu sistemdeki zayıf nokta, aylık anahtara sahip olunduğu zaman başka hiçbir şeyin gerekli olmamasıdır. U30'daki program EPROM'un üzerine yazıldığı için sıra maskesi görmezden gelinmiştir. Sıra maskesi kontrolü olmadığından dolayı bütün sıralar geçerliydi ve kod çözücü bu servisteki bütün kanalları düzeltebilmekteydi [1].

Doğal olarak televizyon kanalı bu hack işlemine karşı tedbir alabilirdi. Havadan bazı bilgiler ileterek programın sıra maskesi ile kod çözücününkini karşılaştıran güvenli bir işlemci

hazırlamak mümkündü. Böylece eğer sıra maskeleri birbirine uymazsa o zaman kod çözücü durdurulabilecekti.

2) Preview Bit Hack işlemi

Bu sistemdeki diğer bir hack işlemi, sıra maskesindeki preview (özel gösterim) bitini kullanmaktır. Televizyon kanalları bazen, kod çözücü kullanıcılarına ne kaçırdıklarını göstermek için kısa bir süre yayını izlemelerine izin vermektedir. Bu preview biti kod çözücüye sinyali düzeltmesi için birkaç dakikalığına izin vermektedir. Genellikle ses çözülmekte, görüntü karartılmakta ve bir uyarı mesajı gösterilmekteydi. Videoyu düzeltmek için basit bir video kod çözücüsü kullanarak ve sesi düzeltmek için VideoCipher-II kod çözücüsü kullanılarak açık bir televizyon yayını elde etmek mümkündü [1]. Fakat televizyon kanalı bunu fark edince bu zayıf nokta düzeltildi.

3) Clone Hack işlemi

Bu, VideoCipher-II sistemindeki en basit hack işlemidir. Kod çözücü adresi ve anahtar grubu orijinal bir kod çözücüden elde edilir ve diğer bir VideoCipher kod çözücüsüne bunlar yüklenir. Orijinal kod çözücü, yetkili kılınmış olarak kaldığı süre boyunca klonlanmış olan bu kod çözücülerin tamamı çok iyi çalışmaktadır [1]. Televizyon kanalı, klonlanmış bir orijinal kod çözücü tespit ettiği zaman bunu iptal ederek bir seferde yüzlerce klon kod çözücüyü kullanım dışı bırakabilmektedir. Bazı klon hack etme işlemleri, sadece batarya destekli RAM'lere anahtar grubunun yazılmasından ibaretti. Bu, orijinal anahtar grubu ve adresini güvenli işlemcinin (TMS7000) içinde bırakmaktaydı. Televizyon kanalının buna karşı almış olduğu tedbirlerden biri, grupların aynı olup olmadığını kontrol etmekti [1].

4) Wizard Hack işlemi

VideoCipher-II sisteminde gerçekleştirilmiş olan en mükemmel hack işlemidir [1]. Korsan düzelticiye aylık anahtarın bir tuş takımı ile girilmesine izin vermiştir. Bu aylık anahtarlar, ilgili internet sitelerinde ve BBS'lerde mevcuttur.

3. DÜZELTİCİLERİN YAPI BLOKLARI

Seksenli yıllardaki karıştırıcı sistemlerin büyük bir bölümü, kısmen dijital teknikler kullanan analog sistemlerdir [1]. Doksanlı yılların sistemleri ise dijital teknolojiye daha fazla bağımlı hale gelmiştir. Bunun bir sonucu olarak, hack etme işlemlerinin büyük bir kısmı orijinal kod çözücüleri korsan bir biçimde çalıştırmaya dayalı hale gelmiştir. Genellikle bu durum, orijinal akıllı karttaki kodlamada değişiklik yapmak veya bir korsan akıllı kart geliştirmek veya bir kart emülatörü programı oluşturmak anlamına gelmektedir.

Fakat tamamen analog olan tekniklerden bu uzaklaşma, analog tekniklerin tamamen işe yaramaz olduğu anlamına gelmemektedir. Günümüzde, kullanımda olan bir çok analog sistem vardır. Fakat analog sistemleri hack etme teknikleri korsanlar tarafından bilindiği için, bu analog sistemlerin de güvenli kalma şansı yoktur [1].

Korsan kod çözücü endüstrisinin son birkaç yıl içinde göstermiş olduğu gelişme, dijital televizyon sistemlerinin gelecekteki durumunun pek parlak olmadığına işaret etmektedir. Analog ve dijital sistemlerin her ikisi de piyasada mevcuttur. Analog sistemler, bilgisayar korsanları için kolay hedeftir ve bu sistemleri hack ederken büyük bir problemle karşılaşılmamaktadır [1]. Analog teknikleri kullanmakta olan televizyon kanallarının yapmış olduğu bir sonraki hamle, dijital sistem kullanan bir servis olma girişimleridir. Bu servislerin en kayda değeri olan FilmNet, kullanmış olduğu SATPAC sistemine dijital bir ses karıştırıcı ilave etmiştir [1].

Bundan sonraki diğer aşama D2-MAC EuroCrypt sistemine geçilmesidir [1]. Bu sistemin standardının (D2-MAC) arkasındaki teknoloji ve tasarımlar o zaman için gerçekten iyiydi. Bu durum, PAL standardından daha sağlam ve daha kullanışlı bir standarda yönelmeyi işaret etmektedir.

Korsan kod çözücü endüstrisinde, hızlı yol ve yavaş yol konumu olmak üzere iki yol (track) bulunmaktaydı. Uydu sistemlerinin büyük bir kısmı hızlı yol konumu ile temsil edilmektedir. Bir transponder, coğrafi olarak geniş bir alanı kapsayabildiği için uyduda kullanılan bir sistemde gerçekleşen bir hack işlemi, geniş bir uygulama alanına sahip olmakta ve televizyon kanalına çok fazla zarar vermekteydi [1].

Düşük ücretli kanallar ve kablolu sistemler, yavaş yol konumu ile temsil edilmektedir. Bu kanallar ve operatörler, kullandıkları karıştırıcı sistemin güvenliğinden özel bir biçimde kaygı duymuyorlardı. Kablolu sistem operatörleri, sistemlerinin geniş çaplı bir korsanlıktan muaf olduğunu düşünmekteydi. Bu yüzden kolayca hack edilebilen eski sistemlerin büyük bir

kısmının, uzun zaman önce uydu kanalları tarafından kullanımının bırakılmasına rağmen kablolu sistemler tarafından hala kullanılmaktadır [1].

Eski analog karıştırıcı sistemlerin sadece birkaç tanesi hala kullanımdadır. Avrupa'da küçük çaplı kablolu sistemlerin hızla artmasıyla, ucuz bir tercih olduğu için eski ve az güvenli karıştırıcı sistemler tercih edilmektedir. Bunun sonucunda, bu bölümde bahsedilmiş olan temel yapı bloklarının büyük bir kısmı bu eski versiyon karıştırıcı sistemler için geçerliliğini korumaktadır.

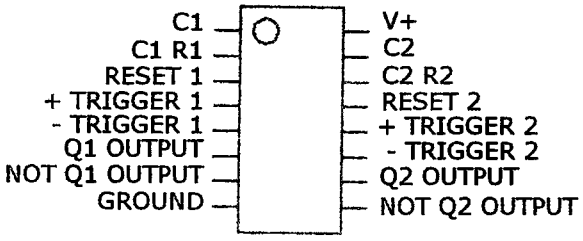
Bu bölümde incelenmiş olan devreler, bilgisayar korsanları tarafından hack işlemlerinde en yaygın olarak kullanılmış olan devrelerdir. CMOS devre yapısı, tamamen gürültüden muaf olduğu için neredeyse alternatifsiz olarak kullanılmaktadır. Alıcılar (receiver), çoğu ASTRA alıcısında olduğu gibi mikroişlemci kontrollü olduğu zaman bu devreye sahip olmak büyük bir avantajdır [1]. TTL devre yapısı, çok güç harcadığı için kullanılmamaktadır. Kristal kontrollü osilatörler için düşük güçlü, hızlı TTL kullanımına ise artarak devam eden bir yönelme vardır.

3.1 Tekkararlılar

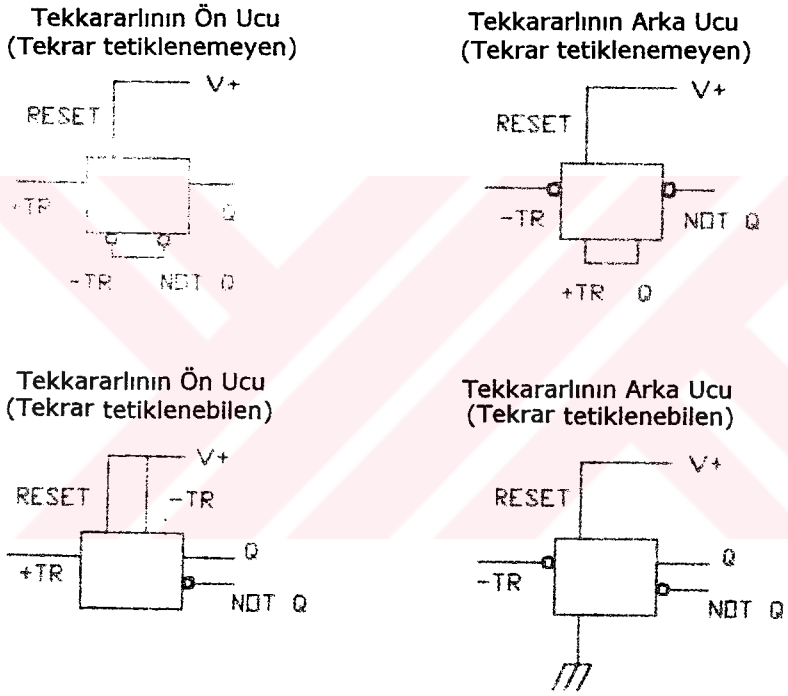
Basit analog karıştırıcı sistemlerin büyük bir kısmında görüntü, video sinyalinin senkronizasyon kısmı ile engellenir. Bu yüzden, bilgisayar korsanlarının senkronizasyon darbelerini yeniden üretmeleri gereklidir. Bu çalışma tarzı için birden fazla kullanım alanı olan devre tekkararlı (monostable) multivibratördür. NE555 mikroçipi iyi bir seçim olarak görünse de aslında değildir. Çünkü bu tekkararlı, bir tasarımcıya veya bilgisayar korsanına kapılanmış tekkararlı multivibratördeki özelliklerin aynısını sunmamaktadır [1].

Zamanlama bazlı karıştırıcı tasarımlarını hack etmek için en çok kullanılan devre, kapılanmış tekkararlı multivibratördür. Bilgisayar korsanları bu devrenin çoğunlukla üç versiyonunu kullanmaktadır. Bunlar; 4098, 4528 ve 4538 tekkararlı entegre devreleridir (Şekil 3.1). Bunların içinde en hassas versiyon 4538 mikroçipidir ve düşük maliyetli düzelticilerde çok nadir olarak kullanılmıştır [1]. Her bir entegre devre iki adet tekkararlı içermektedir. Her bir tekkararlının zamanlama sabiti bir RC düzeni ile ayarlanmaktadır. Her bir tekkararlı, ön ucundan veya arka ucundan tetiklenmiş olabilir (Şekil 3.1). Her bir tekkararlının, Q ve NOT Q olmak üzere iki çıkışı vardır. Zamanlama sabitleri için formül, 4098 ve 4528 mikroçipleri için T=0.5(RC) ve 4538 mikroçipi için T=0.7(RC) 'dir. Gümüş mika veya polistiren kondansatörler ve metal film dirençler gibi hassasiyet bileşenleri tavsiye edilmektedir. Eğer

hassasiyet dirençleri piyasadan temin edilemiyorsa karbon film-preset (ön ayar) kombinasyonunun kullanılması gereklidir. Bu devreler, korsan analog düzelticilerin temel devreleridir. Zamanlama sabitlerini ayarlamak için seramik kondansatörlerin kesinlikle kullanılmaması gerekir. Çünkü bu kondansatörler, ciddi senkronizasyon problemlerine yol açma eğilimindedir [1].



4098, 4528 ve 4538 Tekkararlı entegre devrelerinin bacak bağlantıları



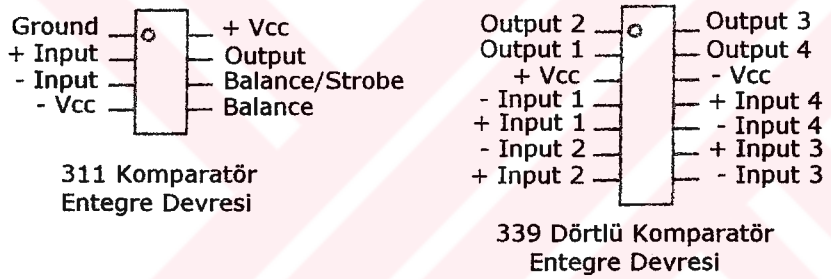
Şekil 3.1 Tekkararlı entegre devresinin bacak bağlantıları ve tetiklenme biçimleri [1]

Analog düzeltici tasarımlarındaki en yeni yaklaşım, tekkararlıdan türetilmiş pencereden (window) ziyade clock'tan türetilmiş pencere kullanımıydı. Clock osilatörü genellikle 2.0 MHz'de veya bu frekansın üzerinde çalışmaktadır ve bu pencereyi türetmek için bazı dizisel ve kombinasyonel lojik kullanılmıştır. Bununla beraber, bu gibi tasarımlar seri imalat bantları için hazırlanmıştır. Tekkararlılar, incelenecek olan satır alanını seçmek için ayarlanabildiğinden dolayı bir karıştırıcı sistemi hack etmek için yapılan ilk denemelerde yaygın olarak kullanılmıştır [1]. Genellikle geliştirme aşaması tamamlandıktan sonra bu

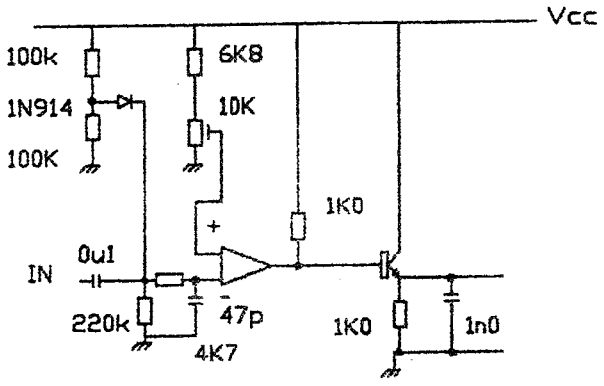
tasarım, seri üretimi daha kolay olan clock bazlı bir biçime dönüştürülmektedir [1].

3.2 Komparatörler

Karıştırıcı sistemlerin büyük bir kısmında belirli bir voltaj düzeyinin bulunması gereklidir. Genellikle bu voltaj düzeyi, bazı zamanlama veya işlem yapma devre yapılarını tetiklemektedir [1]. Voltaj düzeyi video sinyalinin bir parçası olduğu zaman, video sinyali kuvvetlendirilmektedir. Video sinyalini belirli bir referans düzeyi ile karşılaştırmak için 311 komparatör entegre devresi kullanılmıştır. Referans girişindeki ön ayar, çok dönüşlü bir ön ayar direnci ile yapılmaktadır. Ayrıca bu komparatör, darbeleri temizlemek için bir Schmitt Trigger olarak da kullanılmıştır. Bazı durumlarda iki veya daha fazla komparatör gerekmektedir. Bu durumlarda, dörtlü komparatör olan 339 entegre devresi kullanılmaktadır. Bu entegre devre, ikili komparatörlerden daha ucuzdur ve bu yüzden, sadece iki komparatör gereken durumlarda bile bu kullanılmıştır. Bu komparatörlerin her ikisinin de bacak bağlantıları Şekil 3.2'de gösterilmiştir.



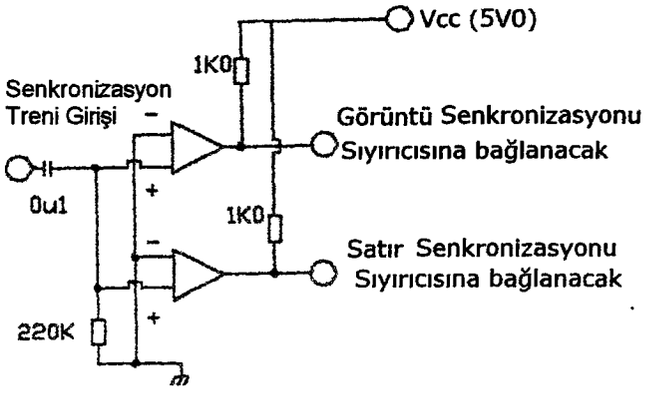
Şekil 3.2 311 ve 339 komparatör entegre devrelerinin bacak bağlantıları [1]



Şekil 3.3 Senkronizasyon sıyırıcı devresi [1]

FilmNet düzelticilerinde komparatörler, senkronizasyon darbesini temizlemek (Şekil 3.4) veya yatay senkronizasyon kullanarak video polaritesini bulmak için kullanılmıştır. Discret sisteminde kullanılmış olan düzelticilerde ise, her bir satırdaki videonun başlangıç noktasının

bulunması için komparatörler kullanılmıştır [1]. Bu durum, siyah düzeyini bir örnekleme devresi ve bir tutucu (hold) devre ile örnekleyerek gerçekleştirilmiştir. Daha sonra örneklenmiş olan bu düzey, video sinyali ile karşılaştırılmıştır [1].



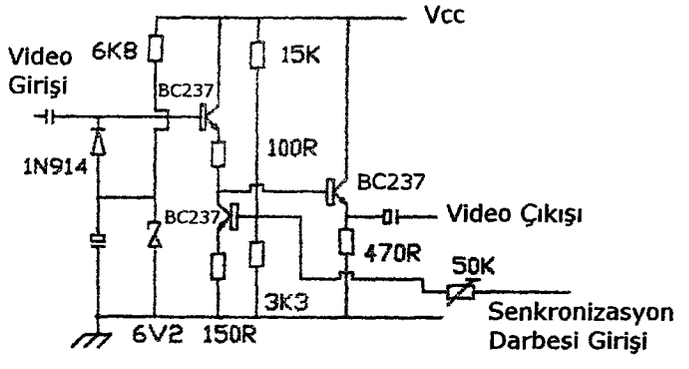
Şekil 3.4 Senkronizasyon darbesi temizleyici [1]

3.3 Senkronizasyon Darbesi Ekleme ve Yenileme

Video sinyalindeki senkronizasyon darbelerinin yeniden eklenmesi veya yenilenmesi için pek çok metot mevcuttur. Bu bölümde verilmiş olan devreler en yaygın olarak kullanılmış olan devrelerdir. LuxCrypt sistemindeki gibi bazı durumlarda, senkronizasyon darbelerinin tamamen yeniden yaratılması gerekmektedir [1].

3.3.1 İki amplifikatör - bir tespit devresi metodu

İki amplifikatör - bir tespit devresi metodu, senkronizasyonu gerçek düzeyine çekmek için kullanılabilmektedir [1]. Fakat bu tür bir devre senkronizasyonu gerçek düzeyine yenilemek için kullanılabilmesine rağmen senkronizasyon darbesini yeniden eklemek için kullanılamaz.



Şekil 3.5 İki amplifikatör - bir tespit devresi ile senkronizasyon darbesi eklenmesi [1]

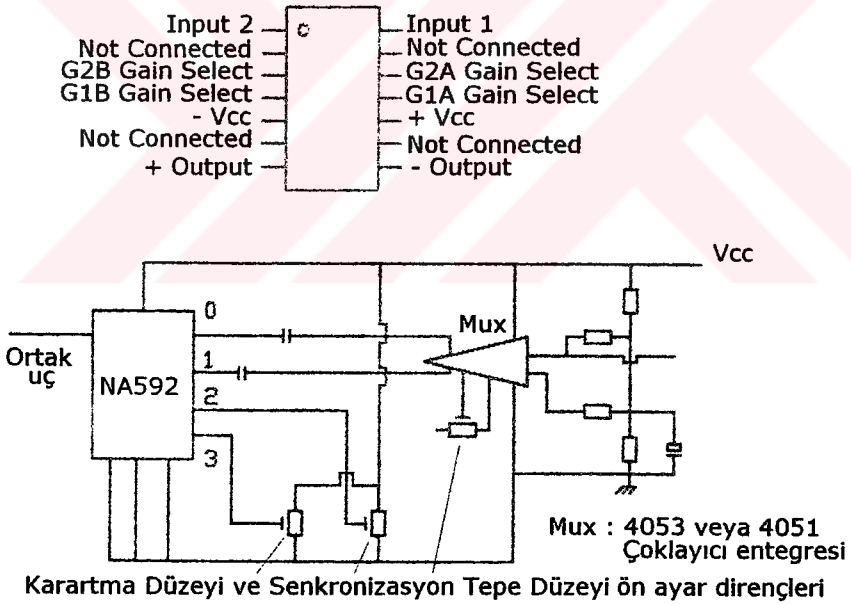
İki amplifikatör - bir tespit devresinin modifiye edilmiş bir benzeri pek çok tecrübeli bilgisayar korsanı tarafından kullanılmıştır. Şekil 3.5'te gösterilmiş olan devre Elektor Electronics isimli dergide yayımlanan devredir [1].

3.3.2 Çoklayıcı metodu

Bu devre, karartma düzeyinin ve senkronizasyon tepe düzeyinin yeniden eklenebilmesini sağlamaktadır. Karatma ve senkronizasyon tepesinin voltaj düzeyleri ön ayar dirençleri ile ayarlanır. Çoklayıcı, videoyu kapatmakta ve senkronizasyonu yenilemek için doğru voltaj düzeylerinde açmaktadır [1].

Bu amaç için en yaygın olarak kullanılmış olan sekiz giriş ve bir çıkışlı 4051 çoklayıcı entegre devresidir. Bunun iki girişine, normal ve ters çevrilmiş video sinyalleri bağlanmıştır. Diğer iki girişine ise siyah düzeyi ve senkronizasyon tepe düzeyleri bağlanmıştır. Bazı harici devre yapıları çoklayıcının adresleme bacaklarını kontrol etmektedir.

Şekil 3.6'da gösterilmiş olan uygulama devresinde, çoklayıcıya normal ve ters çevrilmiş videoyu sağlaması için bir NE592 video amplifikatörü kullanılmıştır.



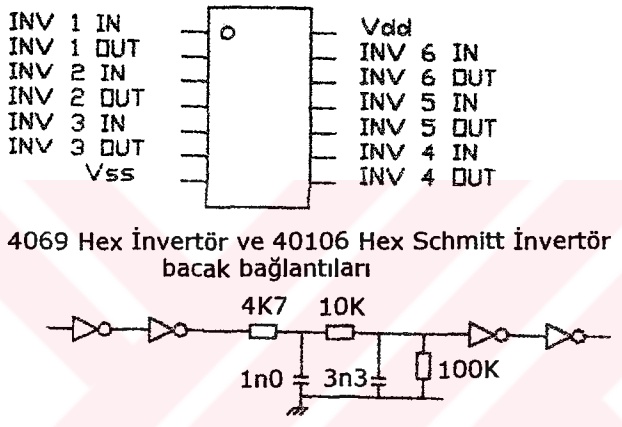
Şekil 3.6 ile Çoklayıcı kullanılarak oluşturulan senkronizasyon darbesi ekleme devresi [1]

Bu devre tipi, polarite anahtarının veya dijital ses bilgisinin karıştırılmış dalga biçiminden ayrılmış olmasını gerektiren uygulamalarda çok kullanışlıdır. Bu devre, çoklayıcının yerine 4066 veya 4016 CMOS anahtarları kullanarak da gerçekleştirilebilir [1].

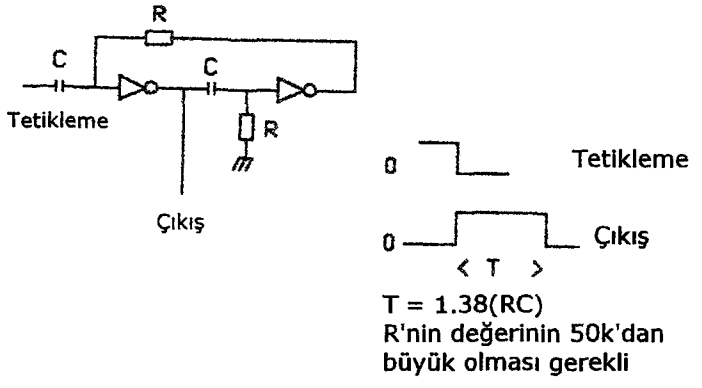
3.4 CMOS Devreleri

3.4.1 CMOS integratör

CMOS devre yapısı, analog uygulamalarda kullanılabilmektedir. Bir CMOS invertörünün bir operasyonel amplifikatör (OPAMP) gibi çalışması sağlanabilir. Bazı uygulamalarda bir integratör devresi gerekmektedir. OPAMP olarak kullanılan CMOS invertörlü tipik bir devre bloğu Şekil 3.7'de gösterilmiştir. Bu özel devre, 7.56 MHz taşıyıcı üzerinde iletilmekte olan senkronizasyon sinyallerinden görüntü darbesini ayırmak için FilmNet kanalının kullanmış olduğu tekkararlılı düzeltici tasarımlarında kullanılmıştır [1]. İkinci kondansatörün uçlarına 100 kΩ'luk bir direncin bağlanması ile integratörün çalışması iyileştirebilir. Verilmiş olan bu değerler kritik değerler değildir.



Şekil 3.7 Senkronizasyon sinyallerinden görüntü darbesini ayıran CMOS integratör [1]



Şekil 3.8 NOR kapıları kullanılarak bir tekkararlının çalışma şeklinin sağlanması [1]

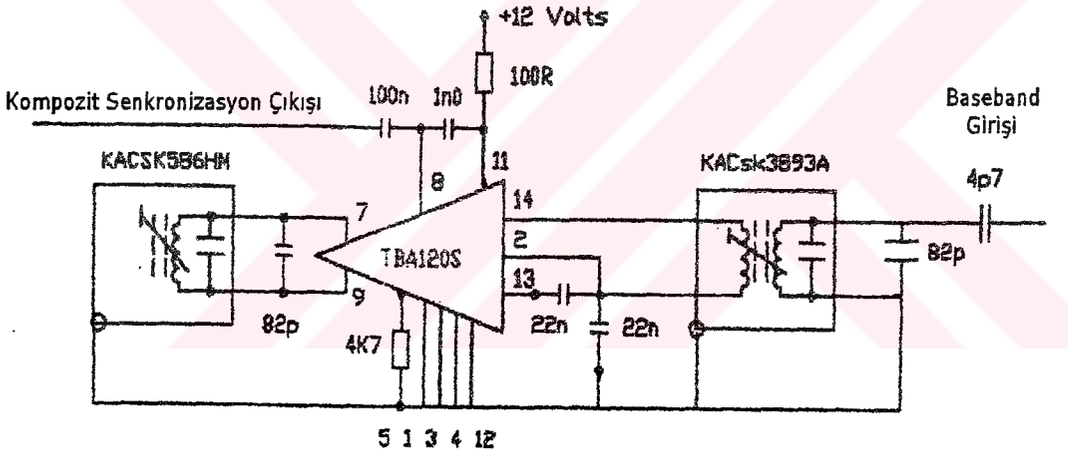
3.4.2 NOR kapıları oluşturulan CMOS tekkararlı

Bilgisayar korsanları, yapmış oldukları düzeltici tasarımlarını ters mühendislikten korumak için çoğunlukla alışılmamış tasarım tekniklerine başvurmaktadır. Bir tekkararlı için en

belirgin tercih 4528 mikroçipi kullanımıdır [1]. Şekil 3.8'de gösterilmiş olan devrede kullanılmış olan NOR kapıları ile bir tekkararlının çalışma şekli sağlanmıştır. Bu devre, hassas zamanlamanın gerekli olmadığı genel uygulamalar için kullanılabilmektedir.

3.5 Kompozit Senkronizasyon Demodülatörleri

Burada, harici senkronizasyon taşıyıcıları için ayrı bir demodülatör gereklidir. Böyle bir demodülatör için pek çok devre mevcuttur. FilmNet SATPAC sistemi, senkronizasyon taşıyıcı bir sistemin iyi bir örneğidir [1]. Korsan düzelticilerin büyük bir kısmı senkronizasyon taşıyıcısının demodülasyonu için TBA120 entegre devresini kullanmıştır [1]. Genellikle, TBA120 entegresinden önce akortlu bir filtre gelmektedir. Bu durum, devre maliyetini arttırmaktadır. Kaliteli korsan düzelticilerin bazılarında 7.56 MHz'lik senkronizasyon taşıyıcı, standart bir 10.7 MHz'lik seramik filtreden geçirilerek 10.7 MHz'e dönüştürülmüştür [1]. Bu tür bir demodülatörü akort etmek, sadece akort ön ayarını (preset) ayarlamaktan ibaret olduğu için daha kolaydır. Bu devre tasarımı Şekil 3.9'da gösterilmiştir.



Şekil 3.9 Kompozit senkronizasyon demodülatörü devre tasarımı [1]

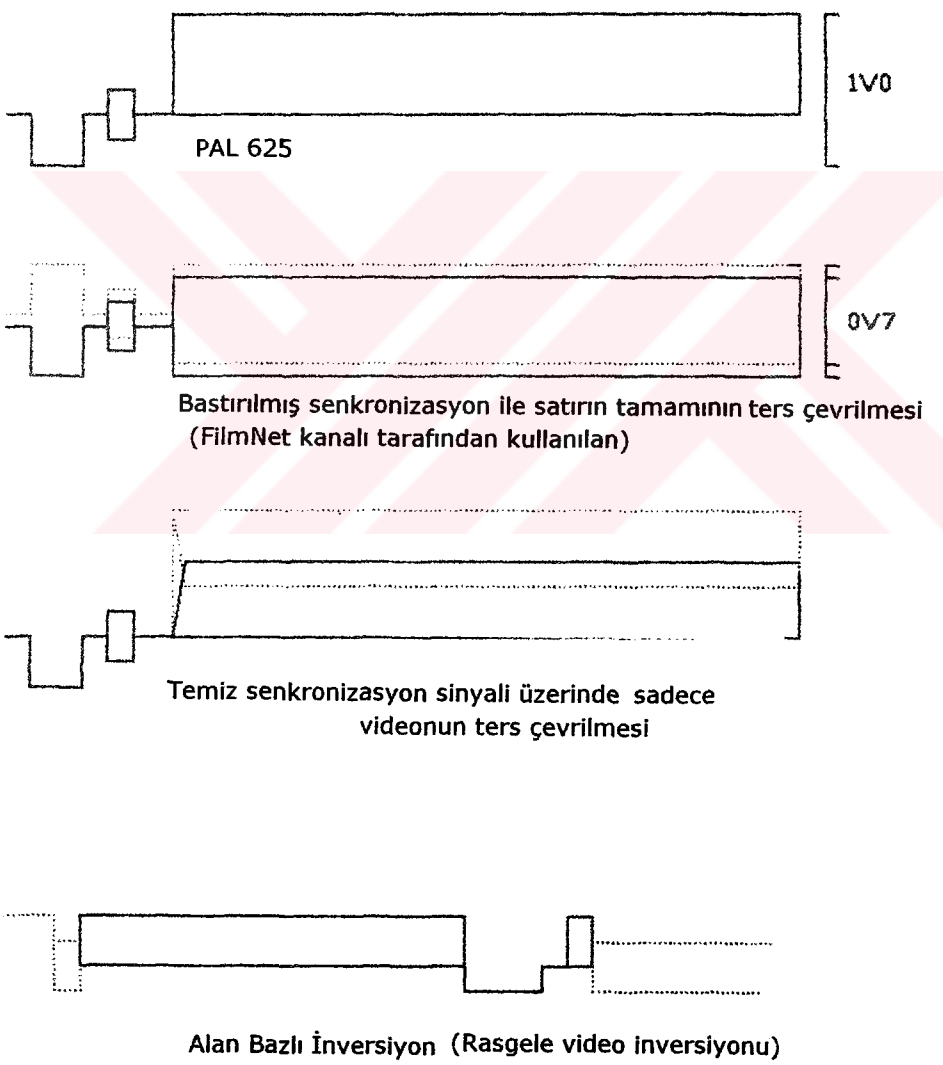
Karıştırıcı frekansı sağlamak için kristal kontrollü bir osilatör kullanımı da bir başka yoldur. Kullanılan frekans genellikle yüksek kenar frekansıdır (18.26 MHz). Hi Tech Xtravision korsan FilmNet düzelticilerinde bu yöntem kullanılmıştır [1].

FilmNet sisteminin kablolu televizyon versiyonunda, frekans modülasyonlu ses alt taşıyıcısındaki senkronizasyon taşıyıcısı modüle edilmiştir. Korsan tasarımların büyük bir kısmı, senkronizasyon sinyallerini bularak ve bir faz kilitlemeli çevrim kullanarak çalışmaktaydı. Bu işlemler, kablolu televizyon kanalları için kod çözücü tasarımında daha iyi sonuç verecektir. Çünkü bazı televizyonlar videoyu kenetlemeye (clamp) yöneldiği için,

modifiye edilmiş bir uydu televizyon kanalı kod çözücüden gelen düzeltilmiş görüntü bunun kablolu televizyon versiyonunda olduğu kadar iyi değildir [1].

3.6 Polarite Bulma

Video inversiyonu, satırın video kısmının ters çevrildiği, fakat satırın yatay karartma kısmının normal polaritede kaldığı durumdur (Şekil 3.10). Video inversiyonu kullanan bir karıştırıcı sistemin hack edilmesi zordur. Fakat, polaritenin doğrusunun bulunmasına izin veren birkaç zayıf noktası vardır. Sistem tasarımcılarının video inversiyonun çok güvenli olduğunu düşünmelerinin sebebi, korsan düzelticilerin büyük bir kısmında mikrokontrolör kullanıldığını hesaba katmamalarıydı [1]. Mikrokontrolörler, bilgisayar korsanlarının video sinyalini örneklemek için doğru zaman slotlarını (yarıklarını) üretmelerine izin vermektedir.



Şekil 3.10 Satır inversiyonu, video inversiyonu ve rasgele video inversiyonu [1]

Rasgele video inversiyonunun üstesinden gelmek için olası bir durum, birkaç satırı dijitalleştirmek ve her bir satırın başındaki ilk birkaç baytı karşılaştırmaktır. Bu, doğru bir sonuç vermek için bir görüntü belleğine ihtiyaç duyabilmektedir. Rasgele satır inversiyonu kullanan sistemlerin bazılarında satırda iletilen bir sinyal, ne tür bir karıştırıcı yöntem beklemeleri gerektiğini orijinal düzelticilere bildirmektedir. Genellikle bu tetikleme sinyali, renk patlamasından sonra ve video bilgisinden önce iletilmektedir. Bu, sistemin güvenliğini zayıflatır ve sistemin hack edilebilmesini kolaylaştırır. Video inversiyonu kullanan sistemlerin büyük bir kısmının 1985 yılından önce tasarlanmış olduğu ve on beş yıl önceki tasarım düşüncelerini yansıttığı unutulmamalıdır.

Ayrıca, ters çevrilmiş satırın sırasını iletmek için düşey karartma aralığı kullanılmıştır. Eğer bu sıra kodlanmazsa, ilerde çok kritik problemler ortaya çıkabilir. Normalde teletekst için kullanılması gereken bir veya birkaç satır, düzeltici bilgisi için boşaltılmıştır. Bir bilgisayar korsanı için böyle bir satırı sıyırmak kolay olacaktı. Osiloskoplar için satır yakalayıcı bir devre, Elektor Electronics dergisinde yayımlanmıştır. Bu devrenin görevi, çeşitli televizyon devrelerinin ve bağlantılarının cevabını analiz etmek için düşey aralık test sinyallerini sıyırmaktır. Bu devre, yakalamış olduğu satıra ön ayar yapabilmekteydi. Bu devreyi, düzeltici verisini yakalamak için değiştirmek aşırı derecede kolaydır [1].

Eski Teleclub korsan düzelticilerinin büyük bir kısmı, her bir alandaki video başlangıç satırlarının siyah düzeylerini kullanılmış olan inversiyon sırasını bulmak için örneklemiştir [1]. Daha sonra bu metot, Teleclub kanalı tarafından video başlangıç satırına yanlış bir sıra dahil edilerek etkisiz hale getirilmiştir.

Sistem operatörünün etkisiz hale getirebileceği en kolay hack yöntemlerinden biri sıra bulma yöntemidir. Korsan düzeltici, bir ön ayar süresinin bir sırasını beklerken bu sıranın herhangi bir varyasyonu geldiğinde düzelticiyi devre dışı bırakmaktadır. Ayrıca, bu satır sırasında gerçekleştirilecek bir değişiklik de korsan düzelticiyi çalışamaz hale getirmektedir. Bu metot Teleclub tarafından korsan izleyicilerin kullanmış olduğu anahtarlanabilir sıra düzelticilerinin çalışmasını engellemek için kullanılmıştır [1]. Bu korsan düzelticilerdeki sıra, bir DIL anahtar kümesi (yığını) kullanılarak kullanıcı tarafından elle (manual) ayarlanmaktaydı. İnversiyon sırasını on saniyelik bir peryot içersinde değiştirilmesi, kullanıcının bu sırayı yeniden ayarlamasını imkansız hale getirmekteydi.

3.6.1 Satır inversiyonu metodu

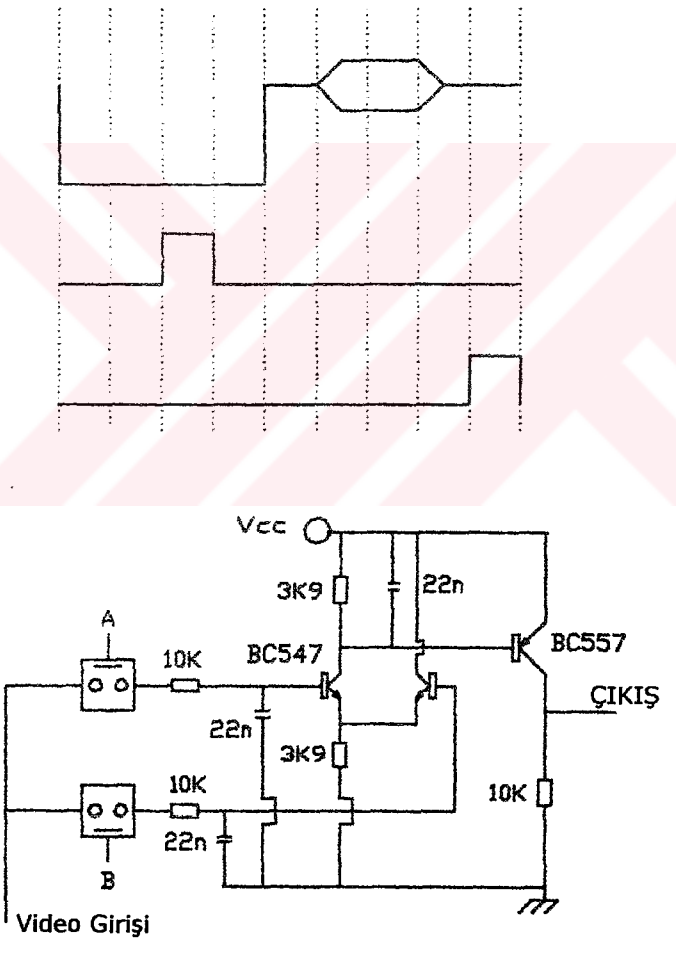
Satır inversiyonu, senkronizasyon bastırma olmaksızın nadiren kullanılmıştır. Satırın tamamı

ters çevrilmiştir. Bu, hack edilebilecek en kolay inversiyon metodudur. Bastırılmış yatay senkronizasyon, polariteyi belirlemek için bir anahtar olarak kullanılabilmektedir.

Bu inversiyon tipi, FilmNet'in karıştırıcı sisteminde kullanılmıştır. Bu nedenle en yaygın analiz edilmiş olan inversiyon tipidir. FilmNet tarafından uygulanan karşı tedbirler oldukça zekiceydi. Fakat tam anlamıyla başarılı olmadıkları için hepsi en geç bir saat içinde hack edilmişti [1].

3.6.2 Anahtarsız bastırılmış senkronizasyon metotları

Anahtarsız (NOKEY) bir sistem orijinal düzelticiye, videonun ters çevrilmiş veya normal olduğunu tanıtan bir anahtara sahip değildir. İnversiyon sırası, bir algoritma ile belirlenmektedir. Genellikle bu tip bir karıştırıcı kullanan sistemler adreslenebilir tiptedir [1].



Eğer A örneği B örneğinden daha büyükse, çıkış yüksek olur. Bu çıkış, bir 4013 Flip-Flop entegre devresini resetlemek için kullanılabilir.

Şekil 3.11 Düzey karşılaştırma ile polarite bulma metodunun devre şeması [1]

3.6.2.1 Düzey karşılaştırma ile polarite bulma metodu

Düzey karşılaştırma ile polarite bulma devresi (Şekil 3.11), yatay senkronizasyon darbe tepesinin bir örneğiyle yatay karartma düzeyinin bir örneğini karşılaştırmaktadır. Bir normal polariteli sinyalde, yatay senkronizasyon darbesinin tepesinin karartma düzeyinden daha düşük olması gereklidir.

Bu devre sadece yatay karartma peryodu süresince aktiftir. Bu devrenin çıkışı, bir flip-flop'u veya bir tekkararlıyı tetiklemek için kullanılmaktadır. Bu flip-flop'un veya tekkararlının çıkışı video çoklayıcısını kontrol eder. Örnekleme noktaları, tekkararlılardan veya sistem clock'undan elde edilebilmektedir. FilmNet düzelticilerinin büyük bir kısmı, clock'tan elde edilmiş slotlar kullanmaktadır.

Bu metot, FilmNet sisteminde kullanılmış olan en yaygın polarite bulma metodudur. Yatay senkronizasyon darbesinde örneğin alındığı noktaya bir darbe yerleştirilerek bu metot yenilgiye uğratılabilmektedir. Clock'tan elde edilen örnek noktalarını kullanmış olan korsan düzelticiler, FilmNet'in gerçekleştirmiş olduğu terfi işleminden en çok zarar görenlerdir. Bu, FilmNet sisteminde kullanılmış olan karşı tedbirlerden biri olmasına rağmen korsan düzelticiler çok kolay terfi edilebildiği için bu sistemin kullanımına son verilmiştir [1].

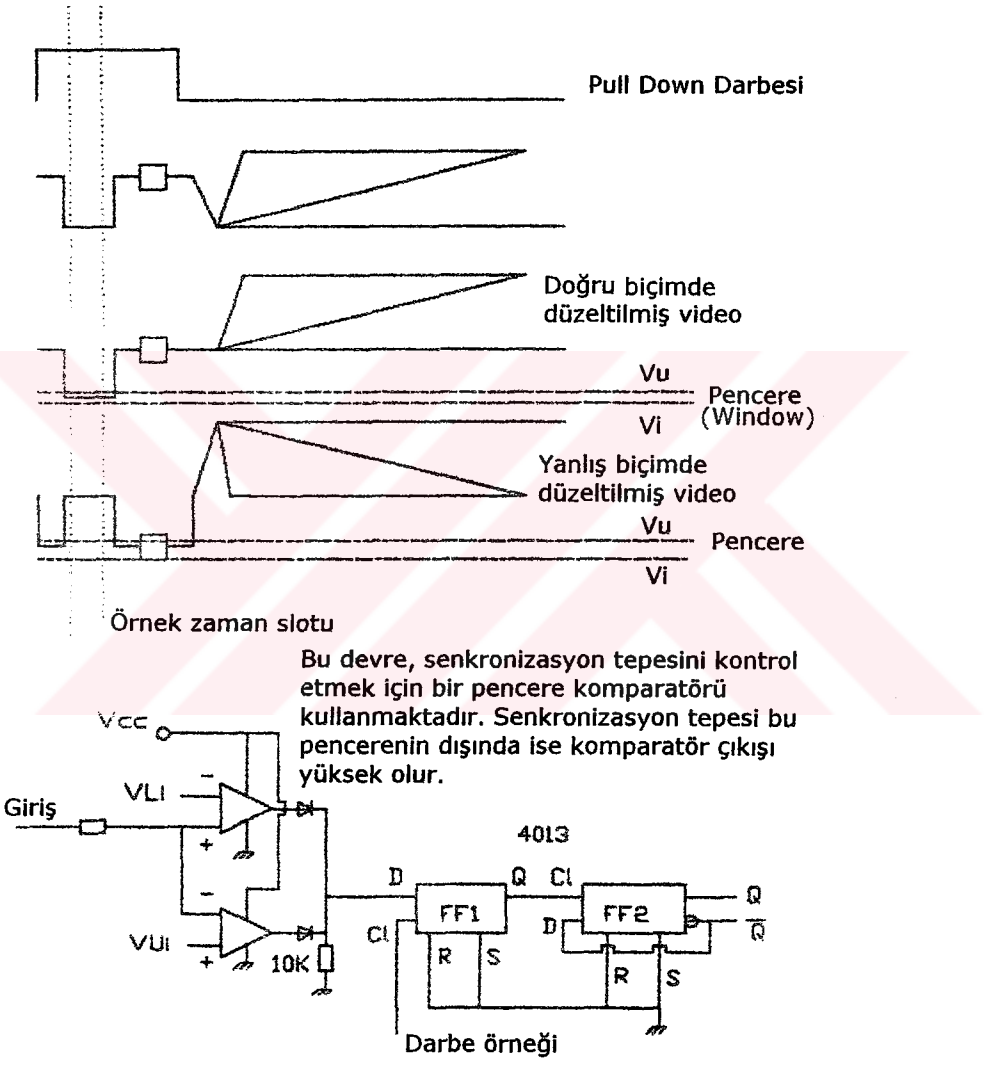
3.6.2.2 Senkronizasyon tepesi bazlı polarite bulma metodu

Uygulanabilecek düzey bulma metotlarının en kolaylarından biri senkronizasyon tepesi bazlı polarite bulmadır (Şekil 3.12). Burada, bulunması gereken sadece bir düzey vardır. Satırın yatay karartma kısmı normal düzeyine çekildikten sonra polarite bulma işlemi gerçekleşir. Eğer polarite doğruysa, o zaman yatay senkronizasyon darbe tepesinin düzeyi kenetleme voltajında veya buna çok yakın olmaktadır. Eğer komparatör, tespit (clamp) voltajından daha büyük bir düzey bulursa, o zaman flip-flop'u başlangıç durumuna getirecektir.

Bu tür bir polarite detektörü ilk defa Pink And Brown Book isimli kitapta, Oak Orion sistemi için korsan düzeltici tasarımında kullanılmıştır (Şekil 3.12). Bu polarite detektörü bu uygulamada, polarite anahtarını bulmak için kullanılmıştır. Hi Tech Xtravision isimli firma bu tür detektör tasarımını korsan FilmNet düzelticilerinde kullanmıştır [1]. Bu tasarım TTL yerine CMOS kullandığından Pink And Brown Book versiyonundan farklıdır. Bu tasarım, polarite bulmadaki en güvenli metot olmasına rağmen televizyon kanalları bu devrenin çalışmasını engelleyecek önlemler alabilmektedir.

FilmNet SATPAC sisteminin 05.11.1990 tarihinde gerçekleştirdiği sistem terfisinin başlıca

amacı, bu tür detektör kullanan korsan düzelticileri çalışmaz hale getirmekti. Bu terfi, yakın renk patlaması frekansının bir sinüs dalgasıydı ve korsan düzelticilerdeki komparatörü şaşırtmaktaydı. Daha sonra gerçekleştirilen bir terfi, sinüs dalgasının düzeyini yaklaşık 1 Hz'lik çok yavaş bir sinüs dalgası kullanarak genlik modülasyonlu duruma getirmişti. Bu terfi, IRDETO sistemi ile benzer özelliklere sahiptir [1]. Bu sistemde dijital ses düzeyi, 15 Hz'lik bir sinüs dalgası kullanılarak genlik modülasyonlu hale getirilebilmektedir. Bu devre, kanallar tarafından alınan karşı tedbirler ile baş edebilmesi için sadece iki komparatör ilave edilerek terfi edilebilen bir yapıdadır.

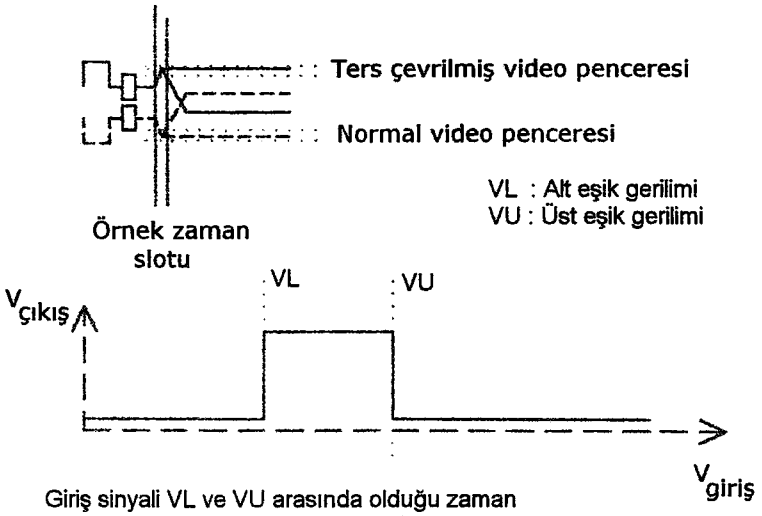


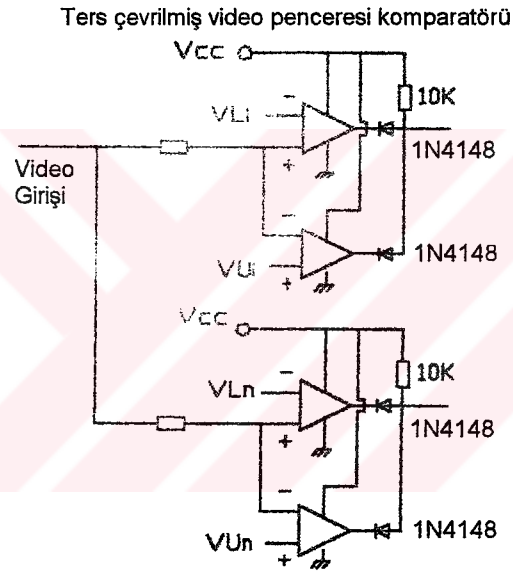
Şekil 3.12 Senkronizasyon tepesi bazlı polarite bulma devresi [1]

3.6.2.3 Enerji konsantrasyonu bulmanın bastırılmış senkronizasyon versiyonu

Bu metot, gerçekleştirilmesi çok zor olan metotlardan biridir. Ayrıca bu, güvenli bir metottur. Her bir satırın video kısmının başlangıcındaki enerji düzeyi örneklenir. Eğer bu düzey, voltaj penceresinin üzerine düşerse video ters çevrilmiştir. Eğer bu düzey, voltaj penceresinin altına

düşerse o zaman video normaldir. Komparatörlerin çıkışları, video çoklayıcısının tekkararlısını veya flip-flop'unu kontrol eden lojik bir devreyi beslemektedir [1].





Şekil 3.13 Enerji konsantrasyonu bulmanın bastırılmış senkronizasyon versiyonu [1]

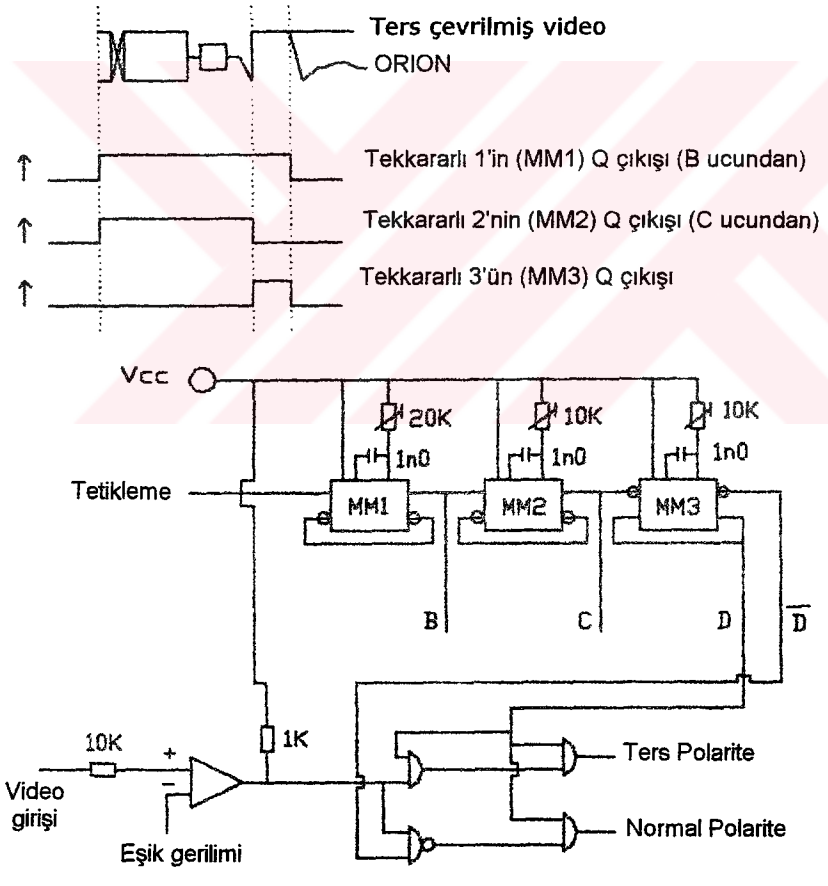
Genellikle bu tür bir metot, 4 MHz bölgesinde bir sistem clock'una ihtiyaç duyar [1]. Bu koşul, mikrokontrolör kontrollü düzelticilerin pek çoğunun sistem clock'unu neden kullandığını açıklamaktadır. Fakat bu durum, daha basit devre yapılarıyla da gerçekleştirilebilmektedir.

Genellikle renk patlaması, normal videoda olduğu gibi karıştırılmış videoda da aynı zaman slotunda kalmaktadır. Bu renk patlaması, referans olarak kullanılmaktadır. Bu referans, 4046 entegre devresinde olduğu gibi bir faz kilitlemeki çevrimi kilitlemek için kullanılmaktadır.

Örnekleme devre yapısını tetiklemek için tekkararlıdan elde edilen veya lojik zamandan elde edilen bir slot kullanılmaktadır. Tercih edilen metot, lojik zamandan elde edilen slottur. Tetiklenmiş bir tekkararlı, uygulamada kullanılırken ustalık ve dikkat gerektirmektedir. Çünkü, zamanlama hassasiyetini elde etmek için bir kondansatör ve bir ön ayar direnci kombinasyonunun kullanılması gerekmektedir. Ayrıca, parçaların eskimesi ve ısınması tekkararlı bileşenlerini etkilemektedir. Bu yüzden slotu değiştirmek kod çözücünün çalışma ömrünü kısaltmaktadır. Faz kilitlemeli çevrimin satır frekansının birkaç katı frekansta çalışması idealdir. 500 ns'lik bir slot için en az 2 MHz'lik bir clock frekansı gerekmektedir [1].

3.6.3 Anahtarlı bastırılmış senkronizasyon metodları

Anahtarlı (KEYED) bir sistem, video polaritesi hakkında orijinal düzelticiye bilgi veren bir anahtara sahiptir. Bu metot, güvenliği çok zayıf olan bir metottur ve LuxCrypt ve Oak Orion sistemlerinin dışında başka hiçbir karıştırıcı sistemde kullanılmamıştır [1].



Şekil 3.14 Anahtardaki video polaritesini bulan bir devre [1]

3.6.3.1 Anahtardaki video polaritesini bulma

Anahtarsız polarite bulma için kullanılan devreler anahtarlı polarite bulma için de kullanılabilmektedir. Bunların arasındaki temel farklılık, örnekleme slotunun zamanlamasındadır. Anahtarların büyük bir kısmı renk patlamasından sonra ve videonun başlangıcından önce yer almaktadır.

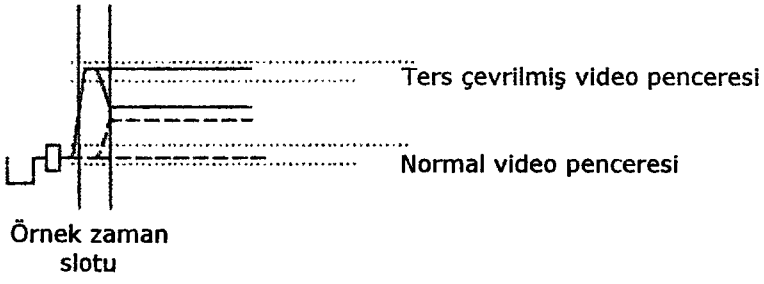
Şekil 3.14'te gösterilmiş olan devredeki MM3 olarak adlandırılmış olan tekkararlı, polarite anahtarı örnek darbesini sağlamaktadır. Buradaki komparatör, anahtar konumunu araştırmaktadır. Lojik kısım ise örnek darbe mevcut olduğu zaman sadece geçerli çıkışlara izin vermektedir. Bu devre için tetikleme, bir PLL'nin satır frekansı çıkışından elde edilmektedir.

3.6.3.2 Temiz senkronizasyon sistemlerinde polarite bulma

Temiz (clean) senkronizasyon sistemlerinde polarite bulma daha zordur. Çünkü bir temiz senkronizasyon sisteminde senkronizasyonlar bastırılmamıştır. Eğer karıştırıcı sistem tasarımcısı gerçekten başarılı bir sistem geliştirmişse, bilgisayar korsanlarının işini çok zorlaşacaktır.

3.6.3.3 Enerji konsantrasyonu bulmanın temiz senkronizasyon versiyonu

Bastırılmış senkronizasyon durumunda kullanılmış olan devre yapısının (Şekil 3.13) aynısı bu uygulamada da kullanılabilmektedir (Şekil 3.15). Zamanlama referansı, yatay senkronizasyon darbesi veya renk patlaması olabilmektedir. Zamanlama referansı olarak renk patlamasının kullanımı daha güvenlidir. Yatay senkronizasyon darbesi Teleclub kanalı tarafından kullanılmış olan PayView III karıştırıcı sisteminde olduğu gibi kararsız hale getirilebilir [1].



Şekil 3.15 Enerji konsantrasyonu bulmanın temiz senkronizasyon versiyonu [1]

3.7 Video Satırlarının Geciktirilmesi ve Yalancı Satır Gecikmesi

3.7.1 Video satırlarının geciktirilmesi

Bir satırdaki videoda satır bazlı gecikme, Discret sistemlerinin esas aldıkları metottur. Video satırlarını geciktirmek için kullanılmış olan birkaç metot vardır. Discret-I düzelticileri, video satırlarını geciktirmek için yüklü akuple aygıt (CCD: Charged Coupled Device) kullanmıştır. Sonraki PAL-SECAM Discret sistemi, video satırlarını geciktirmek için dijital teknikler kullanmıştır [1].

Bu sistemde 0 ns, 902 ns ve 1804 ns'lik gecikmeler kullanılmıştır. Discret sistemini hack eden korsanlar, bu sistemi hack etmek için gerekli olan iki gecikmeyi yaratmak için bir TBA4560 geçici renk geliştirici (colour transient improver) entegre devresi kullanmışlardır [1].

TDA4560 entegre devresi, 888 ns'lik bir gecikme üreten bir jiratör geciktirme satırı içermektedir. Bazı durumlarda bunun yerine TDA4565 entegre devresi kullanılmaktadır. RAI kanalının ve bir çok küçük çaplı kablolu televizyon kanalının kullanılmış olduğu düzelticilerin büyük bir kısmında bu entegre devre kullanılmıştır [1].

TDA4565 entegre devresindeki jiratör geciktirme satırı, herhangi bir bozulma olmaksızın 5.5 MHz'e kadar sinyallerle başa çıkabilmektedir. Fakat bu entegre devre, video sinyalinde 6 dB'lik kayba neden olmaktadır. Yani çıkışta video sinyalinin 6 dB kuvvetlendirilmesi gerekmektedir. Radio Plans tasarımı düzelticide bu kuvvetlendirme işlemi, bir TBA970 entegre devresi kullanılarak gerçekleştirilmiştir [1]. Ayrıca, bu kuvvetlendirme işi için NE592 entegre devresi de kullanılabilmektedir. Fakat bu entegre devre, siyah düzeyi kenetlemesi gerektirmektedir. Gecikme satırlarının yapımında başka çalışmalar da yapılmıştır. Bu çalışmalar, bir İtalyan firması tarafından üretilmiş olan cam gecikme satırları ve kömürlü indüktör kondansatör gecikme satırlarıdır.

Video gecikmesinin dijital bir yaklaşımı orijinal düzelticiler tarafından kullanılmıştır. Bu dijital yaklaşımda, renk patlaması frekansının dört katı bir örnekleme frekansı (17.735 MHz) kullanılmıştır. Bunun sonucunda, düzeltilmiş görüntüde daha belirgin görüntü netliği elde edilmiştir [1].

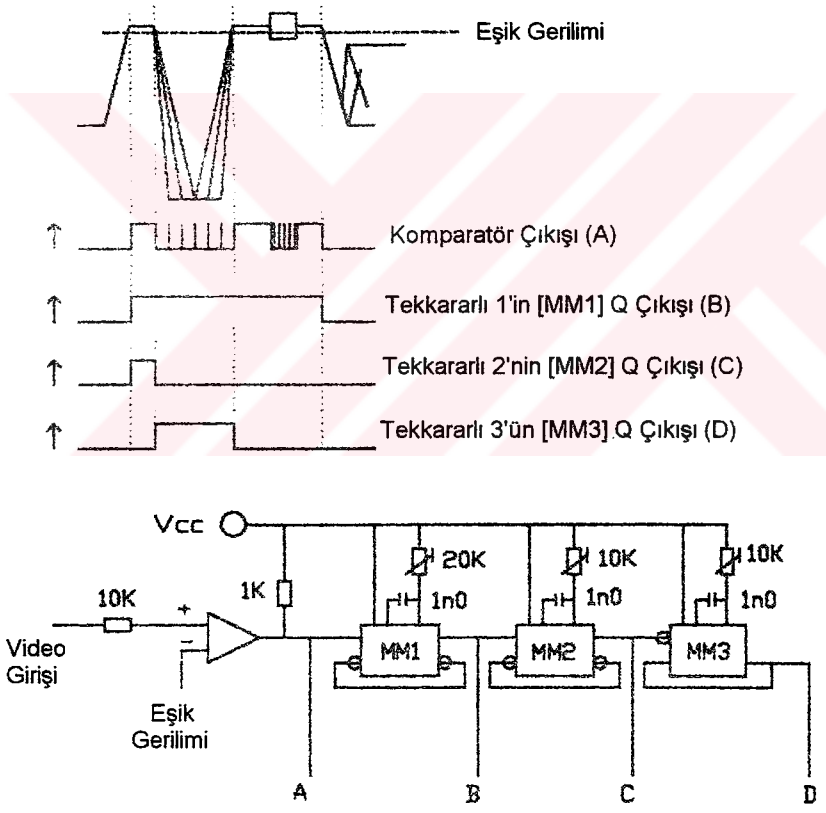
3.7.2 Yalancı satır gecikmesi

Bu teknik, videoyu geciktirmenin en güzel metodlarından biridir. Yatay senkronizasyon darbesi kısaltılmış ve yatay karartma aralığında titretilmiştir. Bu durum, videonun normal

pozisyonda başlamasına rağmen satır gecikmesi etkisi yaratmıştır. Burada değişen sadece, yatay senkronizasyon darbesinin konumudur.

Teleclub kanalının eskiden kullanmış olduğu PayView-III sistemi bu özelliğe sahiptir [1]. Bu sistem ilk kullanıldığı zaman, korsan düzeltici piyasasının % 90'ını etkisiz hale getirmiştir. Sadece, içine yeni bir yatay senkronizasyon darbesi konulan korsan düzelticiler çalışmasına devam edebilmiştir [1].

Korsan düzelticilerin büyük bir kısmı renk patlaması slotunu, zamanlama referansı olarak kullanırken bazı düzelticiler alışılmışın çok dışında bir yaklaşıma sahiptir. PayView-III sistemindeki yatay karartma, beyaz seviyesi üstüne yükseltilmiştir [1]. Yükseltilmiş yatay karartmaya geçişteki yükselen kenarı bulmak için bir komparatör kullanarak, yatay senkronizasyon darbesinin içine yeniden zamanlanmış ve yeniden yaratılmış bir yatay senkronizasyon darbesi sokulabilmektedir (Şekil 3.16).



Şekil 3.16 Yalancı satır gecikmesi bulan devre [1]

3.8 Otomatik Anahtarlama Teknikleri

Otomatik anahtarlama (autoswitching) tabirinin anlamı, düzelticinin karıştırılmış bir sinyali bulması ve kullanıcının müdahalesi olmaksızın otomatik olarak bu sinyali düzeltmesidir. Bu

düzeltici, alıcıdaki video girişinin dönüşüne veya direkt olarak televizyondaki video girişine bu düzeltilmiş videoyu göndermektedir. ASTRA tipi alıcılarda genellikle, SCART veya D-Tipi konnektörler kullanılmaktadır [1]. Bu konnektörler, bir düzelticiyi alıcıya bağlamak için gerekli olan bütün giriş ve çıkış arabirimlerine sahiptir. ASTRA tipi alıcılarda, düzeltici için bir SCART veya D-Tipi konnektör mevcuttur. Düzelticinin bağlandığı SCART konnektörü, standart bir SCART konnektöründen farklıdır. Bir SCART veya D-Tipi konnektör durumunda alıcının, alıcı demodülatör çıkışından ziyade düzeltilmiş video sinyalini alıcının yakalayabilmesi için konnektör pinlerini kontrol etmek için bir anahtarlama gerilimi vermesi gereklidir [1]. Bir televizyona düzeltilmiş videoyu sağlamak için standart bir SCART konnektörü kullanıldığı zaman, bu SCART konnektörünün sekizinci pininde aynı anahtarlama voltajının mevcut olması gereklidir. Bu voltaj, harici video ve audio kaynakları seçimi için 12 Volt ve dahili seçim için ise 0 Volt olmalıdır [1].

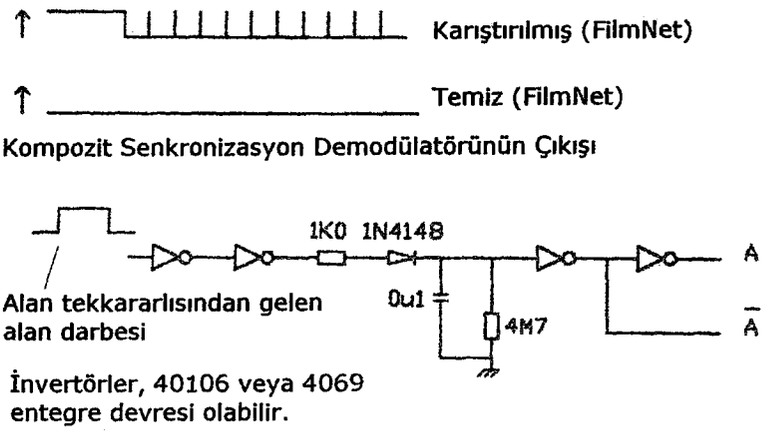
Otomatik anahtarlama işlemi için karıştırılmış sinyalin bulunması çok önemlidir. Orijinal düzelticiler, karıştırılmış sinyaldeki adresleme bilgisini bulmaktadır. Sky Channel'ın kullanmış olduğu VideoCrypt düzelticisi, karıştırılmış Sky Movies sinyaliyle beslenmiş olduğu zaman karıştırılmış sinyale bir kanal tanımlayıcı koymaktadır. Ayrıca, düzelticiyi çevrime anahtarlamak için düzeltici SCART konnektöründe bir anahtarlama pinini aktif hale getirmektedir. Dahili versiyonlar, anahtarlamayı gerçekleştirmek için bir çoklayıcı kullanmaktadır. Fakat, eğer bu çoklayıcı entegre devresi yanarsa karıştırılmış veya temiz kanallardaki video ekranda görünmemektedir.

Otomatik anahtarlamanın türü, düzelticinin çalışma şekline bağımlıdır [1]. Kompozit senkronizasyon taşıyıcı tekniği kullanan bir düzelticinin devre yapısı aşırı derecede basittir. FilmNet SATPAC sistemi buna iyi bir örnektir.

FilmNet, kompozit senkronizasyon taşıyıcısını 7.56 MHz'de karıştırdığı zaman sinyali düzeltmek için gerekli olan kompozit senkronizasyon sinyalini de taşımıştır. Sinyal karıştırılmadığı zaman bu kompozit senkronizasyon sinyali 7.56 MHz'de iletilmemiştir. Bu otomatik anahtarlama devresi, kompozit senkronizasyon sinyalinin bulunduğunu veya bulunmadığını tespit etmek için gerekmektedir. Buradaki ana düşünce, bu devrenin bir ses sinyali üzerinden tetiklenmemesidir.

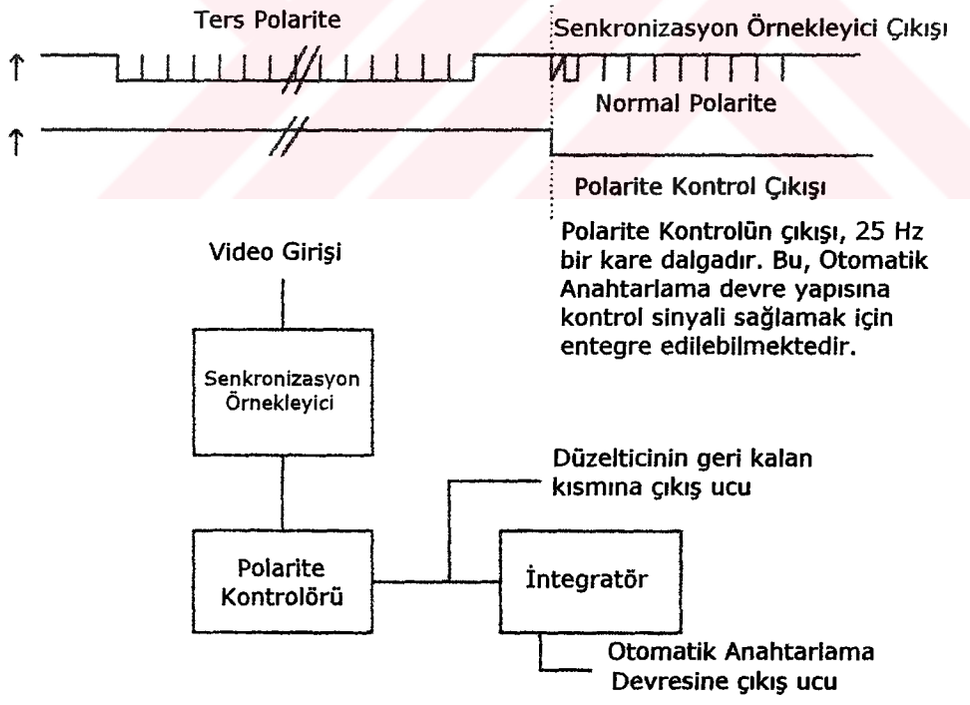
FilmNet düzelticilerinin büyük bir kısmında alan darbesi, kompozit senkronizasyon sinyalinden ayrılmıştır [1]. Alan darbelerinin darbe treni bir integratörü beslemektedir. Bu integratörün çıkışındaki invertör sadece kondansatör yeterince şarj olduğu zaman konum

değiştirmektedir. Kompozit senkronizasyon sinyali olmadığı zaman bu invertörün çıkışı yüksek olmaktadır. Şekil 3.17'de gösterilmiş olan temel devre yapısı pek çok tasarıma adapte edilebilir.



Şekil 3.17 Otomatik anahtarlama yapan basit bir devre [1]

Otomatik anahtarlamayı gerçekleştirmek için başka metotlar da mevcuttur. Bu metotlar genellikle, yatay senkronizasyonun bulunmayışını tespit etmeyi veya ters çevrilmiş senkronizasyonu tespit etmeyi kapsamaktadır. Bu çalışma şekillerinde kullanılmış olan ayrıntılı devreler karmaşık yapıda olabilmektedir.



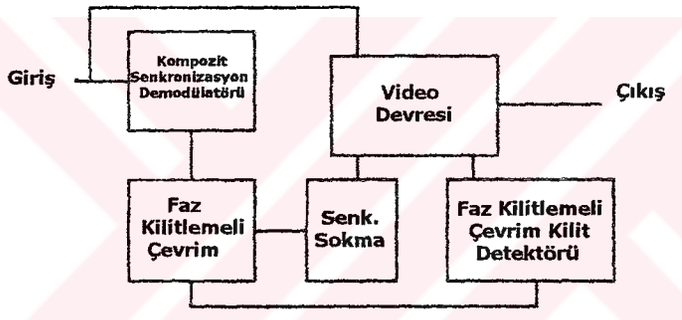
Şekil 3.18 Video polarite seçiminin kontrol edilmesi [1]

Yatay senkronizasyonun bulunmayışını tespit etme, en basit çalışma şekillerinden biridir. Bunu gerçekleştirmek için kullanılmış olan devre sadece bir komparatör devresidir. Video

temiz olduğu taktirde bu komparatörün çıkışı temiz bir senkronizasyon treni olmaktadır.

FilmNet kanalı tarafından kullanılmış olan birbiri ardından gelen inversiyon metodu, otomatik anahtarlamanın uygulamasını kolay hale getirmiştir (Şekil 3.18). İnversiyon alan bazlı olduğu için video polarite seçimini kontrol etmek için gerekli olan anahtarlama dalga biçimi 25 Hz'lik bir kare dalga olmaktadır. Bu kare dalganın yüksek kısmı, ters çevrilmiş videoyu seçmek için kullanılmaktadır. Ayrıca bu kare dalga, karıştırılmış sinyali düzelticinin tanımlayabilmesi için kullanılmaktadır. İnversiyon olmadan doğrudan senkronizasyon bastırılmış bir sinyal olduğu taktirde kare dalga kullanılmamaktadır [1]. Kare dalganın bulunmayışı, video sinyalinin karıştırılmış olmaktan ziyade temiz olduğunu düzeticiye bildirmektedir.

LuxCrypt düzelticilerinde de otomatik anahtarlama gerçekleştirilmiştir. Yatay veya düşey senkronizasyon yoksa bu bir tetikleme gibi davranabilmektedir. Bu sistem için tasarlanmış olan düzelticilerin büyük bir kısmı faz kilitlemeli çevrimleri kullandığı için ikinci tetikleme kilitli bir faz kilitlemeli çevrim olacaktır.



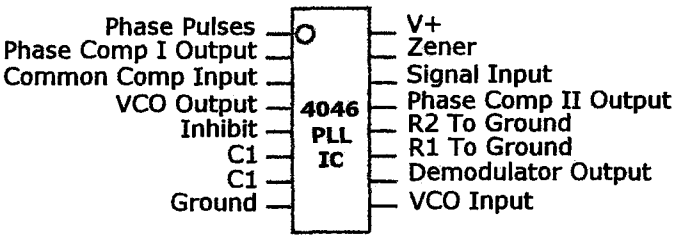
Şekil 3.19 Faz kilitlemeli çevrim bazlı düzelticilerde kullanılan metot [1]

3.9 Faz Kilitlemeli Çevrimler

En kolay temin edilebilen faz kilitlemeli çevrim entegre devrelerinden biri 4046'dır (Şekil 3.20). Bu entegre devre, ticari olmayan uygulamalarda yaygın bir şekilde kullanılmıştır. Bu tasarımlardan bazıları, bir satır senkronizasyon sinyalini yeniden üretmek için 15.625 kHz'de çalışan faz kilitlemeli çevrimlerin bulunduğu FilmNet SATPAC ve Oak ORION düzelticileridir [1].

Faz kilitlemeli çevrimlerin bu düzelticilerdeki başlıca kullanılma alanı senkronizasyon yeniden üretme işlemidir. Faz kilitlemeli bir çevrim kullanmak için bazı referans sinyallerin bulunması gereklidir. Eğer FilmNet kanalında iletilmiş olan kompozit senkronizasyon sinyali gibi bazı referans sinyaller mevcutsa, bu bulma işlemi genellikle kolay bir işlemdir. Buna

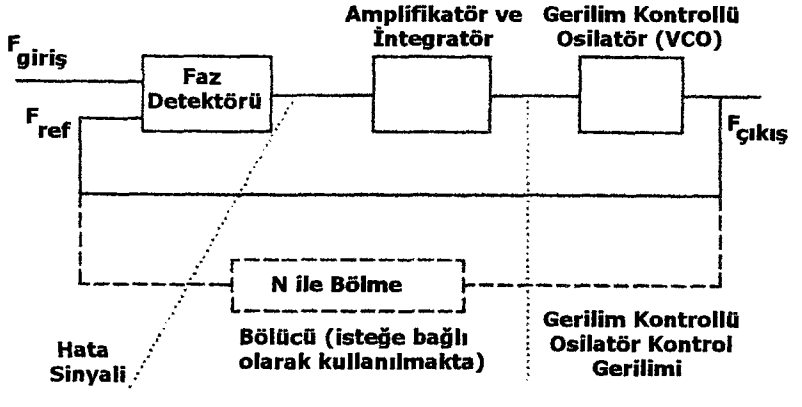
alternatif olarak, bastırılmış yatay senkronizasyonlar kullanılabilmektedir. Bunların kullanılabilmesi için örneklenmesi gerekmektedir.



Şekil 3.20 4046 faz kilitlemeli çevrim entegre devresi bacak bağlantıları [1]

Düzelticilerde faz kilitlemeli çevrimlerin en yaygın kullanılan formlarından biri, giriş veya referans frekansının birkaç katında çalıştığı formdur. FilmNet sinyalinde, yatay senkronizasyon kısmını gerçek düzeyine çekmek için bir sinyalin elde edilmesi gerekmektedir. 15.625 kHz'de çalışan bir faz kilitlemeli çevrim kullanımı tasarımcıyı, polarite testi için gerekli olanlara benzeyen darbeler üretmek için tekkararlıların kullanımıyla sınırlamaktadır [1]. Yüksek bir frekans çıkışı üretmek için düşük bir frekans girişi kullanan bir faz kilitlemeli çevrim, bir frekans katlayıcı (çarpıcı) olarak adlandırılmaktadır. Bu tip faz kilitlemeli çevrimlere iyi bir örnek, bu bölümünde incelenmiş olan faz kilitlemeli çevrim bazlı FilmNet düzelticisidir.

Faz kilitlemeli çevrim bazlı FilmNet düzelticisinde kombinasyonel lojik kullanılarak 2.0 MHz'lik çalışma frekansı bölünmüştür. Kombinasyonel lojik, senkronizasyonun aşağıya çekilebilmesi için gerekli olan doğru sürenin bir darbesini sağlamaktadır. Ayrıca, örnek kapı darbesi veya polarite test darbesi gibi diğer sinyalleri elde etmek için de kombinasyonel lojik kullanılabilmektedir.



Şekil 3.21 Düzelticilerde faz kilitlemeli çevrim kullanımının blok şeması [1]

Şekil 3.21'de gösterilmiş olan faz kilitlemeli çevrim blok şemasında gerilim kontrollü osilatörün minimum frekans menzili VCO kontrol gerilimi V_{ss} gerilimine eşit olduğu zaman (3.1) eşitliğinden ve maksimum frekans menzili ise VCO kontrol gerilimi V_{dd} gerilimine eşit olduğu zaman (3.2) eşitliğinden elde edilmektedir [1].

$$F_{min} = \frac{1}{R_2(C_1 + 32pF)} \tag{3.1}$$

$$F_{max} = F_{min} + \frac{1}{R_1(C_1 + 32pF)} \tag{3.2}$$

Şekil 3.20'de gösterilmiş olan faz kilitlemeli çevrim entegre devresinin 2 ve 9'uncu pinleri arasına PLL'nin kilit menzilini saptayan bir alçak geçiren filtre bağlanmaktadır. Kondansatör toprak ve 9'uncu pin arasına, direnç ise 2 ve 9'uncu pinlerin arasına bağlanmaktadır. Bu kilit menzili (3.3) eşitliğinden elde edilmektedir [1].

$$F_l = \frac{(F_{max} - F_{min})}{2} \tag{3.3}$$

Yakalama menzili ise (3.4) eşitliği ile tanımlanmaktadır. (3.4) eşitliğindeki R_3 2 ve 9'uncu pinler arasına, C_2 ise toprak ve 9'uncu pin arasına bağlanmaktadır.

$$F_c = \frac{1}{P_i}\sqrt{\frac{2P_iF_l}{R_3C_2}} \tag{3.4}$$

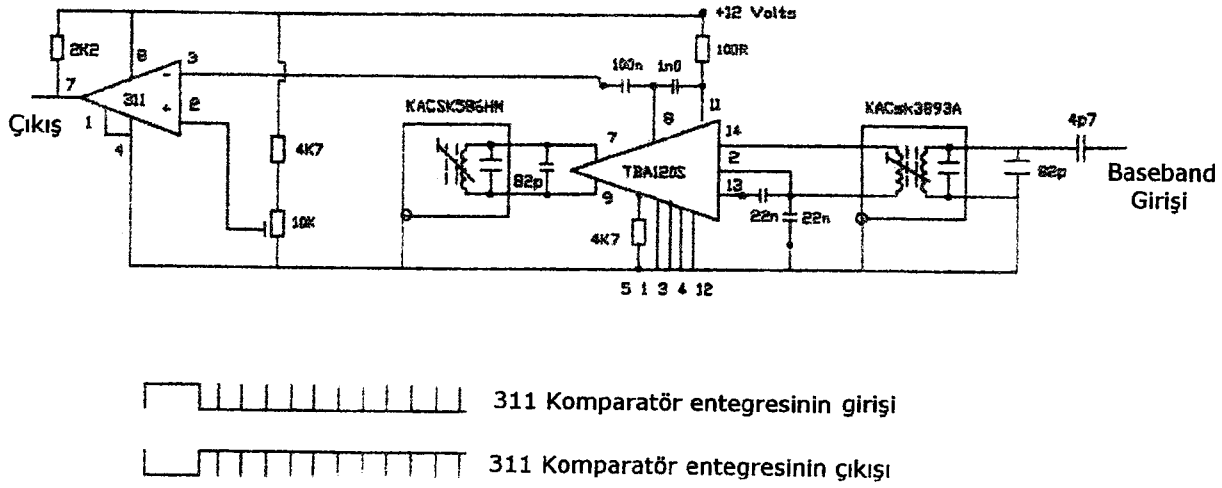
3.10 Düzeltici Tasarımlarının İncelenmesi

3.10.1 Faz kilitlemeli çevrim bazlı FilmNet düzelticisi tasarımı

FilmNet, SATPAC sistemi kullanmayı bırakarak D2-MAC EuroCrypt sistemine geçmiştir [1]. Şekil 3.22'de gösterilmiş olan devrenin kullanılmasının nedeni mikrokontrolör kullanılmadan sadece analog yöntemle nelerin başarılabileceğini göstermektir. Ayrıca FilmNet'in eski SATPAC sistemini Yunanistan'a yayın yapan bir bağlantısında kullandığı için bu devre (Şekil 3.22) hala bazı uygulama alanlarına sahiptir.

Bu FilmNet düzelticisi, yatay karartmayı sağlamak için 2 MHz'lik bir faz kilitlemeli çevrim kullanmaktadır. Yapılan polarite bulma için hiç bir hazırlık olmamasına rağmen otomatik anahtarlama özelliği vardır. Bu devre, kolayca temin edilebilen parçalar kullanılarak gerçekleştirilmiştir.

Verilmiş olan bu devre diyagramı (Şekil 3.22) Hi Tech Xtravision korsan FilmNet düzelticisinin en önemli kısmıdır [1].



Şekil 3.22 PLL bazlı FilmNet düzelticisi için kompozit senkronizasyon demodülatörü [1]

3.10.1.1 Kompozit senkronizasyon demodülatörü

FilmNet SATPAC sistemi, 7.56 MHz'de bir alttaşıyıcı üzerinden kompozit bir senkronizasyon sinyali iletmektedir. FilmNet sinyalinin düzeltilmesi, bu taşıyıcının demodüle edilmesini ve bunun görüntüdeki senkronizasyon düzeylerinin yeniden eklenmesinde kullanılmasını gerektirmektedir.

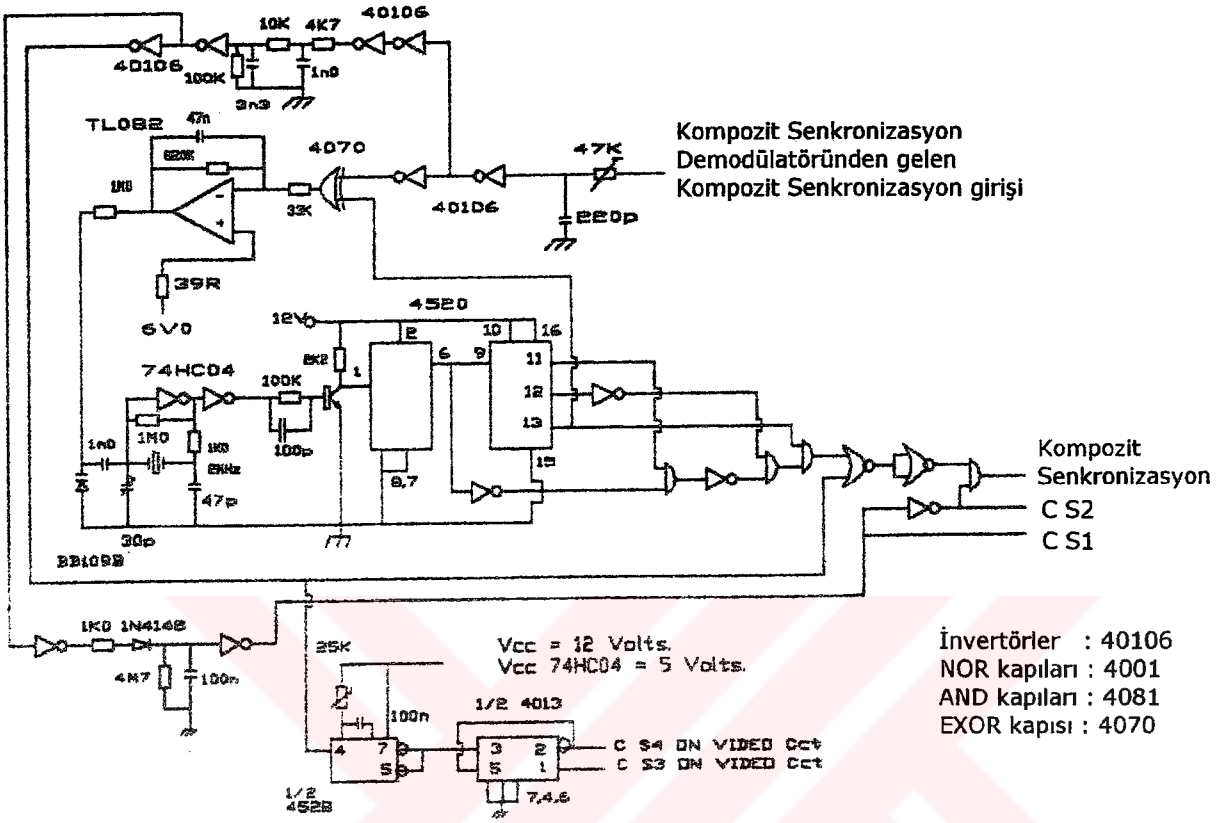
Şekil 3.22'de gösterilmiş olan demodülatör, TBA120S dörtlü demodülatör entegre devresini esas almaktadır. Kurulumu basitleştirmek için iki adet 10.7 MHz'lik transformatör (KACsk586HM ve KACsk3893A) kullanılmıştır. Bu transformatörler, transformatörlerin dahili kondansatörlerine paralel birer 82 pF'lık kondansatör ilave edilmesiyle doğru frekansta rezonansa gelmektedir. Bu uygulamada, NP0 kondansatörlerinin kullanılması gereklidir [1].

Verilmiş olan değerlere göre kompozit senkronizasyon çıkışı yaklaşık olarak 1.0 V tepe gerilimidir. Bu kompozit senkronizasyon sinyali, negatif yönde bir senkronizasyon çıkışı sağlayan bir 311 komparatör entegre devresini beslemektedir. Bu sinyal, ana lojik kısmı beslemektedir.

3.10.1.2 Düzelticinin lojik bölümü

Lojik kısmın ilk bölümü faz ayarlamadır. Şekil 3.23'te gösterilmiş olan bu lojik bölüm, yatay karatma penceresini videoya bağlı olarak doğru biçimde yerleştirmek için kullanılmıştır. Kullanılmış olan invertörler, 40106 Schmitt tipi entegre devrelerdir. Faz detektörü, hemen

ardından bir integratör gelen bir 4070 EXOR kapısıdır. Bu integratörün çıkışı hata voltajını vermektedir ve gerilim kontrollü osilatör kristalinin (VCXO) frekansını kontrol etmek için kullanılmıştır.

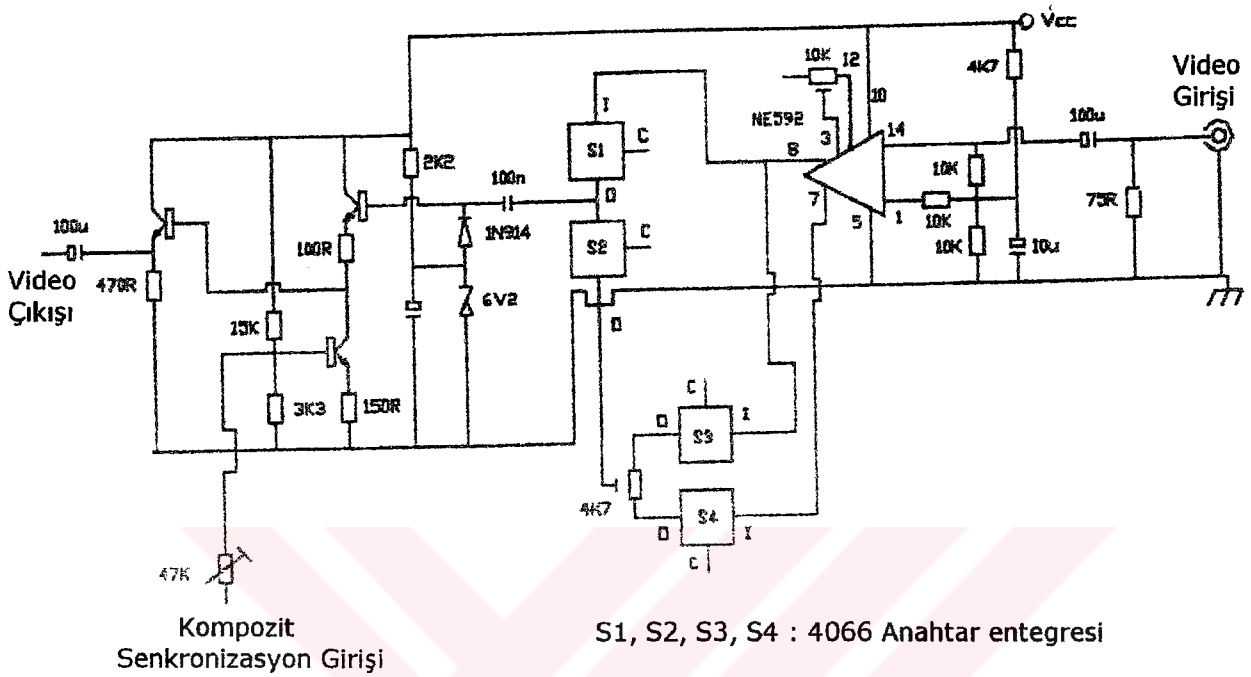


Şekil 3.23 PLL bazlı FilmNet düzelticisi için faz kilitlemeli çevrim devresi [1]

Gerilim kontrollü osilatör kristali, 74HC04 invertör entegre devresini baz almaktadır. Bu entegre devrenin uygun şekilde çalışması için 5.0 V'luk bir besleme gerilimi gerekmektedir. Bu entegrenin başlıca avantajı düşük akımda çalışabilmesidir. Gerilim kontrollü osilatör kristalinin çıkışı, transistörlü tampon ile tepeden tepeye 12 V'luk bir sinyale dönüştürülmüştür

Gerilim kontrollü osilatör kristalinden gelen 2 MHz'lik tamponlanmış sinyal, 4520 ikili binary sayıcı entegresini beslemektedir. Bu entegre, 2 MHz'lik frekansı bölmek için kullanılmıştır. Çıkışlarda kombinasyonel lojik kullanarak doğru olarak zamanlanmış bir yatay karartma penceresi sağlanmıştır. Bu yatay karartma sinyali, doğru olarak zamanlanmış bir kompozit karartma sinyali sağlamak için alan darbe integtatörü ile birleştirilmiştir. Bu sinyal, video sıyırmanın senkronizasyon ekleme kısmını kontrol etmek için kullanılmıştır. Bir AND kapısı, düzeltici devre yapısının otomatik anahtarlama devresi ile kapatıldığı zaman senkronizasyon sinyalinin burada bulunmamasını sağlamaktadır.

Otomatik anahtarlama devresi, alan darbelerinin integralini almaktadır. Eğer alıcı cihaz FilmNet kanalına akortluysa (ayarlanmışsa) bu devrenin girişinde hiçbir alan darbesi mevcut olmayacaktır [1]. Bu durum, S1 anahtarının kapatmasına ve S2 anahtarının açmasına neden olacaktır. Bu çalışma şekli, normal polariteli videodan video kenetleme ve çıkış katına geçmektedir. AND kapısının kompozit karartma çıkışı, düşük olması için bu devre tarafından



zorlanmaktadır.

Şekil 3.24 PLL bazlı FilmNet düzelticisi için video sıyırıcı devresi [1]

3.10.1.3 Düzelticinin video sıyırıcı devresi

NE592 entegre devresi, değişken bir kazanç amplifikatörü elde etmek için kullanılmıştır (Şekil 3.24). Bu entegrenin pozitif ve negatif çıkışları birkaç 4066 anahtar entegre devresini beslemektedir. İlk iki anahtar olan S1 ve S2, video seçimini kontrol etmektedir [1].

Çizelge 3.1 Video sıyırıcı devresinde video seçimini kontrol eden anahtarlar [1]

Kontrol Anahtarları		Video Seçimi
S1	S2	
0	1	Normal video. Düzeltici kapalı
1	0	Karıştırılmış video. Düzeltici açık

S2 anahtarı için kontrol sinyali, bazı uydu alıcılarında tüm döngüyü gerçekleştirmek için kullanılabilmektedir. İkinci anahtar grubu olan S2 ve S3, alan polarite seçicileridir. Bu anahtarlar, lojik kısımdaki alan polarite flip-flop'larının çıkışları ile kontrol edilmektedir. Bir

ön ayar direnci dahil edildiği için çıkışlar arasındaki herhangi bir doğru akım kayması sıfırlanabilmektedir [1].

Seçilmiş olan video kaynağı, dalga biçimindeki dağılmayı gidermek için bir tespit devresini beslemektedir. Senkronizasyonun aşağıya çekilmesi, bir transistör anahtarının açılması ve kapatılması ile gerçekleştirilmektedir. Aşağıya çekmenin düzeyi, 47 kΩ'luk ön ayar direnci ile kontrol edilmektedir.

3.10.2 Radio Plans tasarımı düzeltici

Bu tasarım, Radio Plans dergisinde yayımlanmış olan devre tasarımıdır. Derginin bu sayısı mahkeme kararıyla toplatılmıştı. Fakat daha sonra, Le Quotidien isimli bir Fransız gazetesi bu tasarımı yayımlamıştır ve bu yolla bu tasarım, daha öncekinden çok daha geniş bir kitleye ulaşmıştır [1]. Radio Plans tasarımlı düzeltici, PAL sinyalinden ziyade SECAM sinyalinde kullanılmak için tasarlanmıştır. PAL versiyonundaki zamanlama bundan biraz farklıdır. Ticari bakımdan bu tasarımın uygulanması uygun değildir. Bu yüzden bilgisayar korsanları, bu devrenin büyük bir kısmını daha basit devre yapıları ile değiştirmiştir. Bunun sonucunda ortaya çıkan düzeltici daha ucuza üretilmiştir [1]. Halen kullanımda olan Discret sisteminin yeni versiyonları, sistemin hack edilme problemi arttığı zaman bu tasarımın üstesinden gelinebilmesi için terfi edilmiştir.

Radio Plans devresi beş kısımdan oluşmaktadır. Bu kısımlar; ses düzeltici, video detektörünün başlangıcı, video düzeltici, video çoklayıcı kısım ve senkronizasyon üretici devre olarak adlandırılmıştır. Bu tasarımda birkaç adet pahalı entegre devre kullanılmıştır. Bu yüzden bu devre tasarımı amatör bilgisayar korsanları arasında çok popülerdi. Fakat bu tasarıma yoğun talep, piyasada kritik entegre devrelerin bulunamamasına yol açmıştır. Bu yüzden, bilgisayar korsanları bu tasarımı mecburen başka devrelere uyarlamak zorunda kalmıştır [1].

3.10.2.1 Ses düzeltici devresi

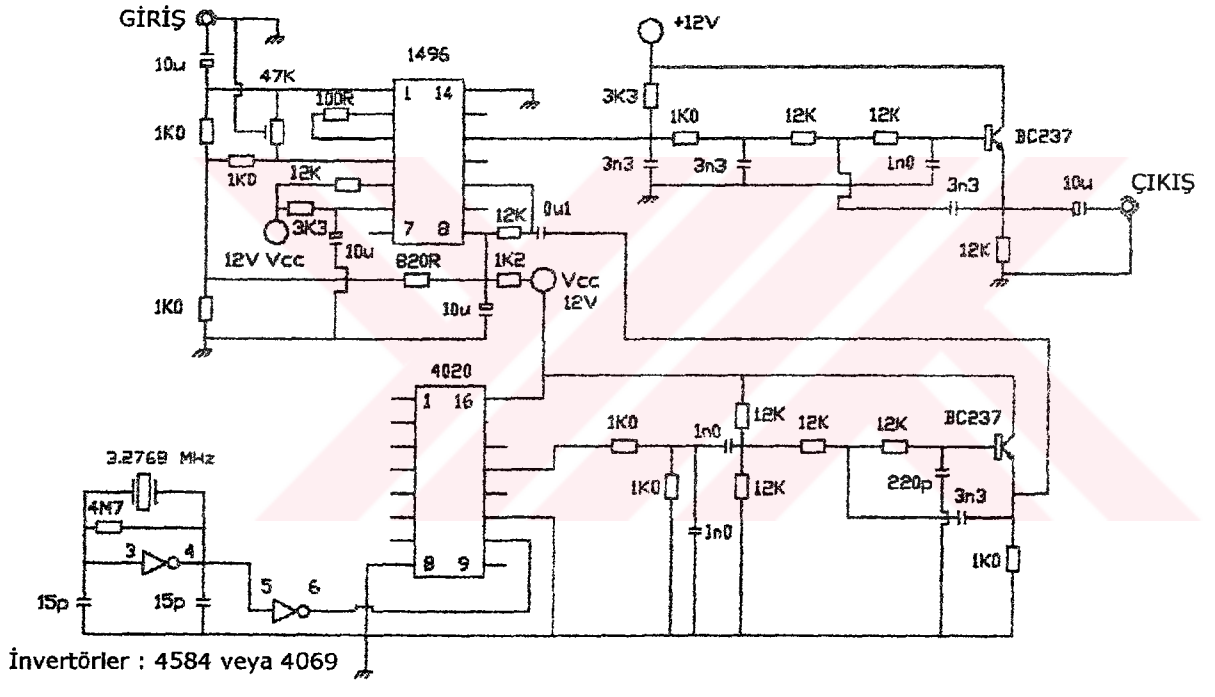
Discret sisteminde ses, 12.8 kHz'lik bir taşıyıcı etrafında yer değiştirmektedir. Şekil 3.25'te gösterilmiş olan Radio Plans Discret ses düzeltici tasarımı, 3.2768 MHz'de çalışan bir kristal kontrollü osilatör kullanmaktadır. Bu osilatör, iki adet 4584 CMOS invertör entegresini baz almaktadır. İnvertör entegrelerinden bir tanesi osilatör olarak, diğeri ise tampon olarak kullanılmıştır [1].

Bu osilatörün çıkışı bir 4080 bölücü entegresini beslemektedir. Bu bölücü, 12.8 kHz'lik

taşıyıcıyı elde edebilmek için osilatör frekansını 256 ile bölmektedir. Bu 4020 bölücü entegrenin çıkışı transistörlü bir filtreyi beslemektedir. Bu filtre, mevcut olan harmonikleri filtrelemek için ve kare dalgayı bir sinüs dalgasına çevirmek için kullanılmıştır.

Daha sonra bu 12.8 kHz'lik sinüs dalgası, bir 1496 dengeli demodülatör entegre devresini beslemektedir. Bu 1496 entegresi, tek yollu çalışması için ayarlanmıştır. Ayrıca, karıştırılmış ses bu entegre devreye girmiştir. 47 kΩ'luk bir ön ayar direnci, dengeleme ve eşitleme kontrolünü sağlamaktadır.

1496 entegresinin çıkışı, düzeltilmiş seste artakalan herhangi bir 12.8 kHz'lik sinyali filtrelemek için tek transistörlü bir filtreyi beslemektedir. Daha sonra, bu düzeltilmiş ses tekrar SCART konnektörünü beslemektedir.

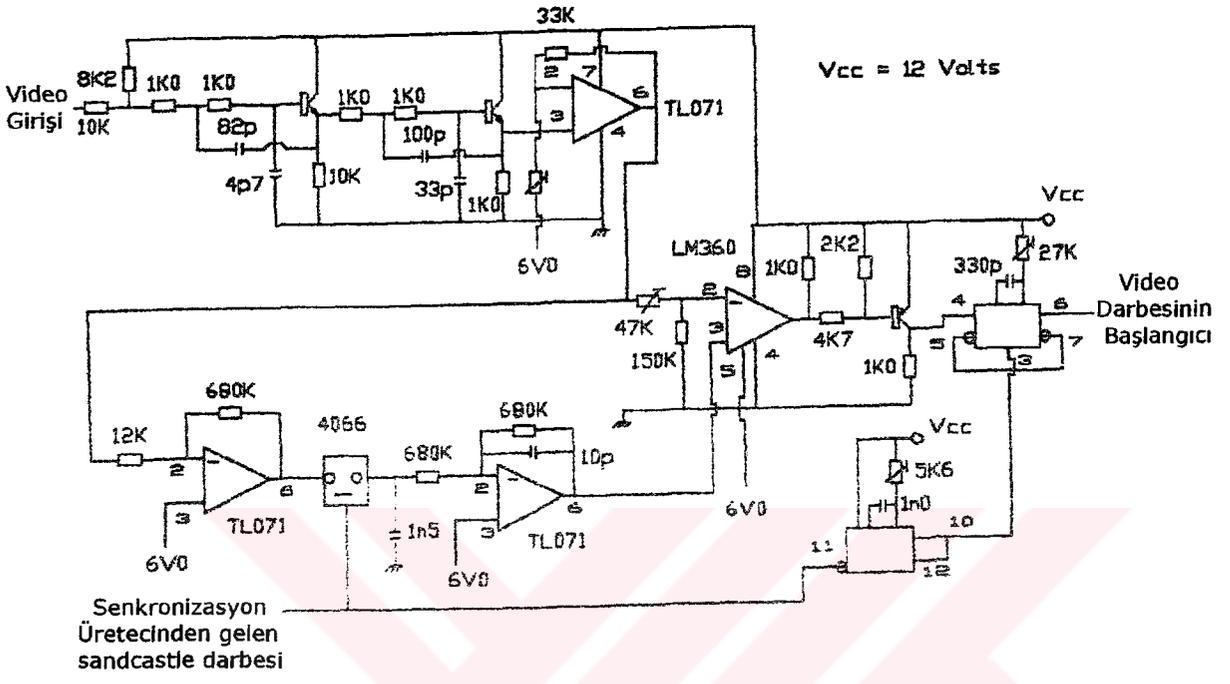


Şekil 3.25 Radio Plans Discret ses düzeltici tasarımı [1]

3.10.2.2 Video başlangıcı detektörü tasarımı

Video düzeltici kısmındaki ilk TBA970 entegresinin çıkışından gelen karıştırılmış video, bir transistörlü iki katlı alçak geçiren filtreyi beslemektedir. Bu filtre, video dalga biçiminden gelen krominansı (renkliliği) gidermektedir. Daha sonra, ortaya çıkan video sinyali 5 çarpanı ile kuvvetlendirilmektedir. OPAMP'tan gelen sinyal, geri düzey örneğini ve tutucusunu ve de komparatörü beslemektedir [1].

Örnekleyici ve tutucu devre, örnekleme anahtarı olarak bir 4066 entegresini ve depolama veya tutma kondansatörü olarak da 1.5 nF'lık bir polistiren kondansatörü baz almaktadır. Tampon olarak kullanılmış olan OPAMP basit bir TL071 entegre devresidir. Bu uygulamada (Şekil 3.26) bu tampon, birleşme kazançlı evirmeyen amplifikatör biçimindedir. Bu amplifikatörün çıkışı komparatörü beslemektedir.



Şekil 3.26 Radio Plans Discret video başlangıcı detektörü tasarımı [1]

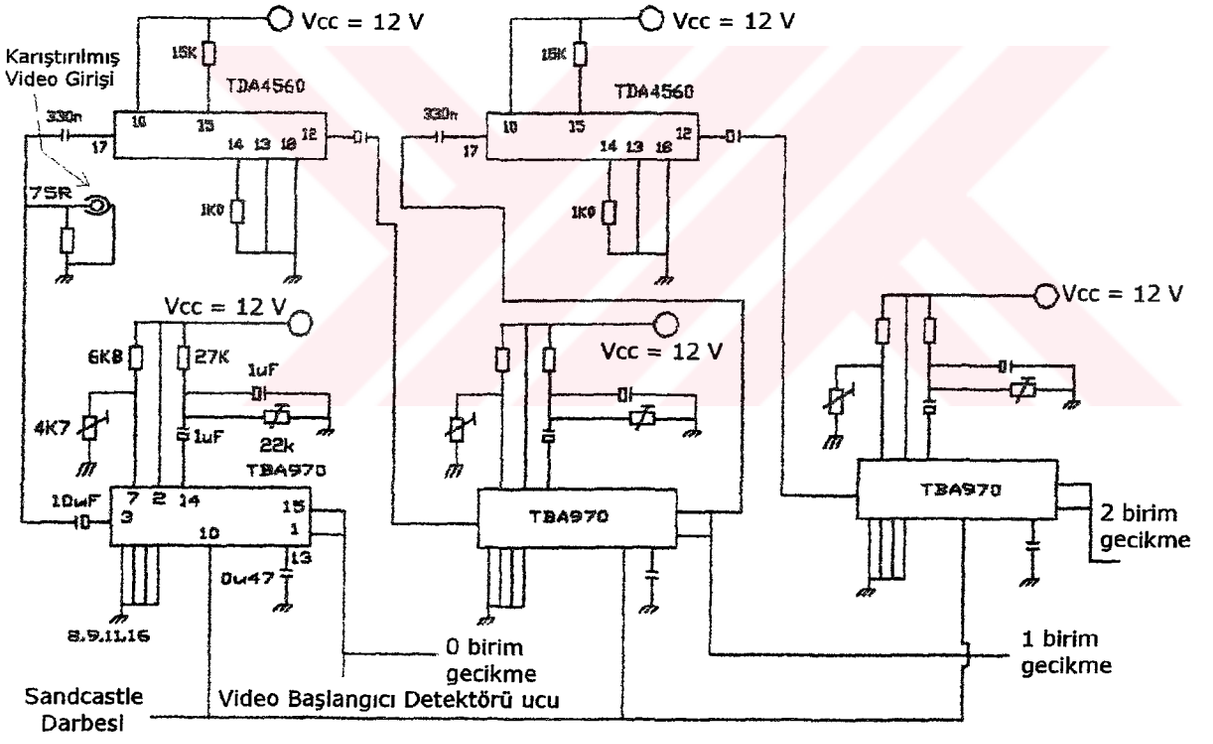
Bu komparatör sürekli olarak, örneklenmiş siyah düzeyi ve video sinyali arasındaki gerilim farkını karşılaştırmaktadır. Bu komparatörün, yaklaşık olarak 150 mV'luk bir artışı tespit etmesi gereklidir. Örnekleme kapısı, senkronizasyon üretici devresi tarafından üretilmekte olan sandcastle darbesi tarafından kontrol edilmektedir. Komparatörün çıkışı, transistörlü bir düzey konvertörünü beslemektedir. Bu, komparatör çıkışını CMOS lojik düzeylerine dönüştürmektedir.

Ayrıca bu sandcastle darbesi ilk tekkararlıyı tetiklemektedir. Bu tekkararlı, satırın doğru alanındaki video penceresinin başlangıç pozisyonuna bir gecikme üretmektedir. Bu tekkararlının çıkışı, video darbesi tekkararlısının başlangıcının etkilileştirilmesini kontrol etmektedir. İkinci tekkararlı ise videonun başlangıcını gösteren sabit uzunlukta bir darbe üretmektedir [1].

3.10.2.3 Video düzeltici devresi

Video düzeltici devresi (Şekil 3.27) gecikme satırları, siyah düzeyi tespit devreleri ve amplifikatörlerinden oluşmaktadır. Gecikme satırları olarak TDA4560 entegresi kullanılmıştır. Bunlar, videoya 888 ns'lik bir gecikme sağlayacak şekilde ayarlanmıştır. TDA4560 jiratör gecikme satırı, 5 MHz gibi iyi bir cevaba sahiptir. Fakat 6 dB kadar bir kaybı vardır [1]. Bu yüzden, düzeyi normale düzeltmek için bazı kuvvetlendirme işlemleri gerekmektedir. Ayrıca bu sinyalin, siyah düzeyi tespitine de sahip olması gereklidir. Bu durum, uygun düzeltme işlemi için gereklidir. Eğer her bir geciktirilmiş video sinyalinin arasındaki siyah düzeyinde bir fark varsa, ekranda strobing etkisi olacaktır. Bazı FilmNet düzelticilerinde bu etki, iki alanın aynı düzeyde olmadığı zamanki etki ile benzerdir.

Video düzelticisinde dört çıkış vardır. Her bir TBA970 entegresinden birer adet olmak üzere üç çıkış, video çoklayıcı devre yapısını beslemektedir. İlk TBA970 entegresinin çıkışı, video detektörünün başlangıcı devresini beslemektedir.



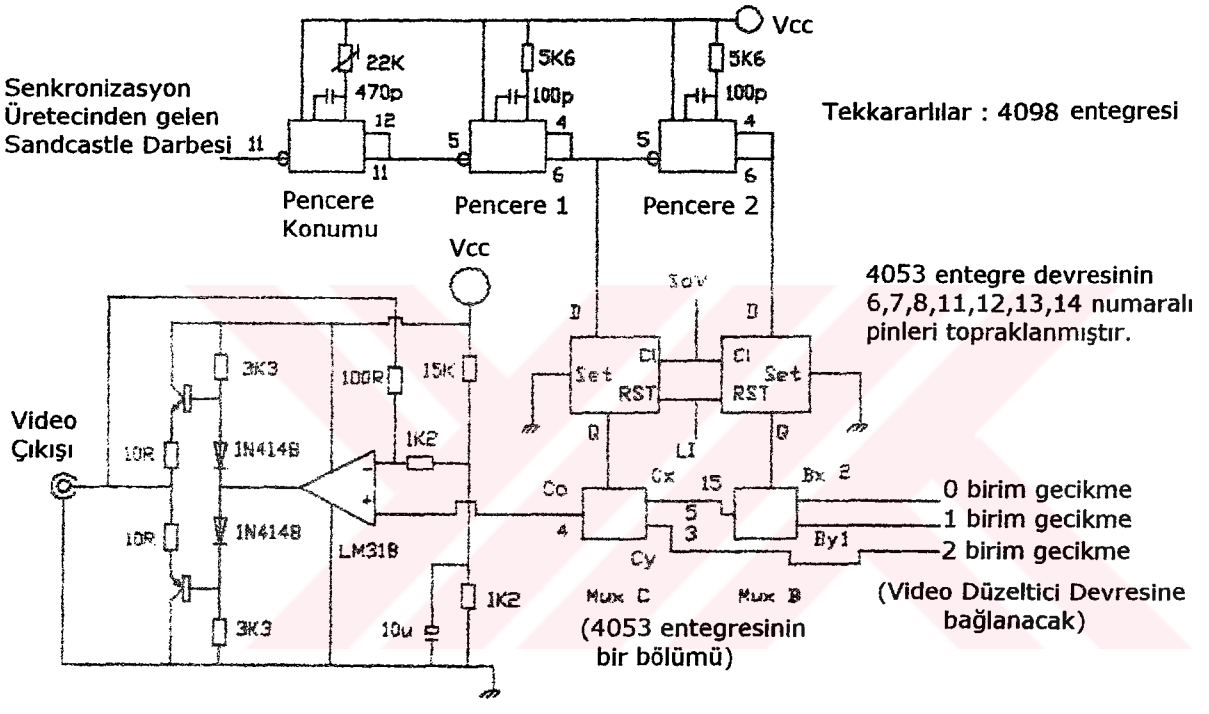
Şekil 3.27 Radio Plans Discret video düzeltici tasarımı [1]

3.10.2.4 Video çoklayıcı devresi

Düzeltici sistemin video çoklayıcı kısmında temel (Şekil 3.28) olarak dört eleman vardır. Bunların birincisi tekkararlı zamanlama zinciridir. Bu, üç tekkararlıdan oluşan bir zincirdir. İlk tekkararlı, diğer iki tekkararlının çıkışlarını konumlandıran bir gecikme üretmektedir.

Diğer tekkararlılar ise flip-flop'lar için pencere veya veri sinyallerini üretmektedir [1].

Bu flip-flop'lar, çoklayıcıyı kontrol etmektedir. Her bir flip-flop'taki D bacağı sadece her birinin kendi penceresi boyunca yüksektir. Video darbesinin başlangıcı her bir flip-flop'ta clock'lama darbesi (CL) sağlamaktadır. Senkronizasyon üretici devresinden gelen LI sinyali, her bir flip-flop'un RESET bacağını beslemektedir. Bu sinyal, yatay senkronizasyon darbesinin başlangıcında flip-flop'ları resetleyerek çoklayıcıların iki gecikme moduna geçmesini sağlamaktadır. Bu durum, satırın senkronizasyon ve renk patlaması kısmının geciktirilmeden geçmesini sağlamaktadır. Düzeltilmiş görüntüdeki düzgün satır kararlılığı için bu çok önemlidir.



Şekil 3.28 Radio Plans Discret video çoklayıcı tasarımı [1]

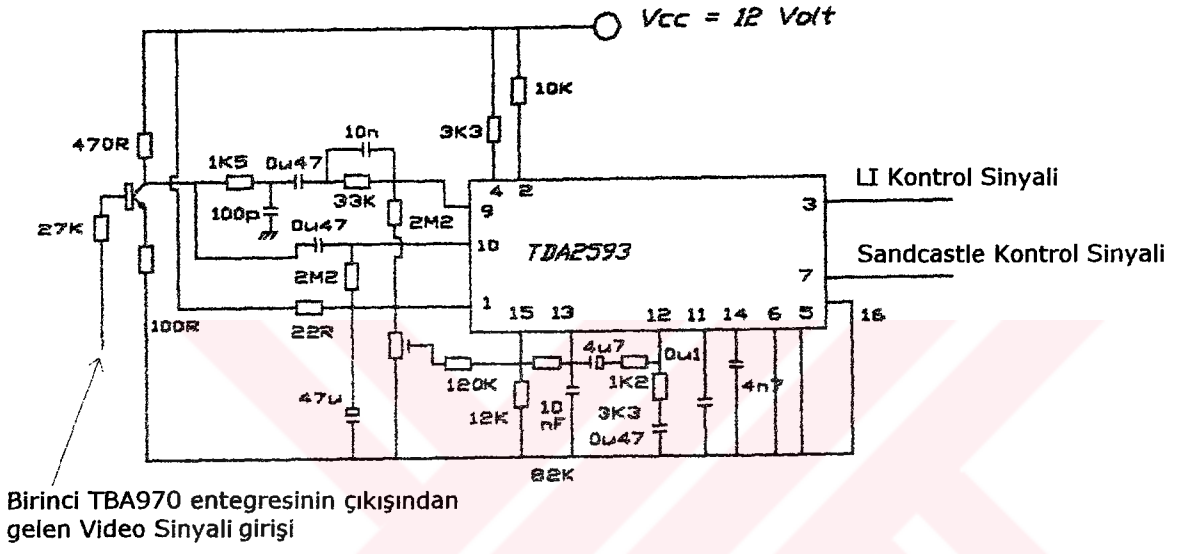
Bu devre tasarımında 4053 çoklayıcı entegresi kullanılmıştır. Bu entegre devre, üç tek kutuplu çift düzenlemeli anahtarlara sahiptir. Fakat bu anahtarlardan sadece iki tanesi bu tasarımda kullanılmıştır. Bazı korsan düzeltici tasarımlarında, 4053 entegresinin yerine bir adet 4066 entegresi ile iki adet invertör kullanılmıştır.

İkinci çoklayıcı anahtarının çıkışı video amplifikatörünü beslemektedir. Bu amplifikatör, TDA1034 veya LM318 op-amp'tır. TDA1034 entegresinin çıkışı, push-pull amplifikatöre taşınmıştır. Korsan düzeltici tasarımlarının büyük bir kısmında video amplifikatörü kısmının tamamı, ikinci çoklayıcı anahtarının çıkışında bulunan tek transistörlü bir emitör takipçisi ile değiştirilmiştir [1].

3.10.2.5 Senkronizasyon üreteci devresi

Devresinin senkronizasyon üretici kısmı, sandcastle kontrol sinyalini ve LI kontrol sinyalini üretmek için kullanılmıştır. Bu, karıştırılmış videodan gelen senkronizasyonları çıkarmakta ve bunları bir satır osilatörünün faz kilitlemesinde kullanmaktadır.

Şekil 3.29'da gösterilmiş olan devre, standart bir televizyon yatay senkronizasyon devresidir. Bu devre, amatör kişilerin yapacağı korsan düzelticiler için oldukça masraflıdır. Bu yüzden bu devrenin yerine, bir senkronizasyon sıyırıcı ve bir tekkararlı kombinasyonu yaygın bir şekilde kullanılmıştır [1].



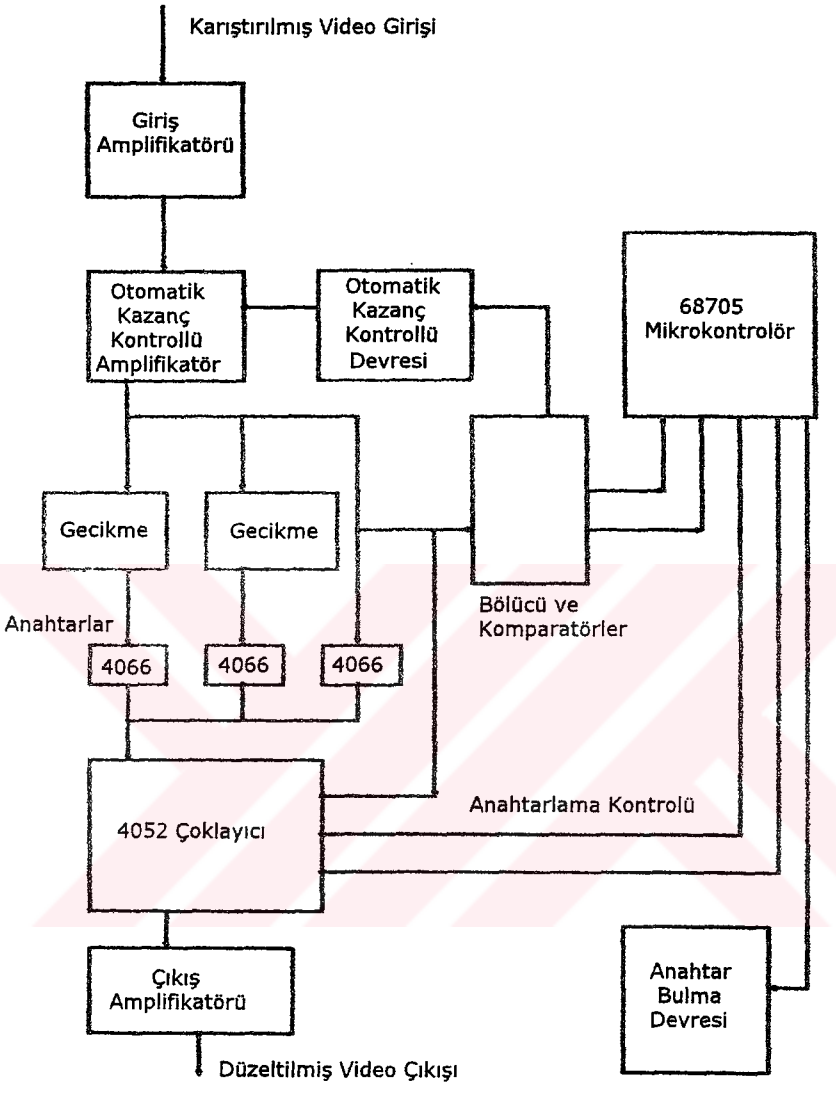
Şekil 3.29 Radio Plans Discret senkronizasyon üreteci devre tasarımı [1]

3.10.3 Hi-Tech Discret düzeltici tasarımı

Hi-Tech Discret düzeltici tasarımı (Şekil 3.30), mikrokontrolör bazlı bir tasarım ile neler yapılabileceğini gösteren en iyi örneklerden biridir. Bu tasarım, 68705 EPROM tipi bir mikrokontrolör kullanmaktadır. Discret sistemi, her bir satırdaki videoyu 0 ns, 902 ns ve 1804 ns'lik gecikmelerden biri ile geciktirerek çalışmaktadır. Standart sinyal düzeltici metoduna Radio Plans tasarımı öncülük etmiştir [1]. Bu metot, videonun başlangıcındaki siyah düzeyindeki yükselmeyi bulmayı gerektirmektedir. Eğer video geciktirilmemişse, iki gecikme birimi ilave edilmektedir. Eğer video bir birim ile geciltirilmişse, o zaman diğer gecikme birimi ilave edilmektedir. Eğer video iki birim ile geciktirilmişse, o zaman video doğrudan kapılanmaktadır. Bu, ekranın sol tarafında siyah bir bant yaratmaktadır. Fakat televizyonların büyük bir kısmında bu siyah bant overscan ile kaybedilmektedir [1].

Siyah düzeyinden yükselişi bulma çalışmalarındaki problem, televizyon kanalı tarafından

buna karşı tedbir alınmasının çok kolay olmasıydı. İlk Radio Plans bazlı korsan düzelticileri kullanım dışı bırakmak için Canal Plus'ın yaptığı tek şey, gecikme alanına siyahtan başka bir düzey eklemekti [1]. Bundan dolayı korsan düzelticiler siyah düzeyini bulamayacak ve bu yüzden tespit etme devreleri başarısız olacaktı.



Şekil 3.30 Hi-Tech Discret düzeltici blok diyagramı [1]

Hi-Tech firması, video düzeltici kısmını muhafaza etti ve gecikmeleri slotlamak için farklı bir metot kullandı. Sinyali düzeltmek için gerekli olan veri, düşey karartma aralığı satırlarının birinde iletilmektedir. Bu bilgiyi kullanarak ve bunu 68705 mikrokontrolörü ile işlemden geçirerek, siyah düzeyindeki yükselmeyi tespit etmeksizin gecikme satırlarını ayarlamak mümkündür. Bu düzeltici iki bölümden oluşmaktadır. Bu bölümler video sıyırma ve mikrokontrolör bölümleridir.

3.10.3.1 Düzelticinin video sıyırma bölümü

Video sıyırıcının giriş kısmı, iki transistörlü bir tasarımdır. Bir FET, otomatik kazanç kontrolü sağlayan bir değişken kazanç direnci olarak konfigüre edilmiştir. Bu, veri ve senkronizasyon sıyırma için önemlidir. Otomatik kazanç kontrolü, video amplifikatörünün girişine uygulanmıştır. Bu amplifikatörün çıkışı tamponlanmaktadır ve bu çıkış, gecikme satırlarını beslemektedir.

Sinyali düzeltmek için üç video sinyali gerekmektedir. Bunlar; geciktirilmemiş bir video sinyali, bir gecikmeli video sinyali ve iki gecikmeli video sinyalidir. Sinyaller boyunca sabit bir genliği korumak için sıfır gecikme ve iki gecikme zincirlerine iki ön ayar dahil edilmiştir. Tek bir son verici direnç, bir gecikme zincirine dahil edilmiştir. Video sinyalleri arasında anahtarlama, üç adet 4066 anahtar entegresi ile sağlanmaktadır. Bu anahtarların herbirinin çıkışı bir 4052 çoklayıcı entegresinin girişlerinden birini beslemektedir. 4052 çoklayıcı entegresi, senkronizasyon ve video sinyalleri arasındaki anahtarlamayı kontrol etmektedir. Düzeltilmiş video, iki katlı bir transistörlü tamponu beslemektedir. İkinci transistörün emiterindeki 1.0 kΩ'luk ön ayar direncinden video çıkışı elde edilmektedir [1].

3.10.3.2 Düzelticinin mikrokontrolör bölümü

Bu tasarımda kullanılmış olan mikrokontrolör 68705 entegre devresidir. Bu, güvenliği olan bir EPROM versiyonudur. Kristal frekansı 4.0 MHz'dir [1]. Kontrol sinyalleri, bir bölücü ve komparatör takımı tarafından videodan elde edilmektedir. Bu komparatör, video sinyalinden veriyi sıyırmakta ve mikrokontrolörü beslemektedir.

İkinci komparatör, otomatik kazanç kontrolü bir komparatörüdür. Bu komparatör, 4538 tekkararlı entegresini tetiklemektedir. Bu tekkararlı, karartma düzeyini örnekleyen 1 μs'lik bir pencere yaratmaktadır. Kapılanmış bir komparatör, sinyali örnekleyerek çıkışı tümleşik yapmakta ve TL081 otomatik kazanç detektörü amplifikatörünü beslemektedir. Bu yolla video sinyalinin genliği sabit kalmaktadır. Bu, voltajlar belirtilenden farklı olduğunda doğru olarak çalışmayan bölücü-komparatör zinciri gibi bir kod çözücü türü için önemli bir gereksinimdir [1].

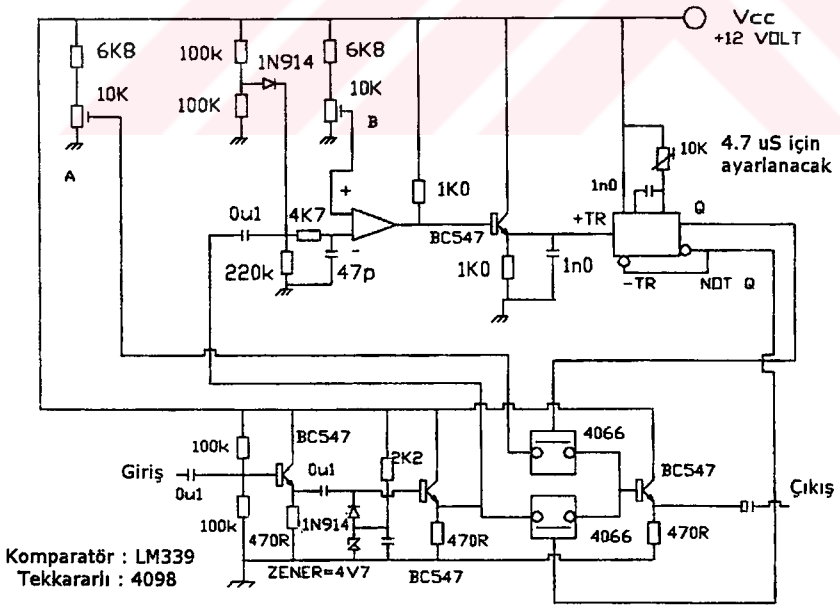
Üçüncü komparatör, senkronizasyon sıyırıcıdır. Bu, mikrokontrolöre bir senkronizasyon treni sağlamaktadır. Böylece, veri çıkarmak için doğru satırlar seçilebilmektedir. Bu mikrokontrolör, 4052 çoklayıcı entegre devresine anahtarlama kontrol sinyallerini sağlamaktadır. Anahtarlama kontrol sinyalleri, düzeltilmiş video ile uygun senkronizasyon

sinyallerini birleştirmektedir. Bir kilit tespit etme devresi, bu mikrokontrolör tarafından çalıştırılmaktadır. Bu devre, SCART kontrol devre yapısına bir düzeltici seçme sinyali göndermektedir.

3.10.4 EBU senkronizasyon yenileyici tasarımı

EBU iletim formatlı sistem, bir uydu iletim sisteminde gücü en üst düzeyde kullanmak için tasarlanmıştır. Normal bir uydu iletiminde ses, 5 MHz ile 8 MHz arasındaki menzilinde bir alt taşıyıcı üzerinden iletilmektedir [1]. Bu durum, mevcut gücün bir kısmını harcamaktadır. EBU sisteminde ise ses, video dalga biçiminin içine konularak mevcut güç ekonomik olarak kullanılmıştır. Yani, EBU iletim formatı sadece bir video dalga biçimidir. Bunun bir sonucu olarak, bir ses alttaşıyıcısı için kullanılması gereken güç artık video için kullanılabilecektir.

EBU sound in synch sistemi aslında darbe kodlu modülasyonlu bir PAL 625 sinyalidir. Veri, yatay senkronizasyon kısmına sokulmuştur. Darbe kodlu modülasyon verisi, bazı monitörlerin ve televizyonların senkronizasyon sıyırıcı devre yapısının şaşırmasına sebep olmaktadır. Bu durum, verinin sürekli değişme özelliğinden dolayı ortaya çıkmaktadır. Senkronizasyon detektörü, temiz bir darbenin gelmesini beklemektedir. Fakat bunun yerine karışık bir darbe kümesi almaktadır. Fakat kenar tespit etme yöntemi kullanan bazı televizyonlarda ve monitörlerde hiçbir problem çıkmamaktadır.



Şekil 3.31 EBU senkronizasyon yenileyici devre yapısı [1]

Bu sistemde videoyu yeniden elde etmek, karıştırılmış sinyaldeki yatay senkronizasyon darbesi alanını yeni bir uygun şekilde zamanlanmış yatay senkronizasyon darbesi ile

değiştirmeyi gerektirmektedir. Şekil 3.31'de gösterilmiş olan devre tasarımı bu sistem hakkında bir fikir vermektedir. Buradaki devre elemanları test edilmiş ve düzeltici tasarımlarında kullanılmıştır [1].

Bu çalışma şekli için birkaç devre elemanı gerekmektedir. İlk olarak, bir senkronizasyon sıyırıcı gerekmektedir. Bu bölümde daha önce bahsedilmiş olan komparatör tipi, bu devrede kullanılmıştır. İkinci devre elemanı, bir tekkararlı entegre devresidir. Bu tekkararlı, dijital veriyi anahtarlamak için gerekli olan zamanlama darbesini sağlamakta ve senkronizasyon tepesi için sabit bir düzeyi yeniden eklemektedir.

Üçüncü kısım ise video kısmıdır. Video kısmının giriş sinyali, tespit edilmemiş video sinyalidir. Bu video sinyalinin, uygun işlemlerden geçirilebilmesi için tespit edilmesi gereklidir. Bunun için kullanılmış olan devre, basit bir uydu televizyon alıcı devresidir. Kullanılmış olan zener diyotun voltaj sınıfı 4.7 V'tur. Tespit edilmiş olan video sinyali iki adet 4066 kapı entegre devresi içeren çift kutuplu bir anahtarı beslemektedir. Bu elektronik anahtarın görevi, videonun kapılanmasını ve dijital verinin değiştirilmesini sağlamaktır. Video anahtarı, dijital sesin peryodu hariç olmak üzere normalde kapalıdır. Dijital ses kapısı ise normalde açıktır. Fakat dijital ses peryodu için kapalıdır. Bu kapı, senkronizasyon tepe voltajını ayarlayan ön ayarlı bir dirence bağlıdır.

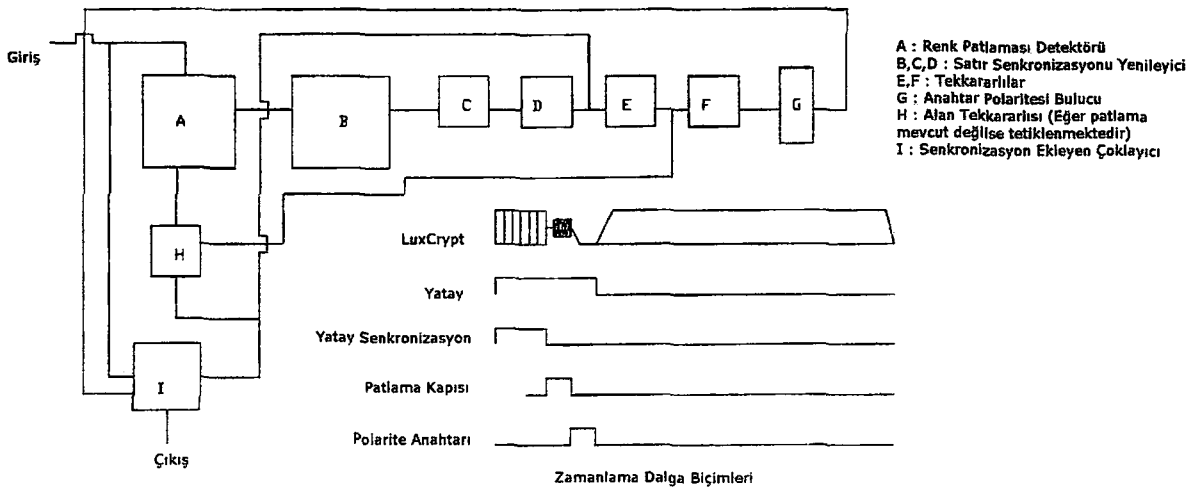
Bu iki kapının (gate) çıkışları bir tampon transistöre bağlanmıştır. Transistörlü amplifikatörün çıkışı, dijital ses olmaksızın videoyu tespit etmektedir. Bir alan darbe detektörünü ve sinyalin alan darbe kapısındaki kapılama tetiklemesini durdurmak için bazı lojik elemanların ilave edilmesi gerekebilmektedir.

3.10.5 LuxCrypt sistemi düzeltici tasarımı

IRDETO sisteminin patenti 1982 yılında alınmıştır [1]. Bu sistem, OAK Orion sisteminin atasıdır. Bu sistemin patent bilgileri incelenirse, sistemin en yıldırıcı özelliğinin dijital ses olduğunu görülür. RTL4-V kanalı tarafından kullanılmış olan karıştırıcı sistem LuxCrypt sistemidir ve bu sistem IRDETO sisteminin bir uyarlamasıdır.

Bu sistem gücünü videoyu karıştırmak için senkronizasyon darbelerinin yenilenmesini kullanmadan almaktadır. Karıştırılmış video sinyalinde senkronizasyon darbeleri olmadığı zaman televizyon alıcısı görüntüyü kilitleyememektedir. Digisynch ve PDS Synch Generator gibi eski senkronizasyon üreteci düzelticileri, karıştırılmış olan IRDETO sinyalini gerçek formatına kilitleyebilmektedir.

LuxCrypt sistemi gücünü aktif video inversiyonundan almaktadır. Patent şartnamesinde birkaç değişik video inversiyonu tipi verilmiştir. 1990 yılı Ocak ayında gerçekleştirilen terfide kullanılmış olan video inversiyonu, Ortalama Tepe Düzeyi'dir [1]. Bu inversiyon tipi, eğer bir sahnedeki beyaz veya siyah miktarı önceden ayarlanmış olan bir değeri geçerse video polaritesini değiştirmektedir. İnversiyonlar arasındaki en kısa süre üç saniyedir.



Şekil 3.32 LuxCrypt düzelticisinin blok diyagramı [1]

Piyasada mevcut olan korsan düzelticilerin büyük bir kısmı her bir alanın başlangıcındaki videonun polaritesini tespit etmektedir. Bu yüzden bu tip inversiyon kullanımı en iyi metot değildir. Her bir satırda bir polarite anahtarı vardır. Orijinal düzeltici, ucuz maliyetli bir ünite olduğu için karıştırılmış videodaki siyah düzeyini yeniden yerleştirmek için bazı özelliklere ihtiyacı vardı. Bu polarite biti, böyle bir yeteneği temin etmekteydi.

Renk patlaması, video sinyalindeki diğer bileşenlere bağlı olarak zamana göre değişmemektedir. Bu yüzden kullanışlı bir referanstır. Temel düşünce, akortlu bir devre kullanılarak renk patlamasının tespit edilmesi ve bunun 4046 veya TBA920 gibi bir faz kilitlemeli çevrimi senkronize etmek için kullanılmasıdır. Korsan SRP1000 tasarımının (FilmNet düzelticisinin üçüncü terfisi için geliştirilen düzeltici), akortlu devrenin çıkışında bir tepe detektörü veya komparatör kullanarak, bu şekilde kullanım için adapte edilmesi mümkündür. Akortlu devrenin çıkışı, renk patlamasının sonunda maksimum değerine ulaşmaktadır.

Alan senkronizasyonu, renk patlamasının sayısını hesaplayarak veya birtakım tekkararlıları tetikleyerek yeniden yaratılabilmektedir. Alan darbesini pozisyonlandırmak için iki tekkararlı kullanılmaktadır.

Video polaritesini saptamak için prosedür üç adıma ayrılabilir. Bunlar;

1) Renk patlaması tespit edilmesi ve bunların zamanlama referansı olarak kullanılması

2) Patlamanın (karartma düzeyinin) örneklenmesi

3) Polarite anahtarının örneklenmesi

Eğer patlama düzeyi polarite anahtarı düzeyinden daha yüksekse, bu durumda video polaritesi normaldir. Eğer patlama düzeyi polarite anahtarı düzeyinden daha düşükse, bu durumda video polaritesi terstir. Eğer patlama düzeyi polarite anahtarı düzeyine eşitse, bu durumda sinyal karıştırılmamıştır.

Faz kilitlemeli çevrimli FilmNet düzeltici tasarımında kullanılmış olan 2 MHz'lik faz kilitlemeli çevrim, bu uygulamada kullanmak için uyarlanabilir. Temel değişiklik, sayıcının çıkışındaki yatay karartma kod çözücüsünde olacaktır. Renk parlaması tepesini bulmak için bir komparatör kullanılır. SRP1000 korsan düzeltici tasarımındaki gibi bir örnekleme kapısı devresi, yanlış tetiklemelerin bazılarını eleyecektir.

RTL-5 kanalı, ASTRA 1-C uydusu üzerinden LuxCrypt sistemine benzeyen bir sistem kullanarak yayın yapmaktadır. Bazı eski korsan düzelticiler sinyali kilitleyememektedir. Bu durum, bu sistemin Ortalama Tepe Düzeyi inversiyonunu kullanmış olduğunu göstermektedir.

3.10.5.1 Hi-Tech Galaxy RTL4-V düzeltici tasarımı

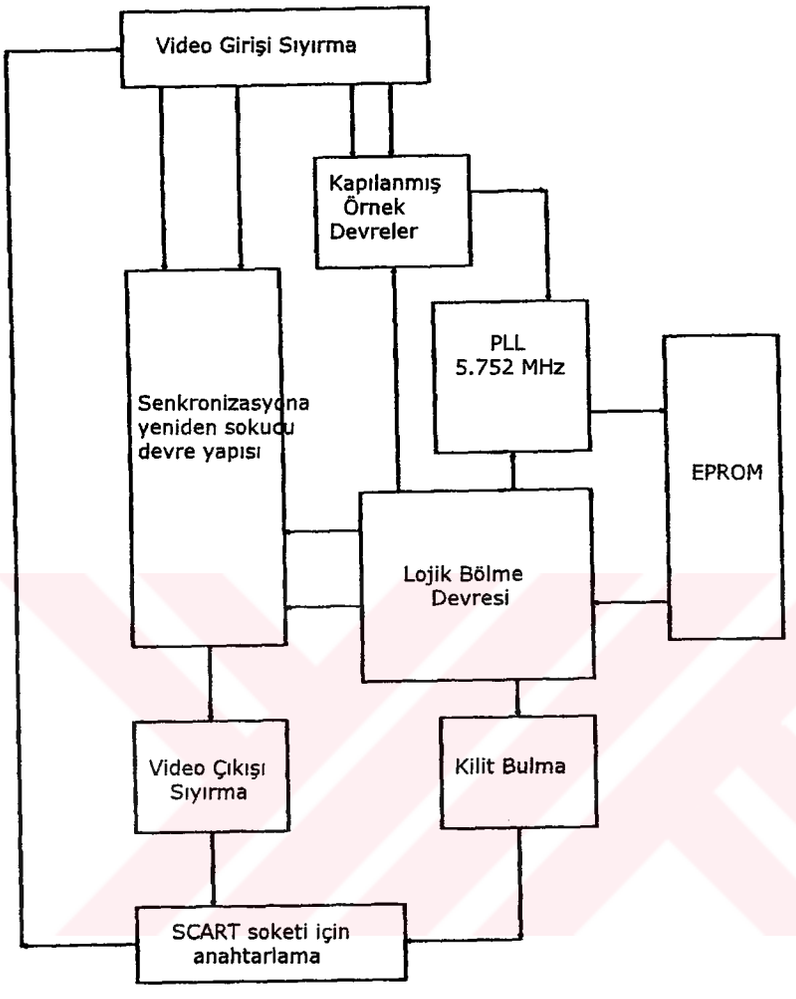
Bu korsan düzeltici, RTL4-V kanalının kullanmış olduğu LuxCrypt sistemi için tasarlanmış olan bir düzelticidir. LuxCrypt sisteminde gerçekleştirilmiş olan sistem minimum özelliklere sahipti. Bu sistem, IRDETO sisteminin bir türevidir. IRDETO sisteminin en etkili özelliği olan ses karıştırıcı yaklaşımı, bu sistemde kullanılmamıştır [1].

RTL4-V kanalının bilgisayar korsanlarının ilgisini çekmesinin sebebi, karasal yayın yapan televizyon kanallarının büyük bir kısmını göstermesiydi. LuxCrypt sistemi, gerçek anlamda hiçbir ciddi koruması olmayan bir karıştırıcı sistemdi. Korsan RTL4-V düzelticisi, faz kilitlemeli çevrim esasına dayanan bir tasarımdır. Temel olarak üç kısımdan oluşmaktadır. Bu bölümler video girişi sıyırma, faz kilitlemeli çevrim ve video çıkışı sıyırmadır.

1) Video girişi sıyırma

Video girişi sıyırmanın ilk kısmında, baseband girişini kuvvetlendirmek için iki ayrı transistörlü amplifikatör kullanılmıştır. İkinci amplifikatörün giriş düzeyi, ilk amplifikatörün

çıkışındaki 500 Ω'luk bir ön ayar direnci ile kontrol edilmektedir. İkinci amplifikatörün çıkışı, video bantgeçiren bir filtreyi beslemektedir. Bu filtrenin çıkışı tamponlanmıştır ve eviren ve evirmeyen bir tamponu beslemektedir. Bu, sinyali düzeltmek için gerekli olan normal ve ters çevrilmiş video sinyallerini sağlamaktadır.



Şekil 3.33 RTL4-V düzelticisinin blok diyagramı [1]

2) Faz kilitlemeli çevrim

Faz kilitlemeli çevrimin gerilim kontrollü osilatör kristali, yaklaşık 5.752 MHz'lik bir kristaldir. Bir 74HC04 Hex Schmitt invertörün iki kapısı kullanılmıştır. Faz komparatörü anahtarlı bir tiptir. Anahtar, bir 4066 kapı entegre devresidir ve osilatör çıkışı (CLK5M7) ve örneklenmiş clock sinyali arasında anahtarlama yapmaktadır.

Yatay ve düşey zamanlama, lojik devrenin farklı kısımları tarafından üretilmektedir. Alan zamanlaması, 27256 EPROM'u etrafında inşa edilmiş olan yatay zamanlama kısmını tetiklemek için ve kod çözücü seçimi kontrolünü tetiklemek için kullanılmıştır. Düzelticinin en önemli kısmı 27256 EPROM'dur. Faz kilitlemeli çevrim, EPROM'daki adreslemeyi

kontrol eden iki sayıcı entegresini clock'lar. EPROM çıkışlarında birtakım sayıcı ve kombinasyonel lojik kullanılarak, sinyali düzeltmek için gerekli olan örnekleme ve kontrol slotlarını üretmek mümkündür.

3) Video çıkışı sıyırma

Video çıkış katı, Pink And Brown Book kitabında yayımlanmış olan OAK Orion korsan düzeltici tasarımına çok benzemektedir [1]. Clock örneklemesini ve tespitini gerçekleştirmek için 4066 anahtar (switch) entegre devreleri kullanmaktadır. Tespit etme işlemi, senkronizasyon darbelerini ve düzeltilmiş videodaki karartma düzeyini yeniden kurmak için gereklidir. Bu çalışma şekli için anahtarlama, bir 4051 entegre devresi ile sağlanmaktadır. Video çıkışı tamponlanmakta ve daha sonra çıkışı beslemektedir.

Bu düzelticideki konnektörler, diğer Galaxy tipi düzelticilerde kullanılanlar ile aynıdır [1]. İki SCART konnektörü ve iki ses (hoparlör) çıkışı vardır. Çevrim ve anahtarlama, bir faz kilitlemeli çevrim tarafından kontrol edilmektedir. Ayrıca bu tasarımda, bir röle de kullanılmıştır.

4) Güç kaynağı

Güç kaynağı, 15 Volt'luk bir transformatörü besleyen bir köprü doğrultucu kullanmaktadır. Bu köprü doğrultucudan önce 1 A'lik bir sigorta kullanılmıştır. Gücün mevcut olup olmadığının görülmesi için ise bir LED kullanılmıştır.

7812 ve 7805 regülatör entegre devreleri, +12 V ve +5 V'luk besleme gerilimlerini sağlamak için kullanılmıştır. Her bir regülatör entegre devresi, kendisine ait 470 nF'lık bir depolama kondansatörüne ve 470 nF'lık bir dekuplaj kondansatörüne sahiptir [1].

3.11 Güvenli Mikrokontrolörlerin İçeriklerinin Okunması

Güvenliğin kaldırılması, bir hack işleminin sonucunda ortaya çıkmaktadır. Bu genellikle, yazılımdan çok donanımdan kaynaklanmaktadır. Bunun sebebi, inceleme altında olan elemanın genellikle bir mikrokontrolör olmasıdır.

Güvenliğin kaldırılması işlemi için kullanılan tabir "popping"dir. Bunun kökeni, elektronik cihazların tamir edilmesi işinden gelmektedir. Bir ünitenin tamir edilmesi gerektiği zaman muhafazasının veya kapağının kaldırılması gereklidir. Bu nedenle bu ünitenin kapağı kaldırılır (pop). Mikroçipin silikon kalıbına erişimin sağlanması için temel teknikler, mikroçipin üst kısmını kaldırılmayı gerektirir.

Yazılım teknikleri mevcut olduğu zaman en sağlam ve en tehlikeli teknikler, silikon mikroçipin etrafını saran maddenin kaldırılmasını esas almaktadır. Bunu gerçekleştirmenin en iyi yolu, Sülfürik veya Nitrik asit gibi kuvvetli asitler kullanmaktır. Fakat bu, gerekli tedbirlerin alınmasının şart olduğu aşırı derecede tehlikeli bir prosedürdür.

Bu konu ile ilgili internet sitelerinde ve BBS'lerde mevcut olan bazı dökümanlarda, akü asidini kaynatarak bu işlem için gerekli olan sülfürik asidin daha saf bir formunun elde edileceğinden söz edilmektedir. Fakat asidi kaynatmak aşırı derecede tehlikelidir. Çünkü kaynatırken zehirli bir duman açığa çıkmaktadır. Sülfürik veya Nitrik asitleri de kaynatırken bu durum ortaya çıktığı taktirde bu duman öldürücü olabilmektedir. Nitrik asidin kuvvetli çözeltilerinde açığa çıkan buhar, solunum sistemini tahriş etmekte, deriyi ve gözleri yakabilmektedir. En kötü durum ise, bu konsantre buhardan ciğerlere birkaç defa çekildiğinde bu durumun öldürücü olabilmesidir [1].

Bu zehirli dumanın çalışılan alandan atılması gereklidir. Uygun bir biçimde donatılmış olan bir laboratuarda, bu işi bir duman dolabı (cupboard) kullanarak gerçekleştirmek mümkündür. Bu tür bir hack işlemi ev ortamında gerçekleştirilebilecek bir işlem değildir.

Sülfürik asidi kaynatarak daha kuvvetli ve daha konsantre bir asit formu elde etme işi aşırı derecede tehlikelidir. İlgili internet sitelerinde ve BBS'lerde mevcut olan bazı dökümanlarda bu asidin, pyrex bir kabın içinde sülfür diyoksitin beyaz dumanı açığa çıkıncaya kadar kaynatılması gerektiği söylenmektedir. İşte açığa çıkan bu zehirli gazın çalışılan ortamdan mutlaka atılması gereklidir [1].

Bu prosedür, bir PIC16C57 entegresinde silikon kalıp görülünceye kadar bir deliğin açılmasını gerektirmektedir. Daha sonra, hipodermik bir şırınga ile bu konsantre Sülfürik asidin az bir miktarının açılan bu deliğe konulması gereklidir. Bu asit, silikon kalıbın üzerindeki arta kalan maddeleri çözmesi için birkaç dakika burada bırakılır. Daha sonra bu mikroçip, asidi atmak ve nötrleştirmek için aseton ile temizlenir. Bundan sonra, yaklaşık olarak beş inçlik bir uzaklıktan ultraviyole silici ile bu mikroçipin üzerindeki sigortaların resetlenmesi mümkündür [1].

Çoğu durumda, mikroçipin silikon kalıbının etrafındaki maddenin bu şekilde temizlenmesi gerekli değildir. Güvenli ROM, EPROM veya EEPROM'lara standart olmayan gerilim ve/veya standart olmayan zamanlama kullanarak erişim sağlamak için kullanılabilecek çok daha basit hack işlemleri vardır.

Son birkaç yıl içinde, belirli mikroçiplerin güvenli olduğu iddiası ortadan kalkmıştır. Bu

endüstri geliştikçe, hack işlemini televizyon kanallarına ve diğer bilgisayar korsanlarına karşı güvenli hale getirmek için süregelen çalışmalar vardır. Bunun sonuçları bazı durumlar için tam bir felaketti. Bunun en iyi örneği, PIC16C84 mikroçipinin güvenliğinin nasıl kaldırılacağına dair bilgilerin internet sitelerinde ve BBS'lerde mevcut olmasıydı.

Analog sistemlerde kullanılmak için düzeltici tasarımlarının yaygın olduğu zamanlarda, mikroçipin güvenliğini kaldırılma teknikleri önemli hale geldi. FilmNet, Teleclub ve RTL4-V kanalları düzelticilerinde mikrokontrolör kullanmaya başlamıştı. En yaygın olarak kullanılmış olan mikrokontrolör, 8051 ve bunun EPROM versiyonu olan 8751'di. Düzeltici üreticileri, bu mikroçipin içindeki kodların kopyalanabileceği olasılığından dolayı endişeliydi. Bu yüzden düzelticilerde, sadece bir defa programlanabilen (OTP: One Time Programmable) EPROM versiyonlarını kullanmışlardır. Sistemlerin büyük bir kısmı oldukça ilkel olduğu için doğal olarak düzelticilerde analog yöntemler hakimdi.

1993 yılı başlarında ilk Ho Lee Fook mikroçipi kullanılmaya başlanmıştır. Başlangıçta bu mikroçipin orijinal VideoCrypt düzelticisindeki 8052 ile değiştirilmesi amaçlanmıştı. Bu şekilde, akıllı kartsız VideoCrypt düzelticisi yaratılabilecekti. Bu mikroçipler, 8752 ve 8751 mikrokontrolörlerini baz almaktadır.

3.11.1 8752/8751 Futuretron mikrokontrolörlerinin içeriğinin okunması

Bu hack işlemi için kullanılan program, Futuretron mikroçiplerini hack etmek için assembler dilinde yazılmış olan orijinal programlardan biridir [1]. VideoCrypt 07 versiyonunda gerçekleştirilmiş olan Futuretron hack işlemi, 8752 ve daha sonra da 8751 mikroçipini baz almıştır. Kullanılmış olan bu mikroçip, sadece bir defa programlanabilen versiyondu. Bu mikroçipin bir defa programlanabilen versiyonu ile EPROM versiyonu arasındaki tek fark, mikroçipin tekrar programlanabilmesi için EPROM versiyonunda quartz bir cam pencerenin bulunmasıdır.

Mikroçipin üst kısmının fiziksel olarak çıkarılması ve konvansiyonel teknikler kullanarak sigortaların resetlenmesi mümkündür. Fakat, mikroçipin güvenlikli EPROM'undaki bilgileri elde etmek için daha basit ve daha az karmaşık metotlar vardır.

Bu hack etme programı, mikrokontrolörü kandırarak bir an için harici EPROM'a anahtarlaması, rutini okuması, tekrar dahili EPROM'a geri anahtarlaması ve rutini uygulamaya koyması için MOV a, @DPTR komutlarını kullanmaktadır. Bu rutin, güvenlikli EPROM'un içeriğini seri porttan dışarıya atmaktadır. Bu hack işlemi şu prosedürde

çalışmaktadır:

1) Mikrokontrolör, dahili EPROM ile çalıştırılır (boot).
2) Mikrokontrolör dahili EPROM'da çalıştığı zaman, entegrenin EA bacağı harici EPROM'u seçmek için anahtarlanır.
3) Daha sonra mikrokontrolör, 200h'ta EPROM'dan bu rutini okur ve güvenlikli EPROM'un içeriğini seri porttan dışarı atar.
4) Bir terminal programın çalıştırıldığı bir bilgisayar, bu seri portun çıkışını kaydeder.

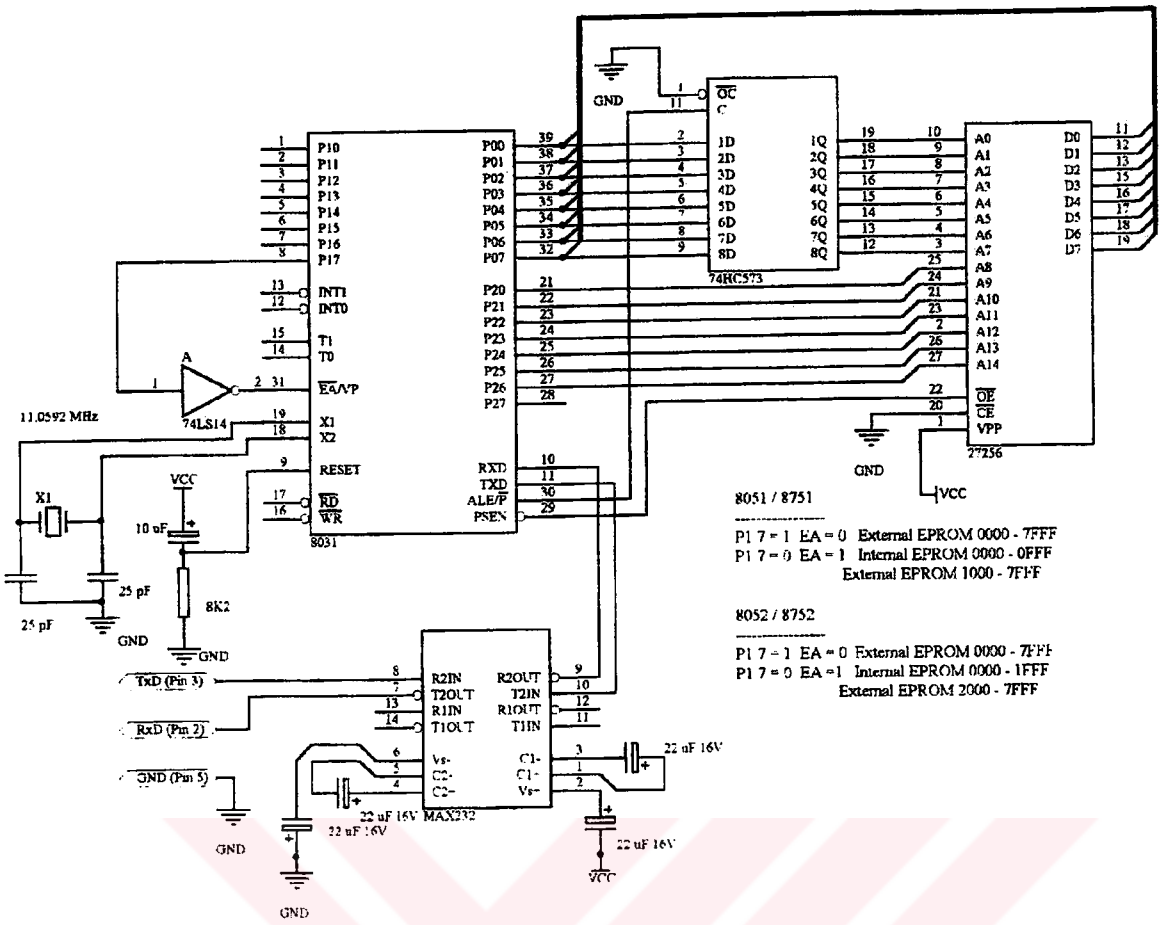
Bu hack işleminde, bir 8052/8051 geliştirme bordunun kullanılması gereklidir. Bu hack işleminde kullanılan HACK.ASM isimli program derlenir ve bir EPROM'a yüklenir. Bu EPROM ve okunmak istenen mikroçip geliştirme borduna yerleştirilir ve ünite açılır. Daha sonra bilgisayardaki terminal program, yakaladığı güvenlikli EPROM'un içeriğini daha sonra kaydetmek ve çevirmek üzere bir kütüğe (log) atamaktadır.

Farklı mikrokontrolör türleri için buna benzer hack işlemleri de mevcuttur. Seksenli yılların sonunda ve doksanlı yılların başında en popüler hack işlemlerinden biri, benzer özelliklere sahip olan 68705 mikroçipi için gerçekleştirilmiştir.

3.11.2 8051/8052 mikrokontrolörlerinin içeriğinin okunması

Bu hack işleminin daha verimli bir versiyonu, bu konu ile ilgili internet sitelerinde ve BBS'lerde uzun zamandan beri mevcuttur. Kodlama çok verimli hale getirildiği için display rutinlerine sahip değildir. Ayrıca önceki hack işlemine nazaran daha iyi dökümantasyona sahiptir [1]. Ayrıca güvenliği kaldırmak için kullanılan elektronik devre diyagramı da verilmiştir (Şekil 3.34).

Bu EPROM kopyası bir 27C256 için geçerlidir. Bu devre, 74HC573 mikroçipini kullanmaktadır. Devrenin besleme gerilimi 5 V'tur ve Vcc bacakları ve besleme dekuplaj kondansatörleri gösterilmemiştir. Temel olarak rutinler, bir önceki örnektekiler ile benzerdir. Bu, daha açık ve daha etkili bir yaklaşım olduğu için bir önceki örnekteki gibi display rutinlerini içermemektedir.



Şekil 3.34 8051/8052 mikrokontrolörlerinin içeriğinin okuyan devre [1]

3.11.3 PIC16C84 mikrokontrolörünün içeriğinin okunması

PIC16C84'ün EEPROM'u, kod koruma özelliği ile güvenli hale getirilmiş olmasına rağmen EEPROM'un içeriğinin okunabilmesine izin veren bir tasarım hatasına sahipti [1]. Başlangıçta bu bilgi çok sıkı gizlenmişti ve herkes tarafından bilinmiyordu. Fakat 1995 yılının Nisan ayında, PicBuster prosedürünün detayları internet üzerinde yayımlandı [1]. Bunun üzerine, PIC16C84 için düşüş başlamıştır. İnternet üzerinde yayımlanmış olan bu bilgi sonucunda, PIC16C84'ün güvenliğinin nasıl kaldırılacağı herkes tarafından öğrenilmiş oldu. Bunun sonucunda, VideoCrypt 09 ve D2-MAC sistemlerinde gerçekleştirilen her hack işlemlerinin kodlaması birkaç gün içinde internet sitelerinde ve BBS'lerde birikmeye başlamıştı. Bu yüzden artık PIC16C84 hakkında hiçbir gizli bilgi kalmamıştır [1].

Bir PIC16C84'nin kodlamasını okumanın standart metodu, mikroçipin üst kısmını açarak koruma sigortalarını devre dışı bırakmaktır. Bu teknik başlangıçta, PIC16C54 ve PIC16C57 gibi PIC mikrokontrolörlerinin sadece bir defa programlanabilen EPROM versiyonlarında kullanılmıştır. Bu mikrokontrolörler EPROM versiyonu olduğu için PicBuster metodu bu

mikroçiplerde çalışmamaktadır. Bununla birlikte PIC16C84 mikroçipi bir EEPROM kullanmaktadır.

Genellikle, PicBuster gibi teknikler mikroçipi belirtilen maksimum sınırlarının üzerine çıkmaya zorladığı için bu tekniklerin çalışmayacağı düşünülmekteydi. Koruma sigortaları resetlemenin standart sonucu, PIC16C84'ün belleğinin tamamının resetlenmesidir. Normal programlama modunda, programlama voltajıyla (yaklaşık 13.8 V) besleme voltajı (5 V) arasında büyük bir fark vardır.

PicBuster tekniğinde, programlama voltajıyla besleme voltajı arasındaki fark yaklaşık olarak 0.6 V'tur. Diyotun uçları arasındaki gerilim düşümü 0.6 V ile 0.7 V arasındadır. Bu 0.6 V'luk voltaj farkı belleğin tamamını resetlemek için yeterli olmayabilmektedir. Fakat, konfigürasyon sigortalarının resetlenmesini sağlamak için yeterlidir. Bu konfigürasyon sigortaları ilk önce resetlenmesi gereken sigortalardır [1].

Mikroçipi okuma işlemi oldukça basittir. Koruma sigortası yeniden yazıldığı için mikroçip belleği okunabilmektedir. Bu sırada programlayıcı cihaz bir hata mesajı verecektir. Fakat bu mesaj önemli değildir. Koruma sigortası üzerine yazma işleminin birkaç defa yapılması gerekmektedir.

PicBuster tekniğiyle işleme tabi tutulan mikroçiplerde bazı problemler gözlemlenmektedir. Bu mikroçipleri yeniden programlanması denenirken, silme prosedürü bellek içeriğini tamamen silmediği için programlama başarısızlıkla sonuçlanabilmektedir. Daha sonra, programlama voltajı 5 V'a resetlenir ve programlayıcı cihaz kapatılır. Bir süre sonra programlayıcı açılır ve mikroçipin belleğinin içeriği okunur. Bu işlem görüldüğü gibi oldukça basittir.

Korsan düzeltici endüstrisinde kullanılmış olan PIC16C84 programlayıcılarının büyük bir kısmı, mikroçipi programlamada seri metodu baz almaktadır. Birkaç programlayıcı tasarımı kullanılmıştır. Bunların en popüler olanları Henk Schaer ve David Tait tasarımıdır. Bu tasarımlar, uydu televizyonları ile ilgili olan internet sitelerinde ve çoğu BBS'te mevcuttur. Her iki tasarımın da yapılması kolay ve fazla masraflı değildir [1].

PIC16C84, hala yaygın bir şekilde kullanılmaktadır. Otomobillerdeki kapı kilitlerinin kontrol edilmesi gibi bazı uygulamalarda da kullanılabilmektedir. 1994 yılında İngiltere'de bir mahkeme duruşmasında bir kişi, elektronik anahtarlardan RF verisini yakalayan ve bu veriyi kilitleri açmak için okuyan bir cihaza sahip olduğu için suçlanmıştı [1].

Arizona Microchip, PicBuster tekniğinin çalışmasını engellemek için PIC16C84 kalıbında bazı modifikasyonlar gerçekleştirmiştir. Bu mikroçipin yeni versiyona PIC16C84A ismi verilmiştir. Bununla birlikte, bu hack işlemine karşı savunmasız olan çok miktarda korsan PIC16C84 bazlı akıllı kart mevcut olduğu için bu modifikasyon işe yaramamıştır. Ayrıca, bu mikrokontrolörü kullanan D2-MAC EuroCrypt-M kartları, PIC16C84'ün perakende satış fiyatından daha ucuza satılmaktaydı [1].

4. AKILLI KARTLAR ve UYGULAMA ALANLARI

İlk çıkan karıştırıcı sistem tasarımları, içine yerleştirilmiş güvenli mikrokontrolör prensibini baz almaktaydı. Fakat akıllı kart yaklaşımının ortaya çıkmasıyla bu durum değişmiştir. Bu akıllı kart yaklaşımı, ayrılabilir güvenli mikrokontrolör prensibinin bir parçasıdır. Akıllı kart bazlı bir karıştırıcı sistemin kurulumu biraz masraflıdır. Fakat akıllı kart, sistemin kolay bir şekilde terfi edilebilmesine izin verir. Bu yüzden yeni karıştırıcı sistemler, bu iki yaklaşımı da birlikte kullanmaya yönelmiştir [1].

Akıllı karta benzer bir düşünce modeli, dijital video yayıncılığına geçilmesinde de görülmektedir. DVB'nin teknik özelliklerinin, korsanlığı engelleyecek tek şey olduğu düşünülmekteydi. Fakat DVB'nin bile kodlama kaplamasını standardize etmede problemleri olduğu görülmekteydi. Bu yüzden bu dijital sistemlerin de hack edilmesi mümkündür [1].

Bu bölümde, akıllı kartların teknolojisi ve nasıl hack edileceği üzerinde durulmuştur. Bu konudaki bazı maddelere daha önceki bölümlerde değinilmiştir. Ayrıca bu konuda, konturlu telefon kartlarının nasıl hack edilebileceği üzerinde de durulmuştur. Çünkü bazı karıştırıcı sistemlerin kullanmış olduğu görüntü başına ödemenin (PPV) teknik özellikleri, bu bellek kartlarının ve akıllı kartların bir kombinasyonunu içermektedir. Örneğin VideoCrypt sisteminin düzelticisinde kullanılmış olan 8052 EPROM'u, akıllı kartların ve bellek kartlarının her ikisinde de bulunan rutinleri kullanmıştır. Bu nedenle, VideoCrypt sisteminin PPV'si hack edilmiştir ve bu yüzden, bu bellek kartlarının kullanımına son verilmiştir [1].

4.1 Akıllı Kartlar

Akıllı kartlar, oldukça ucuz ve kullanıldıktan sonra atılabilen bir teknolojidir. Kullanıldıktan sonra atılan teknoloji kavramı modern bir yaklaşımdır. Avrupa'daki ülkelerin büyük bir kısmı, akıllı kartlı telefon kartlarını kullanmaktadır. Ayrıca, İngiltere gibi optik telefon kartları kullanan ülkeler de mevcuttur. Fakat British Telecom, bellek kartlarını kullanmaktadır. Amerika'da, konturlu telefon kartı uygulaması için bellek kartlarını kullanan bazı test programları mevcuttu. Akıllı kartlardaki problem, bu kavramın çok genelleştirilmiş olmasıdır. Aslında bu, birkaç kart türünü kapsamaktadır. Genellikle telefon kartları sadece bir bellek kartıdır.

Bir akıllı kart ise, bir mikroişlemci ve bir bellek içeren bir kart olarak tanımlanmaktadır. Önceden ödemeli uygulamalarda kullanılmış olan bellek kartlarını akıllı kart olarak tanımlamak yanlıştır. Kontaklı ve kontaksız olarak adlandırılan iki tip akıllı kart vardır.

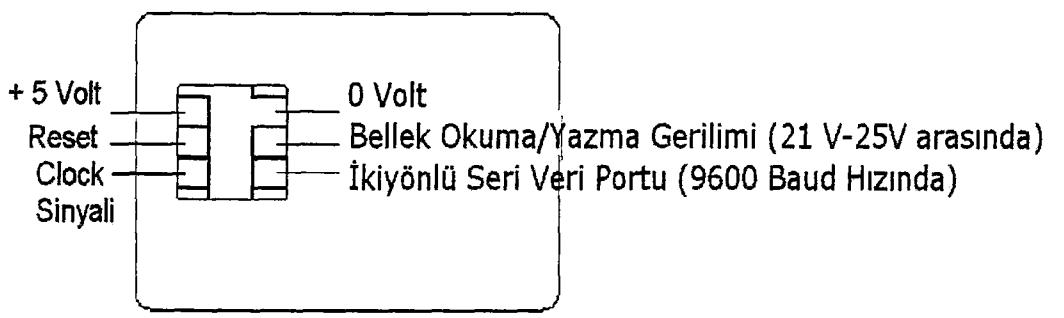
Kontaklı tip akıllı kart, kart okuyucusuna direkt olarak elektriksel bağlantı gerektirmektedir. Birçok bakımdan bu daha ucuz bir tercihtir. Arabirim devre yapısı en düşük düzeyde tutulmaktadır.

Kontaksız tip akıllı kart, kart okuyucusuna direkt bir elektriksel bağlantı gerektirmemektedir. Bunun yerine, kart okuyucusundan gelen sinyalleri okumak için bir takım akortlu devre kullanmaktadır. Bunun için, esas itibariyle üç frekans kullanılabilmektedir. Bu frekanslardan bir tanesi, kartın doğru akım besleme voltajını sağlamak için alternatif akımı doğru akıma çevirmek için ve diğer iki frekans ise veri iletimi için kullanılmaktadır. Fakat böyle bir karmaşık yapı, ödemeli televizyon uygulamaları için tam anlamıyla uygun değildir. Çünkü, bu kartların maliyeti yüksektir ve ödemeli televizyon uygulamaları genellikle, en etkili teknolojiyi en düşük fiyata sağlamakla ilgilenmektedir.

Kontaklı tip akıllı kart, kartın üzerindeki padler ile kod çözücünün soketi arasında direkt bir elektriksel bağlantı gerektirmektedir. Akıllı kartların yapımını ve bağlantı protokollerini yönlendiren ISO-7816 isimli bir ISO şartnamesi mevcuttur. Bu kart protokolleri hakkında detaylı bilgi ilerki bölümlerde verilmiştir.

4.1.1 ISO akıllı kart standardı

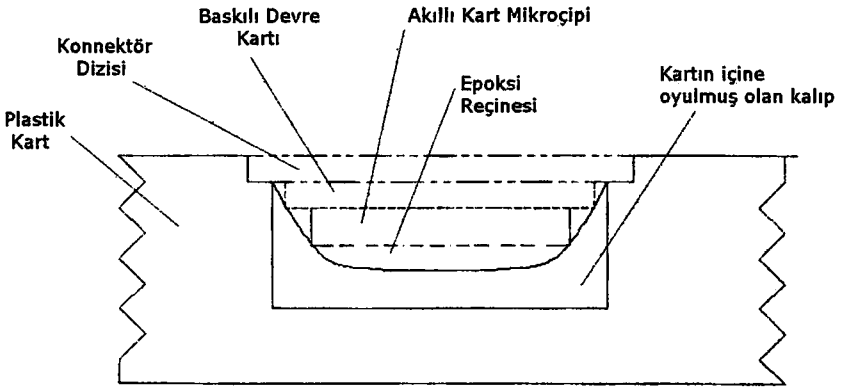
Kontaklı tip akıllı kartlar için konnektör şartnamesi bir ISO standardı ile resmileştirilmiştir. Bu ISO standardı, akıllı kartta sekiz konnektör olduğunu belirtmektedir. Fakat bu sekiz konnektörün sadece altı tanesi aktif olarak kullanılabilmektedir. Ödemeli telefon kartlarında ve bankacılık uygulamalarında kullanılan akıllı kartların büyük bir kısmı Şekil 4.1'de gösterilmiş olan modeli kullanmaktadır. Tipik bir ödemeli telefon kartı, bir akıllı karttan ziyade bir EPROM bellek kartıdır.



Şekil 4.1 ISO akıllı kart standardına göre konnektörlerin işlevi [1]

VideoCrypt karıştırıcı sisteminde kullanılmış olan akıllı kart, Şekil 4.1'deki modele benzememektedir. Bu kartın konnektör düzeninde de altı konnektör kullanılmaktadır. Bir

akıllı kart üzerindeki padlerin yerleşim şekli, kart üreticisinin bir göstergesidir.

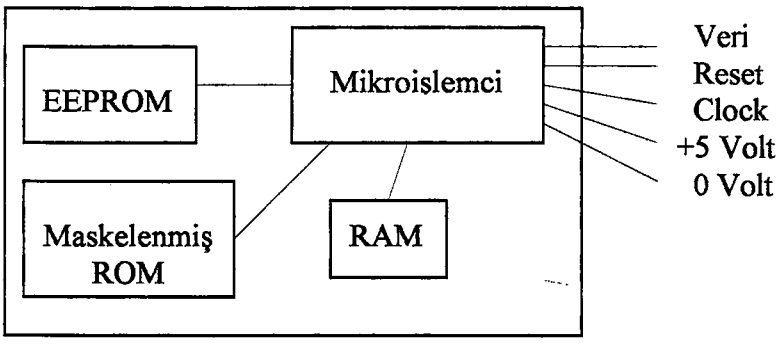


Şekil 4.2 Akıllı kartın kesiti [1]

Ayrıca, akıllı kartın üzerindeki padlerin yerlerini belirten ve kartın gerçek ebatlarını gösteren kılavuzlar vardır. Korsan akıllı kartların büyük bir kısmı, orijinal karttan yaklaşık 20 milimetre daha uzundur. Bu kartlar, yüzeye takılan mikroçiplerin kullanımını kolaylaştırmak için bu şekilde yapılmıştır. Yeni kod çözücülerin ve IRD'lerin bazıları, gömülü kart slotlarına sahiptir ve bu mikroçip, kartın yuvaya tam olarak yerleştirilmesini engellediği için problemlere yol açmaktadır.

4.1.2 Akıllı kartın yapısı

Akıllı kartın yapısı son derecede basittir. Kart, bir mikroişlemci ve bellekten oluşmaktadır. Bu tanımlama, uydu alıcılarını ve video kayıt cihazlarını kontrol etmek için kullanılmış olan mikrokontrolörlere uymaktadır ve gerçekten de bu uygulamalarda aynı mikroçip tipleri kullanılmıştır. Kullanılan bellek tipi değişebilmektedir. Genellikle bu bellek EPROM, EEPROM ve RAM'i kapsamaktadır [1].



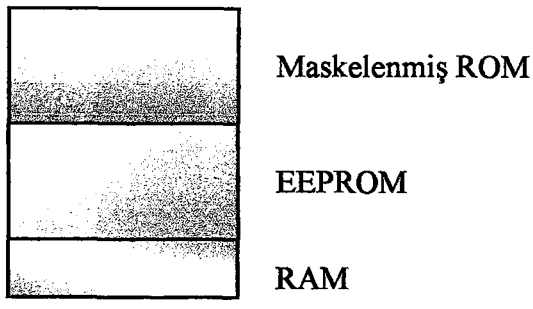
Şekil 4.3 Akıllı kart mikroçipinin yapısı [1]

Maskelenmiş ROM'da depolanmış olan bilgi sabittir ve akıllı kartın tasarımı

değiştirilmeksizin farklılık göstermez. Kartın ROM'undaki temel rutinler, kart arabirimi rutinleri ve diğer hazırlık fonksiyonlarını kapsamaktadır. EPROM'daki bilginin ultra viyole ışığı ile silinmesi gerekmektedir. Yani, kart bir kere programlandığında kartın içindeki bilgi silinememektedir. Bu yüzden, Sky ödemeli televizyon kanalının kullanmış olduğu 05 serisi ve daha önceki akıllı kartlarının servis merkezi tarafından havadan devre dışı bırakılabileceği ve tekrar aktif hale getirebileceği durumların sayısı sınırlıdır. Fakat EEPROM versiyonları bu bakımdan sınırlı değildir. Akıllı kartlarda EEPROM kullanımı daha uygun bir seçimdir. Çünkü, kartın içindeki bu EEPROM tekrar programlanabilmektedir. Fakat bir akıllı kartın EEPROM'unu havadan gönderilen sinyalle çalıştırılması ve yeniden programlanması aşırı derecede tehlikelidir. Çünkü, eğer kart bir bilgisayar korsanı tarafından hack edilmişse o zaman bu kişiler havadan ulaşan bu yeni veriyi izleyebilmekte ve bu veriyi inceleyebilmektedir.

Sky kanalı tarafından kullanılmış olan gerçek akıllı kart tipi, bir Siemens 8051 mikroçipidir. Bu akıllı karttan önce Sky 10 serisi düzelticilerde Motorola 6805 tipi kullanılmıştır. D2-MAC EuroCrypt sisteminin hangi akıllı kart tipini kullandığı tam olarak bilinmemektedir. Fakat buna benzer bir tip olduğu tahmin edilmektedir. Bununla birlikte, Sky kanalının kullanmış olduğu kart bir EEPROM versiyonudur. TV3, TV1000 ve FilmNet kanalları tarafından kullanılmış olan kartların büyük bir kısmı akıllı kartın EPROM versiyonuydu [1].

Bu bilgilere dayanarak, bir VideoCrypt akıllı kartının bellek haritası (Şekil 4.3) tahmin edilebilmektedir. Belleğin ROM bölgesi, temel protokol rutinlerinin ve idareyi sağlayan rutinlerin depolanmış olduğu bölgedir. EEPROM bölgesi, kod çözme algoritmalarını ve anahtarları, servis verisini, PPV verisini, kartın kimliğini saptama verisini ve abonelik bilgilerini içermektedir. RAM ise işlem boyunca verileri geçici olarak depolamak için kullanılmaktadır.



Şekil 4.4 Akıllı kartın bellek haritası [1]

Bu EEPROM, abonenin ödeme yaptığı her bir kanal için bir aktivasyon verisi içermektedir.

Her bir kanal için veri girişi, bir kanal saptayıcı, bir ödeme dönemi bilgisi, bir bölgesel saptayıcı, anahtar verisi ve kanallar için yetki verme verisi içermektedir.

Bir akıllı kartın tasarımı oldukça karmaşıktır ve kartın bir prototipin yapılması birkaç ay sürebilmektedir. Bu akıllı karttaki ROM'un maskelenerek programlanmış olması gereklidir. Yani, ROM'da depolanacak olan programların mikroçipin bir parçası olarak tasarlanması gerekmektedir. ROM'a dahil edilecek olan programlar, bir akıllı kart emülatöründe geliştirilmektedir. Bu emülatör, bir akıllı kart gibi davranacak şekilde konfigüre edilmiş olan bir mikroişlemci geliştirme sistemidir. Bu emülatör, bir bilgisayara bağlanmıştır. Program geliştiren kişi programları bilgisayarda yazmakta, test etmekte ve eğer doğru bir şekilde çalışırsa bunları akıllı kart emülatörüne yüklemektedir. Daha sonra bu akıllı kart emülatörü, bu programların çalışmasını denemek için bir kod çözücüye takılmaktadır.

Daha sonra bu programlar bir diskete alınarak mikroçip üreticisine verilmektedir. Bu üretici, EPROM'u bu programlar ile programlar ve onaylanması için bunu kart dağıtıcısına gönderir. EPROM kontrol edildikten sonra bu üretici, birkaç numune mikroçip üretir. Ayrıca bu mikroçipler de doğru çalışma şekli için test edilir. Eğer her şey yolunda giderse bu mikroçiplerin seri üretimine geçilebilir.

Bu mikroçipler, epoksi reçinesi ile bir baskılı devre kartı tabakasına yapıştırılır. Mikroçipin üzerindeki bağlantı pinleri tabakanın üstündeki bağlantı yerlerine lehimlenir. Daha sonra bu tabaka bağlantıları konnektör düzenine lehimlenir. Gerçek plastik kart, mikroçip için oyularak enjeksiyon ile kalıplanır. Daha sonra bu mikroçip, bu oyuğa yapıştırılır. Bundan sonra kart, çalıştığından emin olunması için test edilir. Bu safhadaki bir akıllı kart, verinin sadece en düşük düzeyine sahiptir. EEPROM'da henüz servis verisi mevcut değildir. Bu veri karta, kart dağıtıcısı tarafından programlanır [1].

Bu işlemin en önemli bölümü test etme aşamasıdır. Akıllı karttaki programlar, kart piyasaya sürülmeden önce yoğun testlerden geçirilmelidir. Bu test aşaması gerçekten çok önemlidir. Çünkü bu kartın yeniden bastırılmasını gerektirecek bir problemin, ancak kart piyasaya sürüldükten sonra fark edilmesi mümkündür. Genelde yeni kart baskısına başlanmadan yaklaşık üç ay önce bu kartların test versiyonları hazırdır.

Akıllı kart güvenliğinde yeni bir eğilim, News Datacom ve Sky kanalları tarafından başlatılmıştır. Sky 10 serisi (0A serisi) kartlarda iki adet mikroçip kullanılmıştır. Bunlardan bir tanesi akıllı kart mikrokontrolörü, diğeri ise uygulamaya özel bütünleşik mikroçiptir (ASIC). Bu, akıllı kart mikrokontrolörlerinin uydu üzerinden yayın yapan televizyon kanalı

uygulamalarında kullanımının artık yeterince güvenli olmadığı gerçeğine kanal tarafından verilmiş olan bir yanıt gibi gözükmektedir.

Bilgiayar korsanları, Sky kanalı 31.10.1995 tarihinde Sky 10 serisi kartını çalıştırdığı zaman bu kartın EEPROM ve ROM'undaki bilgilerin tamamını kopyalamışlardı [1]. Bu korsan kartın, orijinal Sky 10 serisi karttan yaklaşık beş ay sonra piyasaya sürülmesinin sebebi Sky kanalının kullanmış olduğu uygulamaya özel bütünleşik mikroçiptir.

SEASON tipi bir programı gerçekleştirmek isteyenler için problemlere yol açan da bu uygulamaya özel bütünleşik mikroçiptir. Bu problemin olası en iyi çözümü, paralel porttan bağlanabilen bir uygulamaya yönelik bütünleşik mikroçip emülatörüdür.

4.1.3 Akıllı kartın çalışma şekli

Akıllı kart, bir kart üzerindeki kismi bir bilgisayardır. Çalışması için diğer devre yapıları ve girişler gerektiği için kısmi bir bilgisayar kategorisine girmektedir. Akıllı kartın çalışması için gerekli olan ilk şey besleme gerilimidir. Genellikle bu besleme gerilimi + 5 V'tur.

Akıllı kartın çalışması için gerekli olan ikinci şey ise bir clock sinyalidir. Bu clock sinyali, sabit frekansa sahip 5 V genlikli bir kare dalgadır. Bu frekans, kod çözücünün içindeki bir kristalden elde edilmektedir. VideoCrypt karıştırıcı sisteminin akıllı kartında kullanılmış olan clock frekansı 3.57 MHz'dir. Ayrıca daha yüksek clock frekansları da kullanılabilmektedir.

Gerekli olan üçüncü şey resetleme hattıdır. Bu, kart sokete yerleştirildiği zaman kart içindeki programları ve rutinleri başlatmak için kullanılmaktadır. Dördüncü gereksinim ise EPROM voltajıdır. EPROM programlama voltajı yüksektir. Bu voltaj, tipik olarak 20 V'un üzerindedir. Bu voltaj sadece her üç saniyede bir birkaç milisaniye için açıktır. Eğer EPROM sürekli olarak bu yüksek voltajla beslenseydi, mikroçip aşırı derecede ısı üretirdi. Ayrıca akıllı kartın EEPROM versiyonları bu 21 V'luk programlama voltajına ihtiyaç duymamaktadır. Kartın ihtiyaç duyduğu programlama voltajına, kart tarafından iletilmiş olan ATR veri bloğunda işaret edilmektedir.

Gerekli olan beşinci şey bir veri portudur. Veri, karta doğru ve karttan dışarıya doğru olan bir hat üzerinden akar. Bu, seri veridir. Bu port, karttaki RAM'a bağlanacaktır. Bu seri veri RAM'in içine clock'lanır. Daha sonra mikroçipin üzerindeki mikroişlemci, paralel bir biçimde bu veriyi okur. VideoCrypt-I sisteminde veri, 9600 Baud hızında akar. VideoCrypt-II sistemi ve DirecTv sisteminin akıllı kartı 9600 Baud hızında başlatılır. Fakat daha sonra, hızlı veri transferi için 38400 Baud hızına anahtarlanır.

Akıllı kart kod çözücünün içine yerleştirildiği zaman reset pini aktif hale gelir. Bu, RAM'i sıfırlar ve mikroişlemcinin boot-up programını seçmesine neden olur. Programdaki bir sonraki rutin, kartın bu peryot için geçerli olduğunun onaylanmasıdır. Daha sonra akıllı kart, kod çözücüden gelen veriyi okur. Bu veri, EEPROM'dan gelen servis verisiyle birlikte EEPROM'da depolanmış olan kod çözme algoritmasında kullanılır. Daha sonra kod çözme algoritmasının sonucu kod çözücüye geri verilir.

VideoCrypt sisteminde, akıllı karta doğru ve akıllı karttan dışarıya doğru akan bilgi, gerçek kod çözme anahtarı gibi yetki verilecek ve yetki verilmeyecek kartlar için adresleri içerdiği için yararlıdır. D2-MAC EuroCrypt-M ve DSS gibi diğer sistemler, daha karmaşık veri paketi yapısına sahiptir. Bu paket yapılarının bilgisini oluşturmak gerçekten çok zaman almaktadır.

Bu veri, 8052 idareyi sağlayan (housekeeper) mikrokontrolörden geçerek her alanın veya görüntünün başlangıcındaki kesme noktası üreteci için çekirdek üreten başka bir algoritmada kullanılacağı ZC404044 veya ZC404047 gibi bir güvenli mikrokontrolöre geçmektedir. Aslında bu güvenli mikrokontrolör, 6805 mikrokontrolörünün maskelenmiş ROM versiyonudur. Bu mikroçipin içindeki veriler okunmuştur ve bu bilgiler, uydu televizyonları ile ilgili olan internet sitelerinde ve BBS'lerde mevcuttur [1].

Görüntü başına ödeme seçeneğinin bir akıllı kart ile gerçekleştirilmesi çok kolaydır. Abone (kart sahibi), her bir hesap kesim döneminde bir takım kredi veya kontur satın alacaktır. Tipik sayı, 99 konturdur. Akıllı kart bu kontur sayısına programlandığı için kontur sayacı 99 konturu okuyacaktır. Abone, görüntü başına ödemeli bir televizyon programını seyretmek istediği zaman, ekranda bu programın kaç kredilik/konturluk değere sahip olduğunu gösteren bir mesaj çıkacaktır. Bu programı seyredebilmek için abonenin, kod çözücünün ön tarafındaki yetki verme/ödeme butonuna basması gereklidir. Daha sonra kod çözücü, kontur sayacını uygun oranda azaltacaktır.

Her bir servis, farklı bir kontur sayacına sahip olabilir. Ayrıca sayma mekanizmasının gerçek çalışma şekli bundan daha karmaşık olabilir. Kontur sayacını durdurmak ve sürekli bir 99 kontur değeri atamak mümkündür. Genellikle bu tür bir hack işlemi, bilgisayar oyunlarında kullanılır ve "sonsuz yaşam hilesi" olarak bilinmektedir. VideoCrypt için orijinal PPV algoritması genellikle 8052 mikroçipinin içinde bulunur. News Datacom 07, 09 ve 10 serisi akıllı kartlardaki güvenliğinin korsanlar tarafından çökertilmesiyle, PPV protokollerini daha güvenli bir format ile değiştirmek zorunda kalmıştır [1].

Bu yeni protokol, ön kayıtlı bir PPV sistemiydi. Abone, abone yönetim merkezine telefon

ederek abone numarasını söyleyecek ve daha sonra abonenin kartı, belirli bir PPV programı için kanal tarafından havadan aktif hale getirilecektir. Bu PPV programı gerçek olmayan bir kanal kimliğine atandığı için sadece bir kartın bu kanala erişim sağlamak için etkin hale getirilmesi gerekmektedir. Bu PPV televizyon programı sona erdiği zaman bu kanal kimliği iptal edilmektedir.

4.1.4 Akıllı kart güvenliği ve adreslemesi

VideoCrypt sisteminde kullanılmış olan akıllı kartlar, abone yönetim merkezinden kullanıma hazır olarak çıkmaktaydı. Yani, bunlar herhangi bir VideoCrypt kod çözücüsünde kullanılabiliyordu. Fakat bu kartlar, Sky kanalı tarafından havadan gönderilen bir sinyal ile kapatılabiliyordu. Bu Quickstart ismi verilen kartlar, Sky tarafından aktif hale getirilinceye kadar geçerli olmuyordu.

VideoCrypt sistemindeki kapatma (kill) sinyalleri geniş çaplı olarak kullanılabilmektedir. Bu yüzden bütün kanallar bu sinyalle kapatabilir veya aktif hale getirilebilir. Kapatılması gereken akıllı kartların kimliklerini içeren kapatma bilgisiyle birlikte bir dizi paket havadan sürekli iletilmektedir. Bu kapatma dizisi, Kara Liste (Blacklist) olarak adlandırılmaktadır.

Kartı kapatma işlemi gerçekleştirildiğinde karttaki EEPROM'un bir bölümünün üzerine yazılmaktadır. Böylece, bu kart kod çözücüye yerleştirildiği zaman kapatılmış olan bu kanallarda çalışmayacaktır. Sky kanalı, bu kartı tekrar aktif hale getirmek için Beyaz Liste (whitelist) dizisinin bir parçası olarak bu kartın kimlik bilgisini iletir. Bu beyaz liste, kartı açma bilgilerini ve açılacak olan kartların kimlik bilgilerini içeren bir dizi pakettir. Fakat bu liste, devamlı iletilen bir liste değildir. Abone, abone işleri merkezini arayarak kartını açtırabilmektedir. Kapatılacak olan kartların kimlik bilgileri ise kara liste ile sürekli iletilmektedir.

Sky kanalı, 09 serisi Sky kartlarına bir kapalı duruma getirme (drop dead) kodu eklemiştir. Haberleşme protokolünü kontrol eden EEPROM'un belirli bir bölgesine yazarak, kartı sonsuz bir döngüye sokmak mümkündür. Bu kod, Amerika'da DSS kartlarında kullanıldığında Code 99 elektronik karşı tedbiri olarak ve 09 kartlarında kullanıldığı zaman ise Drop Dead elektronik karşı tedbiri olarak adlandırılmıştır. Buradaki ortak faktör, News Datacom kanalının her iki sistemin de güvenliğini sağlamış olmasıdır.

Akıllı kart kullanan sistemlerdeki en yeni eğilim, abonelere kartları aktif olmayan konumda göndermekti. Abonenin kartının havadan gelen sinyalle aktif hale getirmeleri için abone işleri

merkezini araması gerekmekteydi. Fakat bu adresleme metodu çok fazla zaman alıyordu ve bu yüzden de ekonomik olmuyordu.

07 ve 09 serisi VideoCrypt kartlarının hepsi, abonelere gönderildiğinde bütün kanalların anahtarlarını içermekteydi. Bu kanallar, ortak bir algoritma ve anahtar tablosu kullanmaktaydı. Bu yüzden, güvenlik bakımından bu durum tam bir felakettir. Çünkü bu kart, korsan bir Phoenix emülatör programıyla aktif hale getirilebilmekte ve bütün kanallar izlenebilmektedir. Bundan başka, anahtarların kartın içinde yerleştirilmiş olmasının yerine gerekli anahtarları havadan iletilen sinyallerle akıllı karta göndererek korsanlığı en azından kanal bazında sınırlayabilecek bir tedbir de alınmamıştı.

D2-MAC EuroCrypt sistemi, anahtar kullanımı bakımından daha başarılıdır. Bu sistem, peryodik olarak değiştirilebilen ve her bir kanal için farklı olan bir anahtar kümesine sahiptir. Eğer kart geçerli bir yönetim anahtarına sahip değilse, uygun bir şekilde terfi işlemi yapılamayacaktır. Bu sistemde kullanılmış olan algoritma çok sıradan bir algoritmadır. Teorik olarak kişiselleştirme işlemi sırasında, abonenin ödeme yaptığı kanallar EEPROM'a girilmektedir. Böylece abone, sadece ücretini ödediği kanallara erişebilecektir. Diğer kanallar ise kapalı bir şekilde görünecektir.

VideoCrypt sistemi, hariç tutma prensibini baz almaktadır. Buna göre, sistemdeki akıllı kartların tamamı servis tarafından gönderilen kapatma sinyalini alıncaya kadar aktif kalmaktadır. Fakat bunun en güvenli sistem olmadığı kesindir. Çünkü bir kart temin etmek ve bu kartı birkaç ay kod çözücünün dışında tutarak bu kartın kapatılmasını engellemek mümkündü. Çünkü bu kapatma sinyali sürekli iletilmemekteydi. Bu yüzden kartın kapatılamama ihtimali de vardı.

09 serisi kartlardaki başlıca problem, bu sistemin kart adreslemesinin ve aktivasyon yapısının hack edilmiş olmasıydı. Yani, havadan gönderilen sinyallerle kapatılmış olan bir kartı tekrar aktif duruma getirmek mümkündü. Kartların üzerinde verilmiş olan kanal aktivasyonu prosedürüne göre, bir kartın üzerindeki kanalların seçilerek aktif hale getirilmesi mümkündü.

09 serisi Sky kartlarını aktif hale getirmek için kullanılmış olan korsan program Phoenix programı olarak adlandırılmıştır. Bu tabir, bir akıllı kart üzerindeki program kanallarını aktif hale getiren herhangi bir programı tanımlamak için kullanılmaktadır. Bu korsan Phoenix programı Bölüm 6'da detaylı bir şekilde incelenmiştir.

4.2 Bellek Kartları

Bellek kartları, akıllı kartların en basit formudur. Bu kartlar, bir mikrokontrolör içermedikleri için aslında akıllı değildir. Bu kart, bazı adresleme devre yapılarına sahip olan bir bellektir. Sonuçta bu kartlar, seri bellek mikroçipleridir ve bu yüzden kolayca okunabilir ve programlanabilirler. Bununla birlikte, bu kartlar kolayca emüle edilebildiği için telekom firmaları için problem yaratmaktadır [1].

Bu bellek kartları yeterince güvenli olmadığı için uydudan yayın yapan ödemeli televizyon kanalı uygulamalarında yaygın bir şekilde kullanılmamaktadır. VideoCrypt sisteminin orijinal patenti, bellek kartlarını içermekteydi. Fakat bu durum, bu kartların kullanılmak için yeterince güvenli olduğu anlamına gelmemektedir.

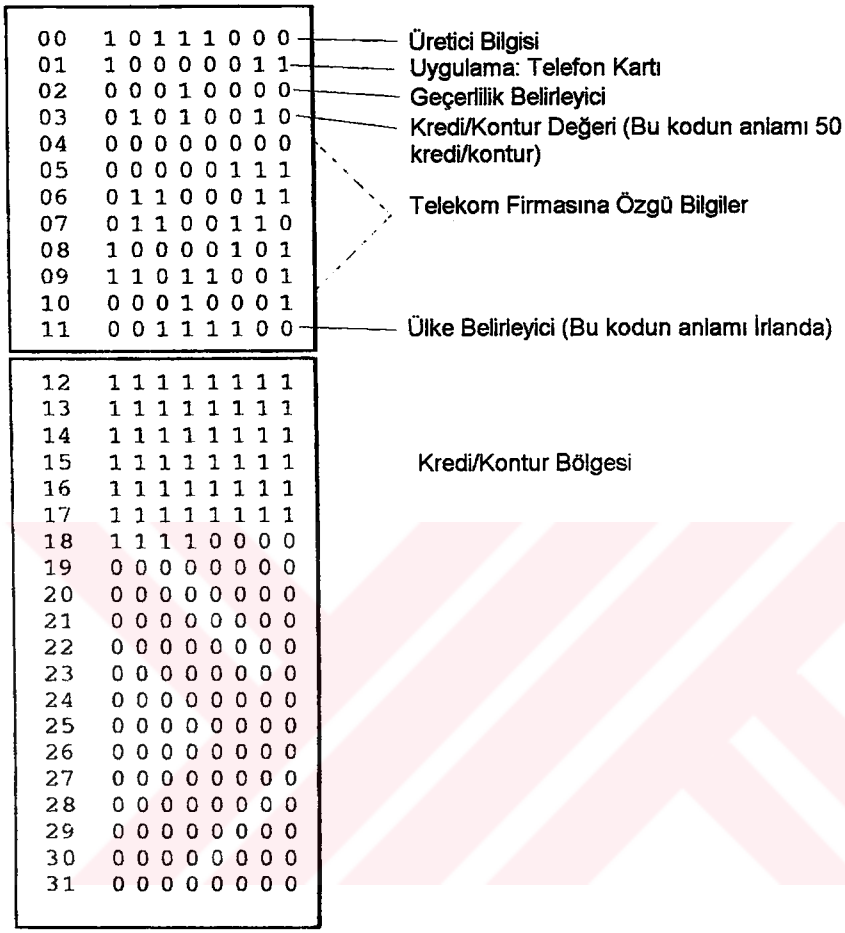
Bellek kartlarının en yaygın olarak kullanıldığı uygulama alanı, ön ödemeli telefon kartlarıdır. Bu telefon kartlarının büyük bir kısmı sadece bellek kartıydı. Daha basit bir ifadeyle, bu kart 265 bitlik seri bir EPROM'dur. Bu kartın yeni versiyonları da piyasada mevcuttur. Fakat bu yeni versiyonlar EEPROM'dur. Bununla birlikte telefon kartlarının büyük bir kısmı, aşırı derecede ucuz olduğu için EPROM versiyonudur.

Telefon kartı uygulamasını kullanmış olan firmalardan biri France Telecom'dur. Bununla birlikte, diğer ulusal telekom firmaları da France Telecom'u izlemiştir. Bu firmalar, teknoloji ile fazla ilgili değillerdi. Telecom Eireann'ın tamamen tehlikede olan bir kart sistemini seçmesindeki sebep tamamen kar amaçlıydı. Telecom Eireann'ın mikroçip kart bazlı telefon ağını gerçekleştirmesi, yüzeysel olarak bakıldığında iyi bir adım gibi görünmekteydi. Çünkü bu mikroçip kart ile çalışan telefon aygıtlarının para biriktirmesi gerekmiyordu ve böylece, telefon haznesindeki paraların çalınma ihtimali ortadan kalkıyordu. Ayrıca, bu telefon kartlarının üzerindeki boş kısma firmalardan reklam alınarak yeni bir gelir kaynağı yaratılabilmekteydi. Sonuç olarak, bu kart güvenlik bakımından detaylı bir şekilde incelendiğinde aslında tam bir felaket olduğu görülmektedir. Çünkü PIC16C84 bazlı korsan telefon kartı emülatörleri Avrupa'nın heryerinde kullanılmaktadır [1].

4.2.1 Telefon kartının bellek haritası

Şekil 4.5'te gösterilmiş olan bellek haritasında 00 ile 95 arasındaki bitler, üretici/dağıtıcı kimliği için ayrılmış olan alandır. Bu alan sigorta korumalıdır ve üzerine yazılamamaktadır. 96 ile 255 arasındaki bitler ise kartın programlanabilen alanını oluşturmaktadır. Bu bitler, telefon bu karttan bir kredi kullandığı zaman değişmektedir. Bu alan bir EPROM olduğu için

buradaki her şey silinmeksizin bu bitler resetlenememektedir. Bu yüzden bu dilimi kartın dışına çıkarmak ve epoksi reçinesini kaldırmak için harcanan zamana ve çabaya deymemektedir. Bu bellek kartları bir seri EPROM olduğundan okunması mümkündür. Radio Plans dergisi tarafından birkaç yıl önce bu konu hakkında faydalı birkaç makale yayımlamıştır.



Şekil 4.5 Telefon kartı bellek haritasının bir örneği [1]

Bir bellek kartının PPV versiyonu, Şekil 4.5'teki modelden pek farklı değildir. Bellek kartında kartın üreticisinin kimliği için ayrılmış olan alan, televizyon programları için anahtar tablolarını çok başarılı bir şekilde tutabilir. Buradaki kredi alanı ise, aboneye ait anahtar tablosu grubunu tutabilir. Kod çözücü, her bir program için anahtar tablosu kullandığı için daha sonra bu belirli tabloların üzerine yazılması gereklidir. Bu yüzden, bellek kartlarının görüntü başına ödeme (PPV) uygulamaları için tek başına kullanılması mümkün değildir [1].

Bilgisayar korsanları, korsan telefon kartları ile fazla ilgilenmemişlerdir. Çünkü korsan Sky ve D2-MAC kartları, bir telefon kartı emülatörünün satış fiyatının iki katına satılmaktaydı. Ayrıca korsan telefon kartı, standart bir korsan kod çözücü kartından farklı bir baskılı devre

kartı gerektirmekteydi ve bunun gerçekleştirilmesi ekonomik değildi. Üstelik bilgisayar korsanlarının büyük bir kısmı, daha güvenli ve yakalanma riski çok daha az olduğu için uydu üzerinden yayın yapan ödemeli televizyon kanallarını hack etmeye yönelmişlerdir.

4.2.2 Bellek kartlarının güvenliği

Bellek kartlarında gerçekleştirilmiş olan hack işlemlerinin büyük bir kısmı telefon kartlarını hedef almıştır. Telefon kartları, güvenlik bakımından çok zayıftır. Bu kartlar, seri EPROM oldukları için bir takım hack etme işlemlerinin gerçekleştirilebilmesi mümkündür.

EPROM'daki 256 bit, 4'er bit genişliğinde alanlar şekilde düzenlenmiştir. İlk 96 bit üreticinin/dağıtıcının kimlik kodunu tutmaktadır. Bu bitler, telekom şirketini ve kartın kullanıldığı ülkeyi göstermektedir. Diğer 160 bit ise, kartın kredi/kontur değerini ve geriye kalan kredi/kontur miktarını göstermektedir. Daha yüksek değerler atamak için bu kartların yeniden programlanması mümkün değildir.

En eski hack işlemlerinden biri Infinite Lives Hack'tir [1]. Başarılı bir yazma işlemi için EPROM'un 21 V ile 23 V arası bir gerilime ihtiyacı olduğu için bu yazma geriliminin akıllı kartın üzerindeki yazma gerilimi padinden gelmesi engellenmiştir. Bunu gerçekleştirmek için izolasyon bantı ve pin cilası gibi bir takım malzemeler kullanılmıştır. Bu hack işlemine elektronik karşı tedbir almak, telekom şirketleri için kolay bir iştir. Telefon aygıtındaki program değiştirilerek kartın yazılabilir olup olmadığının kontrol edilmesi mümkündür. Fakat lojistik bakımdan bu durumu düşünürsek, her bir telefon aygıtının EPROM'undaki programın değiştirilmesi çok zordur.

4.2.2.1 Birinci nesil telefon kartı emülatörleri

Telefon kartları, elektronik bakımdan basit aygıtlardır. Bu yüzden, seksenli yılların başında kullanılmaya başlandığından beri sürekli hack edilmişlerdir [1]. EPROM'un üzerine yazılmasını engelleyen hack işlemleri oldukça ilkeldir. İlk emülatör tasarımı, ayrık devre yapıları kullanılarak bu telefon kartının gerçekleştirilmesiydi. Bu devre yapısı, bazı clock'lama devre yapısından, bazı adresleme devre yapısından ve bir EPROM'dan oluşmaktaydı. Bu EPROM, birkaç telefon kartının birer kopyasını içermekteydi. Bir anahtar, EPROM'un veri satırları arasında anahtarlama yaparak bu kopyalardan uygun olanını seçmekteydi. Telefon kartı seri bir EPROM olduğu için sadece bir adet veri satırı mevcuttur ve adresleme dahili olarak gerçekleştirilmiştir. Bu emülatör tasarımı, ayrık (discrete) ve piyasada kolayca bulunabilen parçalarla bu işlemlerin aynısını gerçekleştirmiştir.

Böylece bu EPROM telefon kartı emülatörü, telefon cihazındaki telefon kartı slotuna yerleştirildiği zaman, sıradan bir telefon kartı gibi çalışmaktaydı. EPROM'un içindeki kart kopyalarının tamamı kullanıldığı zaman bunları yenilemek için EPROM'u yeniden programlanması çok kolaydır. Fakat bu iş için bir bilgisayar, bir EPROM programlayıcı ve bir ultra viyole silici gerekmektedir.

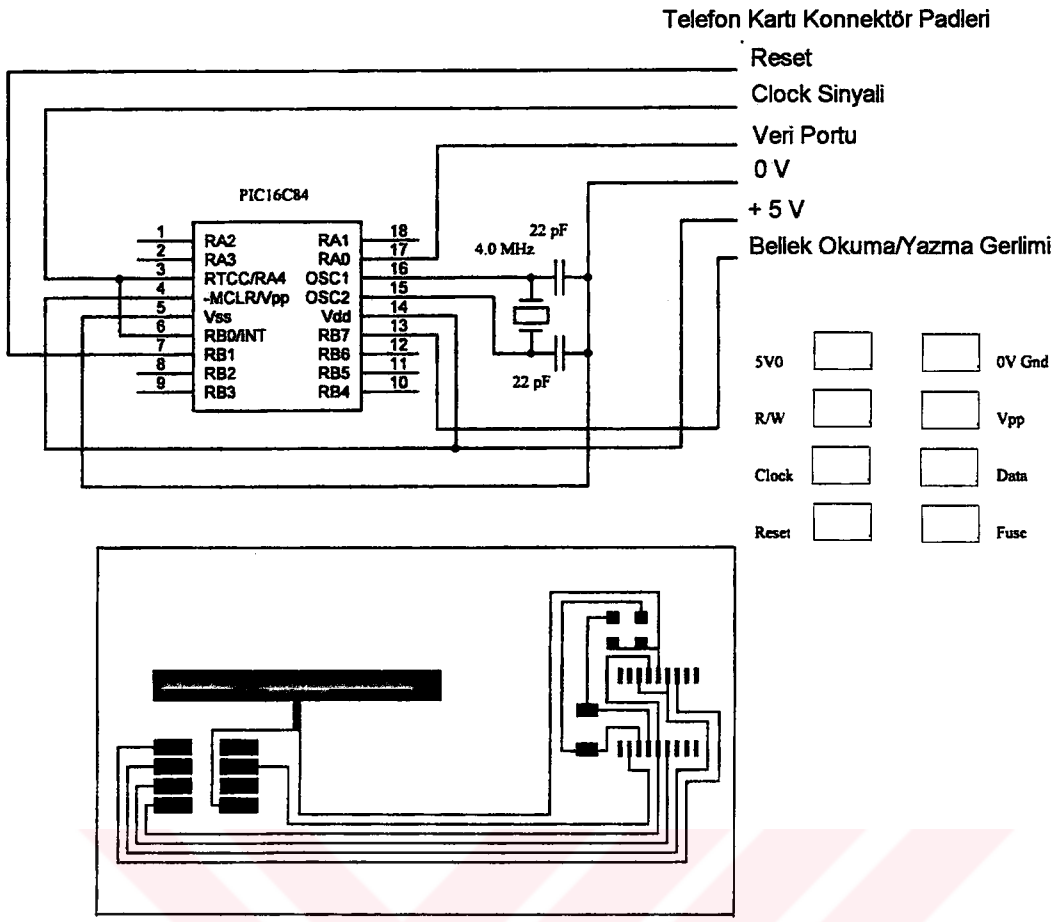
Bu seri EPROM kart emülatörü, devre yapısından dolayı kendi sonunu hazırlamıştır. Bu emülatör, bir baskılı devre kartı üzerine kurulmuş olan ve bir telefon kartına kısmen benzeyen bir aygıttır. Devre yapısını taşıyan geniş bir alana sahip olduğu için normal bir telefon kartından çok daha büyüktür. Bunun farkında olan telefon üreticileri, yeni konturlu telefon aygıtlarına kayar bir kapı dahil etmiştir. Bu kayar kapı, bir seri EPROM kart emülatörü gibi normal bir telefon kartından çok daha büyük herhangi bir kartın telefon kartı yuvasına yerleştirildiği zaman kapanamayacak ve kapı kapanmadığı için de telefon cihazı çalışmayacaktı.

4.2.2.2 İkinci nesil telefon kartı emülatörleri

Bu yeni telefon kartı emülatörü tasarımı, ayrık EPROM'lar ve CMOS lojik yerine mikrokontrolörleri baz almaktadır. PIC16C84 modelinden (Şekil 4.6) önce, en yaygın olarak kullanılan mikrokontrolörler 8751 ve 68705'tir. Bu mikrokontrolörler için telefon kartı emülatör programları, bu konu ile ilgili internet sitelerinde ve BBS'lerde mevcuttur [1].

Telefon kartı belleğinin bir kopyasını emülatör belleğine yüklemenin iki metodu vardır. Bunlardan birincisi, telefon kartı belleğinin kopyasını mikrokontrolör programının bir parçası olarak yerleştirmektir. Fakat bu durum, aynı telefon kartı seri numarasının defalarca kullanılacağı anlamına geldiği için sınırlı kullanımı olan bir seçim olmaktadır. Aynı seri numarasını defalarca kullanan bu tür telefon kartı emülatörlerinin kullanımı, bilgisayar korsanları için çok tehlikelidir. Çünkü telekom şirketleri, bu telefonların aygıtlarının bir dökümünü alarak bu kart emülatörlerinin nerede kullanıldığını bulabilmekte ve kart emülatörünü kullanan kişi tarafından aranmış olan telefon numaralarını bulmak için bu telefondan yapılan aramaları izleyebilmektedir.

Telefon kartı belleğinin bir kopyasını emülatör belleğine yüklemenin ikinci metodu, bir kart okuyucu slot dahil etmektir. Bu metot, mükemmel bir metottu ve eski telefon kartı seri numaralarının kullanımına izin vermekteydi. Bu tür bir hack etme işlemi çoğunlukla, kart emülatörünün 68705 versiyonu ile birleştirilmiştir.



Şekil 4.6 Telefon kartı emülatörünün devre diyagramı [1]

4.2.2.3 Üçüncü nesil telefon kartı emülatörleri

Bu emülatörler, uydudan yayın yapan televizyon kanallarının kullandığı akıllı kartların korsanlığı sonucunda geliştirilmiştir. Avrupa'daki uydu televizyonu akıllı kart korsanlığının temeli PIC16C84 mikrokontrolörüne dayanmaktadır. Çünkü bir 6805 mikrokontrolörünü emüle etmek çok zordur. Fakat 256 bitlik bir seri EPROM'u bu mikrokontrolör ile emüle etmek çok zor değildir [1].

Bunun sonucunda, PIC16C84 telefon kartı emülatör programlarının bir engeli mevcuttu. Bu engel, verilerin okunması ve geniş çaplı dağıtılması için programları telefon kartı emülatöründen elde eden PicBuster rutinine yardımcı olmuyordu. PIC16C84 versiyonu, gerçek anlamda ticari amaçlı ilk telefon kartı emülatörüdür. Çünkü, doğu Avrupa'daki bazı korsan kart üreticileri Avrupa'daki telefon kartı kullanan ülkelerin büyük bir kısmında çalışacak bir telefon kartı emülatörü yapmışlardı. Telefon kartı korsanlığı da dahil olmak üzere korsanlık, uluslararası bir endüstri haline gelmişti [1].

Bir PIC16C84 telefon kartı emülatörünün baskılı devre kartı tasarımı, uydudan yayın yapan şifreli kanallarda kullanılan korsan akıllı kartlardan biraz daha farklıdır. Telekom şirketleri, telefon kartı emülatörlerinin kullanımını engellemek için, telefon kartlarına Vpp padini dahil ederek tasarlamış oldukları bir elektronik karşı tedbiri uygulamıştır.

Bu elektronik karşı tedbir, konturlu telefonlara bir metal detektörünün dahil edilmesidir. Orijinal telefon kartı sadece, mikroçipin olduğu yerde metal alaşıma sahiptir. Bu kartın geri kalan kısmı sadece plastiktir. Fakat telefon kartı emülatörü, akıllı kart padleri ve kartın devre yapısı arasında baskılı devre kartının üzerinde metal yollara sahiptir. Bu metal detektörü kart emülatöründeki bu metal yolları tespit etmekte ve telefonun çalışmasını engellemekteydi.

Fakat telekom firmalarının gerçekleştirdiği bu elektronik karşı tedbirin çözümü oldukça basittir. Çünkü, metal detektörü tasarımında bir kusur mevcuttu. Bu metal detektörünün çalışması topraklanarak engellenebiliyordu. Bu yüzden, telefon kartı emülatörlerinin baskılı devre kartı tasarımları bu metal detektörünün topraklanması için bir metal (bakır) yol ilave edilerek değiştirilmiştir. Bu metal yolun, metal detektörünün probu ile çok iyi temas etmesini sağlamak için bu yol lehim ile kaplanmıştır. Bu basit elektronik karşı tedbir, D2-MAC ve VideoCrypt gibi sistemleri hack eden bilgisayar korsanları için çok basit bir önlemdi.

4.2.2.4 Telefon kartı korsanlığındaki son durum

Uydudan yayın yapan televizyon kanallarının kullandığı akıllı kartlarının korsanlığı, telefon kartı korsanlığından daha kazançlı olduğu için bilgisayar korsanlarının büyük bir kısmı bununla ilgilenmemektedir. Ayrıca, telefon kartı korsanlığında yasal tehlike çok fazladır. Telefon şebekelerindeki gerçek korsanlık mobil telefonlarda meydana gelmektedir. Bir mobil telefonun kartını klonlamak, bir telefon kartı emülatörü yapmaktan çok daha basittir [1].

Mobil telefonların klonlanabilmesindeki kolaylık, telefon kartlarındaki korsanlığı ikinci plana atmıştır. Bu yüzden telefon kartı korsanlığı, telekom şirketleri tarafından büyük bir tehlike olarak görülmemiştir. Bu şirketler daha çok, mobil telefon kartlarının klonlanmasından endişe duyuyorlardı. Çünkü eğer telefon kartı emülatörünün belirli bir konturlu telefonda cihazında kullanılma oranı çok fazla ise, bu telefon cihazını sıradan bir ödemeli telefon cihazı ile değiştirilebilmekteydi [1].

Konturlu telefon cihazları, telefon kartı emülatörleri için bir tehlike oluşturabilecek bazı elektronik karşı tedbirlere sahiptir. Bu tehlike, korsan bir kart tespit eden telefon cihazının merkezdeki bir alarmı tetiklemesidir. Yeni kartların bazıları, Vpp voltajını bile

kullanmamaktaydı. Bunun yerine, mikroçipin içinde dahili olarak Vpp voltajını üretmek için Vcc besleme voltajını çarpan bir donanıma sahipti. Telekom şirketleri, korsanlık konusunda uydudan yayın yapan ödemeli televizyon kanallarından daha ciddiydi ve bu yüzden telefon kartı korsanlığı, bilgisayar korsanları için çok tehlikeliydi.

Daha önce de bahsedildiği gibi, telekom şirketlerinin EPROM kartlarını kullanmalarının nedeni ucuz olması ve kullanıldıktan sonra atılabilir olmasıydı. Bununla birlikte, piyasada görülen bazı yeni versiyonlar EEPROM kartlardı. EEPROM kartları, yapıları itibariyle tekrar kullanılabilmektedir. Bu yüzden, yüksek kontur değerine sahip EEPROM telefon kartlarını piyasada bulmak çok zordu. İrlanda'da, telefon kartı kontur değerleri 10, 20, 50 ve 100 konturdur. 100 konturluk kartların piyasada bulunması neredeyse imkansızdı. Çünkü İrlanda'daki yerel telekom olan Telecom Eireann, bu 100 konturluk kartları piyasadan geri çekmişti. Yüksek kontur değerine sahip telefon kartlarının piyasadan çekilmesinin sebebi, bilgisayar korsanlarının çoğunlukla bu kartların bir kopyasını çıkarma eğilimiydi [1]. Bu kartların piyasadan çekilmesiyle, telefon kartı emülatörlerinin genelde nerelerde kullanıldığının belirlenmesi daha kolay olacaktı.

British Telecom da bu telefon kartlarından kullanmaktadır. Fakat ne tür bir protokol kullandığı tam olarak bilinmemektedir. Bu kartlar, her sıradan telefon kartı gibi Microwire benzeri bir protokol veya I2C'de modellenmiş farklı bir protokol kullanabilmektedir. Ayrıca bu telefon kartlarında, kartın geçerli kalacağı bir süre limiti mevcuttur.

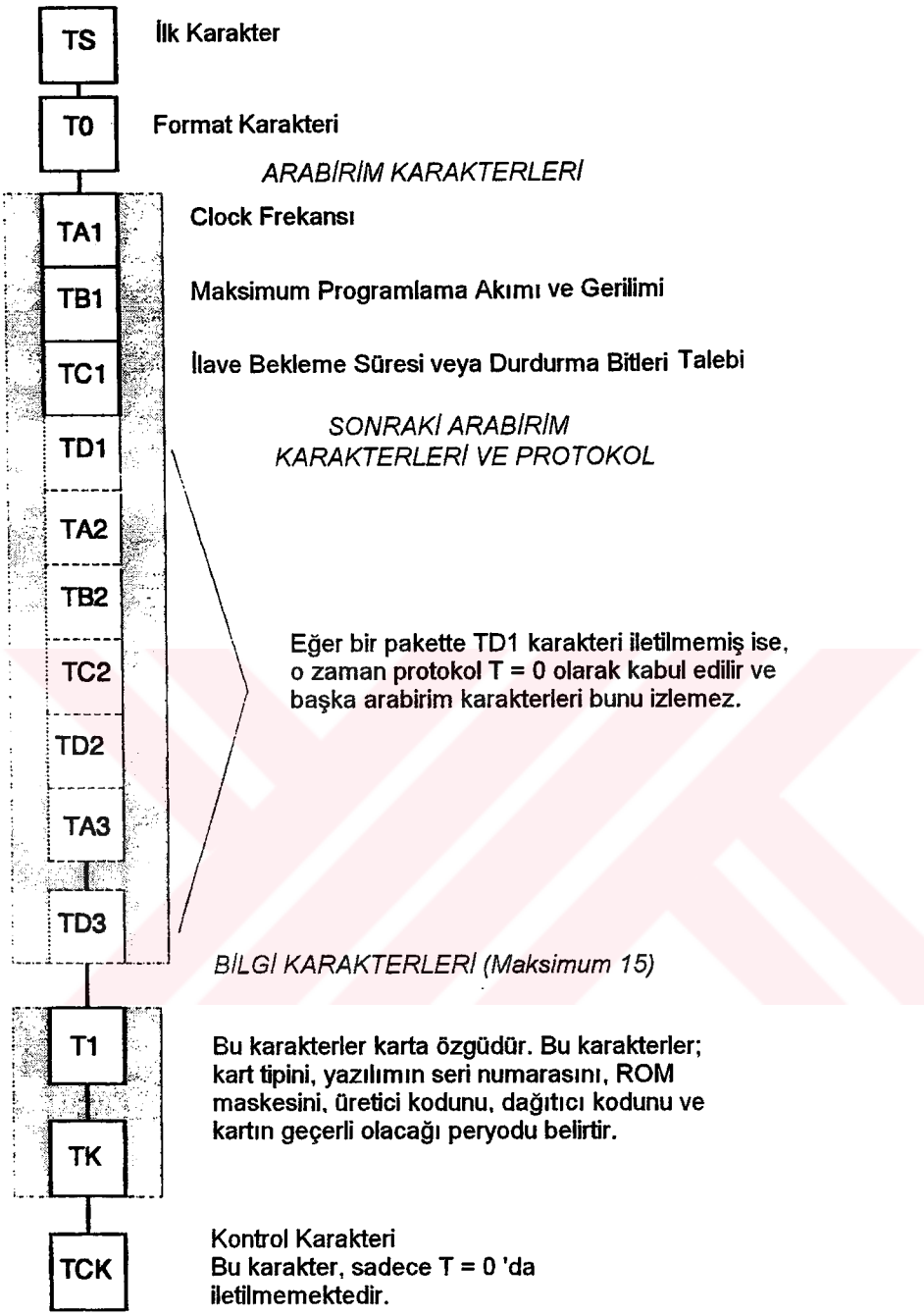
4.3 ISO 7816 Akıllı Kart İletim Protokolü

Karıştırıcı sistemlerin büyük bir kısmında kullanılmış olan akıllı kartlar 9600 baud hızında çalışan bir seri veri bağlantısı kullanmaktadır [1]. Fakat, DirecTv sistemi ve kartı önce 9600 baud hızında başlatıp daha sonra hızlı veri iletimi için 38400 baud hızına geçen VideoCrypt-II sistemi istisnadır. Bütün veriler bu bağlantı yolu ile iletilmektedir. ISO 7816 şartnamesinin üçüncü bölümü, akıllı kart iletim protokollerinden bahsetmektedir.

Akıllı kart düzelticiye yerleştirildiği zaman başlangıç durumundadır ve düzelticiye bir bilgi paketi gönderir. Bu bilgi paketi, ATR olarak adlandırılır. Bu bilgi paketi, düzelticinin ne tür bir haberleşme protokolünün kullanılması gerektiğini ve ayrıca işlem için hangi sinyallerin ve gerilimlerin gerekli olduğunu bildirdiği için akıllı kart tarafından gönderilen en önemli pakettir [1].

Bu ATR paketinin yapısı Şekil 4.7'de gösterilmiştir. Avrupa'da kullanımda olan akıllı

kartların büyük bir kısmı T=0 protokolünü kullanmaktadır. T=0 protokolü bir karakter iletim protokolü, T=1 protokolü ise bir blok iletim protokolüdür.

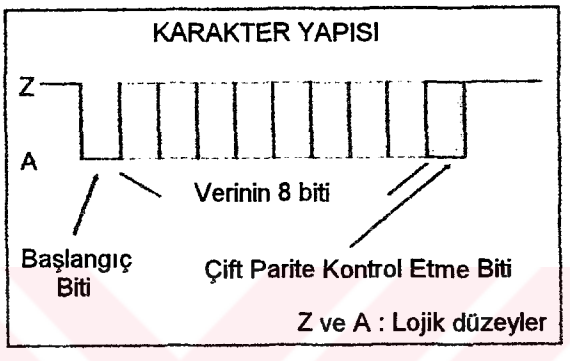


Şekil 4.7 ATR paket yapısı [1]

T=0 protokolü asenkron, yarı dupleks, aktif düşük reset (active low reset) ve ters düzenlidir. Asenkron terimi, protokolün paralel değil seri olduğu anlamına gelir. Paralel iletimde, clock'lama sinyalinin bazı formlarının asenkron bir protokolde gönderilmesi gereklidir. Bu iletimde, farklı clock'lama sinyali yoktur. Yarı dupleks terimi, bu protokolün bir konuş-dinle (talk-listen) protokolü olduğu anlamına gelir. Veri, her zaman sadece tek bir yönde

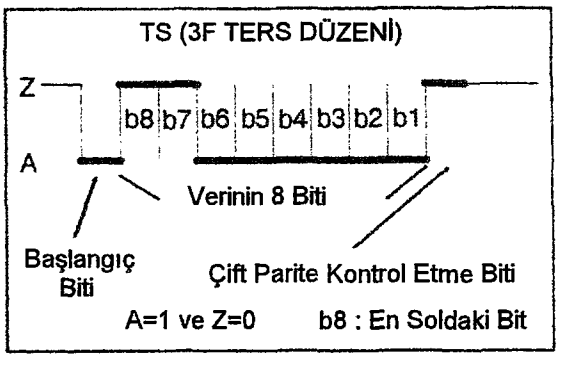
akmaktadır. Ters düzenli tabiri, verinin ters çevrilmiş olmasının gerekli olduğunu ve bitlerin bir RS232 arabirimi ile okunabilmesi için bu bitlerin sırasının ters yönde olması gerektiğini ifade eder. Bu format, RS232 arabirimi üzerinde yaklaşık olarak 8 veri bitine, 1 parite bitine ve 2 durdurma bitine karşılık gelir.

T=0 protokolü, karakter bazlı bir protokoldür. Her bir karakter, 10 bitten oluşmaktadır. İlk bit, bir durdurma bitidir. Sonraki sekiz bit (bir bayt) veri bitidir ve son bit ise çift parite kontrol etme bitidir. Bu bit, hata düzeltmek için kullanılmıştır ve her zaman karakterdeki bitlerden birinin çift sayı olmasını sağlamaktadır. Bu karakter yapısı Şekil 4.8'de gösterilmiştir. Z ve A düzeyleri lojik düzeylerdir.



Şekil 4.8 T=0 protokolünün karakter yapısı [1]

Ters düzende (3Fh), standart lojik polaritesi ters yönde değiştirilmiştir (Z=0 ve A=1). Ayrıca verideki bu bitlerin sırası, ilk önce iletilmesi gereken en soldaki (önemli) bit ile de ters yöndedir (Şekil 4.9).

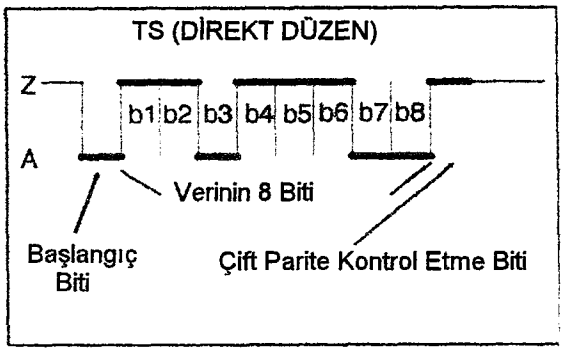


Şekil 4.9 3Fh ters düzenin karakter yapısı [1]

Direkt düzende (3Bh), standart lojik polaritesi kullanılmıştır (Z=1 ve A=0). Bu bitlerin sırası, ilk önce iletilmesi gereken en sağdaki (önemsiz) bit (LSB: Least Significant Bit) ile aynı yöndedir (Şekil 4.10).

T=0 protokolündeki hata düzeltme mekanizması karmaşık değildir. Eğer parite kontrol başarısız olursa, parite bitinden sonra bekleme süresinde bir A düzeyi göndererek bu bitin yeniden iletilmesi istenir. Bu durum, bu karakterin yeniden iletilmesine neden olur. Hata düzeltmenin bu formunun, RS232 arabirimi üzerinde direkt karşılığı yoktur.

TS Karakteri, başlangıç durumu cevabının ilk karakteridir. Bu, ya 3Fh ya da 3Bh olabilir. 3Fh, ters düzenin kullanılmış olduğu anlamına gelir. 3Bh ise direkt düzenin kullanılmış olduğu anlamına gelir.



Şekil 4.10 3B direkt düzenin karakter yapısı [1]

T0 Karakteri, genel format karakteridir. Bu karakter, hangi arabirim karakterlerinin ve kaç adet bilgi karakterin iletildiğini belirtmektedir. Bu karakterdeki bir hata inset box'ta gösterilmektedir. Yüksek nybble, hangi arabirim karakterlerinin gönderileceğini, düşük nybble ise kaç tane geçmişe ait karakterin gönderileceğini belirlemektedir. Arabirim karakterleri aşağıda açıklamaları ile birlikte verilmiştir:

1) TA_1 Karakteri

Bu karakter, clock seçimini kontrol eder. Örneğin VideoCrypt kod çözücüsü, 3.5712 MHz ve 7.1424 MHz gibi iki clock frekansını kullanmak için tasarlanmıştır. Bir 3.5712 MHz clock için değer 11h ve bir 7.1424 MHz clock için değer 31h'tır. Bunlardan farklı clock frekansı, 9600 baud hızını 3.5712 MHz'i 372 ile bölerek elde edildiği gerçeğinden yola çıkılarak oluşturulmalıdır [1].

2) TB_1 Karakteri

Bu karakter, kart için gerekli olan programlama voltajını ve akımını belirlemektedir. Bu karakterin en soldaki (önemli) biti her zaman sıfırdır. Sonraki en soldaki bitlerin ikisi, maksimum programlama akım faktörünü belirler. Örneğin, VideoCrypt sisteminin ATR durumunda, en soldaki bitler 10b'dir ve bunlar 100 akım faktörüne karşılık gelmektedir.

Programlama voltajını ise b1 ile b5 arasındaki bitler, volt cinsinden belirlemektedir. VideoCrypt başlangıç durumu cevabının (0101b) olması durumunda programlama voltajı 5 V'tur.

3) TC_1 Karakteri

Bu karakter, her bir karakterin arasına fazladan ne kadar bekleme süresi veya durdurma biti konulması gerektiğini belirler. Örneğin VideoCrypt kartında beş durdurma biti gerekmektedir. Bu karakterin amacı, kartın her bir karakteri bir sonraki karakter gelmeden önce işleme sokması için yeterli süreyi sağlamaktır.

4) TD_1 Karakteri

Bu karakter, birçok yönden format karakterine benzemektedir. Yüksek nybble, bir sonraki arabirim karakterinin bulunup bulunmadığını saptar. Düşük nybble ise kullanılması gereken protokolü belirler. Eğer orijinal Sky kartlarında olduğu gibi TD_1 karakteri iletilmemişse, o zaman protokolün T=0 olduğu kabul edilir.

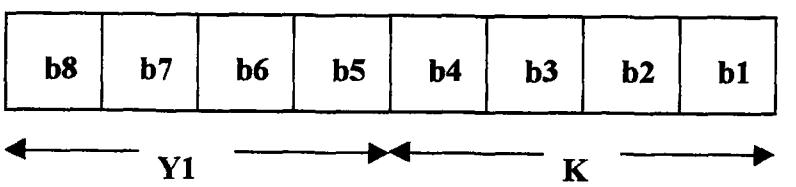
5) T1 - TK Karakterleri

Bu karakterler bilgi karakterleridir. Bunlar, kartın kendisi hakkında bilgi verir. Genellikle bu bölgedeki bilgiler yazılımın versiyonu, işlemci tipi, kart dağıtıcısı, kart üreticisi ve üretim tarihi hakkındadır.

6) TCK Karakteri

Bu karakter, son kontrol karakteridir. Bu, T0 ile TCK arasındaki bütün karakterlerin EXOR işleminin sonucunun sıfır olmasını kesinleştirmek için gerekli olan değerdir. Eğer sadece T=0 protokolü kullanılmışsa, bu kontrol karakteri iletilmez.

Şekil 4.11'de gösterilmiş olan Y1 değeri, hemen ardından gelen arabirim baytlarının olduğunu belirtmektedir. Buradaki bit kümesi ise bunların hangi karakterler olduğunu belirtmektedir.



Şekil 4.11 T0 formatında kullanılan karakterler [1]

Buradaki K değeri, iletilmiş olan bilgi karakterlerinin sayısını belirtmektedir. Bu değer, 0 ile

15 (0h ile Fh) arasında bir sayıdır. T0 formatında kullanılmış olan Y1 değerindeki bitlerin karakter karşılığı Çizelge 4.1'de gösterilmiştir.

Çizelge 4.1 T0 formatında kullanılmış olan Y1 değerindeki bitlerin karakter karşılığı [1]

Bit Değeri	Karakter Karşılığı
b8=1	TA_1 Karakteri (Clock Frekansı)
b7=1	TB_1 Karakteri (Maksimum Programlama Akımı ve Voltajı)
b6=1	TC_1 Karakteri (İlave Bekleme Süresi veya Durdurma Biti Talebi
b5=1	TD_1 Karakteri (Sonradan Gelen Arabirim Karakterleri ve Protokolü)

Birkaç farklı akıllı kartın ATR örnekleri Çizelge 4.2'de gösterilmiştir. Bu örnekler, bir orijinal Sky 07 karta, bir orijinal Sky 09 karta ve bir korsan Sky 07 karta aittir. İlk iki örnek orijinal Sky kartları, diğeri ise korsan bir karttır. Burada, Sky kartlarının gerçek Sky kartı olduğunu gösteren birkaç karakter mevcuttur. Ayrıca, gerçek kart dağıtım numarası ve hangi ayda dağıtıldığını gösteren bazı göstergeler vardır [1].

Çizelge 4.2 Birkaç farklı akıllı kartın ATR örnekleri [1]

07 serisi Sky akıllı kartı	09 serisi Sky akıllı kartı	07 serisi korsan akıllı kart
3F	3F	3F
7E	7E	FA
11	11	11
25	25	25
05	05	05
--	--	00
24	21	01
B0	B0	B0
05	12	02
00	00	3B
00	00	34
4D	4D	4D
59	59	59
00	00	00
01	00	81
80	00	80
53	53	
4B	4B	
07	09	
13	00	

Bu karakterlerin bazılarının asıl fonksiyonu bilinmemektedir. Bununla birlikte, mikrokontrolör kimlik bilgisine ilaveten üreticinin kimlik bilgisinin ve grup numarasının da

olduğu görülmektedir. Orijinal Sky kartları, TD_1 karakterini göndermemesine rağmen korsan kart göndermektedir [1].

En önemli bilgi karakterleri 4D ve 59'dur. VideoCrypt kod çözücü cihazı, içine yerleştirilecek olan her kartın bilgi karakterleri bölgesindeki bu belirli konumunda, bu baytların mevcut olup olmadığını görmek için kontrol etmektedir. Eğer bu karakterler bu konumlarda bulunamazsa, bu kart reddedilmektedir. Bu karakterlerin, VideoCrypt kimlik bilgisi veya kart tasarımcısının imzası olması da mümkündür.

B0 baytı, o kadar önemli olmadığı halde bütün kartlarda görülmektedir. Bu baytın, orijinal akıllı kartın bir 6805 tipi olduğunu gösteren bir mikrokontrolör kimlik bilgisi baytı olması mümkündür.

53 ve 4B karakterleri, Motorola firmasının kimlik bilgisini ASCII kodunda belirtiyor olabilir. Tabiki diğer karakterlerin gerçek ROM maskesi dağıtımını mı yoksa gerçekten programı mı tanımladığı açık değildir. Muhtemelen, VideoCrypt kimlik bilgisinden önceki bilgiler, News Datacom'un dahili program kimliği ile aynıdır [1].

Orijinal Sky kartlarının son iki karakteri en belirgin olanlardır. Sondan ikinci karakter, kartın 07 serisi mi yoksa 09 serisi mi olduğunu göstermektedir. Son karakter ise aboneliğin ne zaman sona ereceğini gösteren bir tamsayı değeri olabilir.

T=0 protokolünde kod çözücü, akıllı karta komutlar gönderebilmektedir. Bu komutları, karta giden veya karttan gelen bir veri iletimi takip eder. Bu protokol, karakter bazlı bir protokol olduğu için bu kart, sınırlandırılmış bazı akış kontrol yeteneklerine sahiptir. Bu yeteneklere ilaveten bu kart, prosedür baytı kullanılarak gerçekleştirilmiştir.

Kod çözücü, bir komutu başlatmak için karta beş baytlık bir üst bilgi (header) gönderir. Bu üst bilginin yapısı Şekil 4.12'de gösterilmiştir.

CLA	INS	P1	P2	P3

Şekil 4.12 Kod çözücünün bir komutu başlatmak için gönderdiği üst bilginin yapısı [1]

Buradaki CLA, sınıfı temsil etmektedir. VideoCrypt sisteminde bu daima 53'tür. INS ise talimattır. Bu, başlatılacak olan komutun talimatıdır. P1 ve P2 baytları VideoCrypt sisteminde kullanılmamıştır. Fakat EuroCrypt sisteminde kullanılmıştır. P3 baytı ise, verinin uzunluğunu bildirmektedir.

Çizelge 4.3 Prosedür baytlarının değerleri ve anlamları [1]

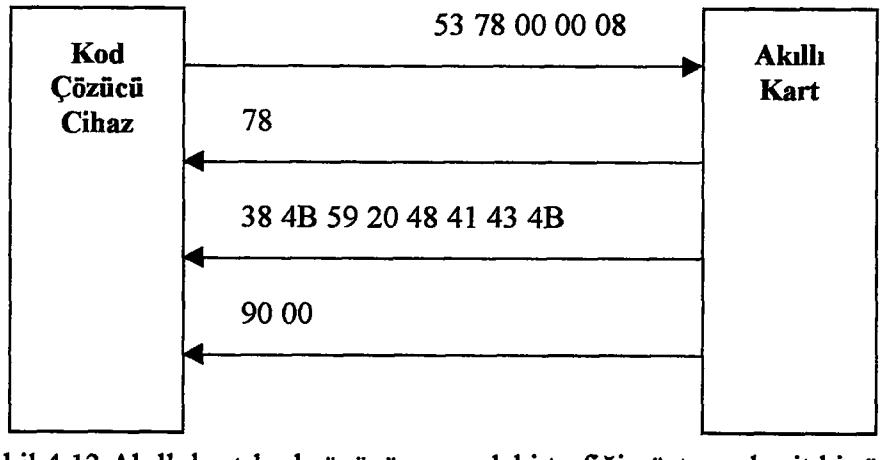
Bayt	Değeri	Anlamı ve Etkisi
ACK	INS	Gönder (Vpp'yi açma)
	INS +1	Gönder (Vpp'yi aç)
	NOT (INS)	Baytı Gönder (Vpp'yi açma)
	NOT (INS +1)	Baytı Gönder (Vpp'yi aç)
NULL	60h	Bekle
SW1	SW1	İletimin Sonu - SW2'yi Bekle

Bu üst bilginin gönderilmesinden sonra kod çözücü, prosedür baytını bekler. Prosedür baytının birkaç tipi vardır. Bunlardan en önemlisi onaylama baytı olan ACK baytıdır. Bu bayt kod çözücüye, veri iletimi ve programlama voltajının kontrol edilmesi hususlarında nasıl hareket etmesi gerektiğini bildirir (Çizelge 4.3). NULL baytı, kod çözücünün yeni bir prosedür baytını beklemesi gerektiğini bildirir. Durum sözcüğü baytları olan SW1 ve SW2, komutun bitmesinden sonra kartın durumunu iletir. Önemli bir hata olduğu zaman SW1 baytı kullanılmaktadır. SW1 hata koşulları Çizelge 4.4'te gösterilmiştir.

Çizelge 4.4 SW1 durum sözcüğü baytının hata koşulları [1]

Koşul	Hata Tanımı
6E	Talimat sınıfı desteklenmiyor
6D	Bilinmeyen talimat
6B	Yanlış adres veya referans
67	Yanlış uzunluk
6F	Bilinmiyor ve yanlış olduğu kesin

Şekil 4.13'te, akıllı kart-kod çözücü arasındaki trafiğe bir örnek gösterilmiştir. Kod çözücü akıllı karta, sekiz bitlik kod çözücü anahtarı istemek için bir üst bilgi gönderir. Bu komut için talimat 78h'tır. Verinin uzunluğu sekiz bayttır.



Şekil 4.13 Akıllı kart-kod çözücü arasındaki trafiği gösteren basit bir örnek [1]

Normal bir komut sonu, 90 00 ile gösterilmektedir. Eski kart trafiği izleme programlarının büyük bir kısmında bu işlem şu şekilde görünmektedir;

53 78 00 00 08 78 38 4B 59 20 48 41 43 4B 90 00

Temel bir iletişim programı, buna benzer bir blok yapısı gösterecektir. Fakat doğru sonuçların elde edilebilmesi için bir tercüme (çeviri) tablosu yazılmalıdır.

4.4 Korsan Akıllı Kart Emülatörleri

Korsan kod çözücü endüstrisi, her zaman yeniliklere açık olmuştur. Bu endüstri, orijinal aygıtlar ile tamamen aynı şekilde çalışacak korsan aygıtlar yaratmıştır. Bazı durumlarda bu korsan aygıtlar, orijinal modellerinden daha iyi sonuç vermiştir. Orijinal kod çözücülerde akıllı kartlar kullanılmaya başlandığı zaman buna da bir çözüm bulunması gerekiyordu. İlk hack işlemlerinden bir tanesi D2-MAC EuroCrypt sisteminde korsan bir akıllı kart kullanılarak gerçekleştirilmiştir [1]. Fakat, Card Tricks hack adı verilmiş olan bu hack işleminin piyasaya sürülmesi biraz zaman almıştır.

VideoCrypt sistemi için ilk çözüm ise, KENtucky Fried Chip hack adı verilmiş olan hack işlemiydi. Bu işlem orijinal kod çözücünün akıllı kart arabirimli 8052 mikrokontrolörünün, 07 serisi akıllı kart için anahtar ve algoritmaya sahip olan bir program ile modifiye edilmiş olan bir 8752 mikrokontrolörü ile değiştirilmesinden ibarettir [1]. Yani, bu hack işleminde bir akıllı karta ihtiyaç yoktur.

Fakat bu hack işlemi hiç pratik değildir. Çünkü, orijinal kod çözücünün içinin açılması, içindeki 8052'nin çıkarılması ve bunun yerine korsan 8752'nin takılması gerekliydi. Bu işi herkesin kendi başına gerçekleştirmesi çok zordu. Bununla birlikte, pek çok bilgisayar korsanının umut ettiği gibi ticari amaçlı olarak uygulanabilen bir hack işlemi değildi.

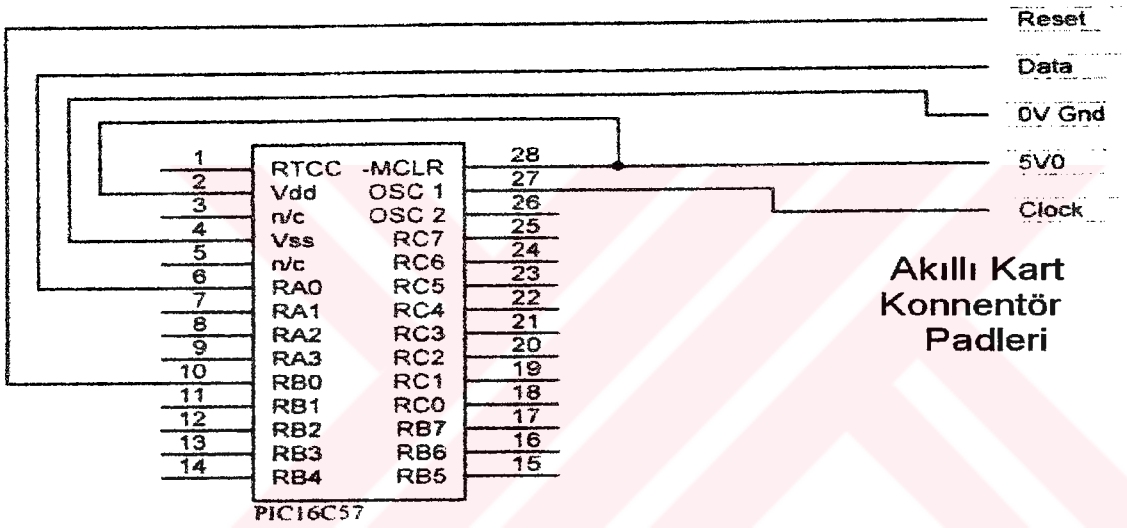
Daha sonra, VideoCrypt 07 serisi akıllı kart için ilk korsan akıllı kart imal edilmiştir. Bu kart, bir PIC16C54 mikrokontrolörünü baz almaktadır ve Ho Lee Fook kartı olarak adlandırılmıştı. Bu PIC16C54, Sky kanalının 07 serisi akıllı kartlarını emüle etmekteydi. Bunu, 8751 mikrokontrolörünü baz alan diğer versiyonları takip etmiştir. Fakat, bu iş için seçilebilecek en iyi mikrokontrolör PIC16C54'tür.

4.4.1 Card Tricks kartı

Akıllı kart bazlı bir sistemde gerçekleştirilmiş olan ilk akıllı kart hack işlemi Card Tricks

adını almıştır. Bu kart, 1992 yılının sonlarına doğru çıkmış olmasına rağmen 1993 yılına kadar bu piyasa tarafından duyulmamıştı [1]. EuroCrypt-M sistemi bu yöntemle hack edildiği zaman, France Telecom ve bu sistemi kullanan diğer kanallar dışında çok az kişi bu duruma şaşırmıştı. Daha sonra France Telecom, kullanmış olduğu EuroCrypt-M sisteminin bir Avrupa standardı olduğunu ilan ederek bu hack işlemine çok yardımcı oldu. Bu sistem bir standart olduktan sonra, sistemin orijinal şartnamesinin satın alınması mümkün hale geldi. Zaten kodlama algoritması herkes tarafından biliniyordu.

Card Tricks kartının baskılı devre kartı yerleşim planı alışılmışın dışındaydı. PIC16C54 mikroçipi, kart üzerinde oyulmuş bir slota yerleştirilmişti. Bunun amacı, kartın kalınlığını azaltarak düzelticilerin büyük bir bölümünde çalışmasını sağlamaktı. Fakat gerçekten çok başarılı modeller için, daha uzun bir baskılı devre kartlarının üretilmesi gerekliydi.



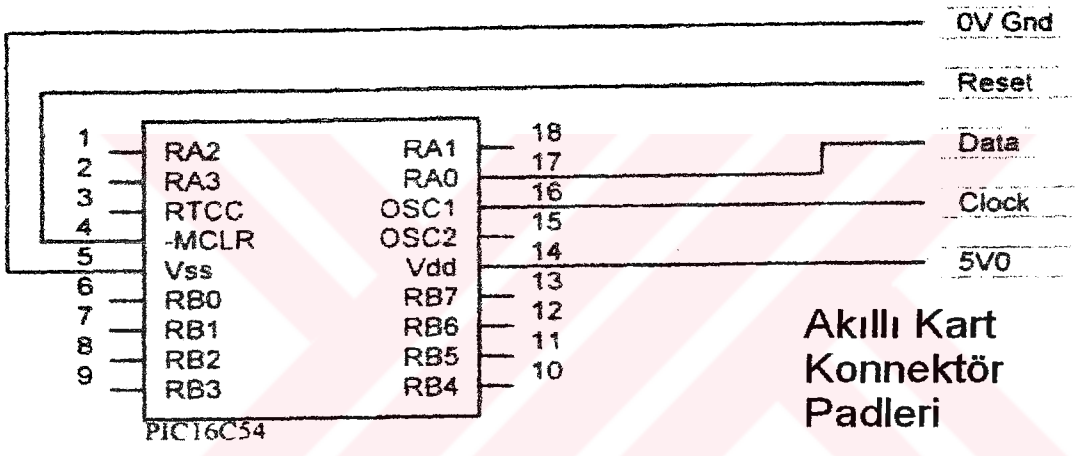
Şekil 4.14 PIC16C57 kullanarak gerçekleştirilmiş olan Card Tricks kartı [1]

Card Tricks kartı çok başarılı çalışmıştı ve tabiki bu durumdan televizyon kanalları rahatsız olmuştu. Bu yüzden, bu korsan karta elektronik karşı tedbir almak için kullanmış oldukları anahtarları değiştirdiler. Bu tip bir korsan kart için özellikle anahtar değişimi çok problem çıkarmaktaydı. Çünkü bu kartta kullanılmış olan PIC16C54 versiyonu sadece bir defa yazılabilen tipti. Yani bu mikroçip yeniden programlanamıyordu. Belleğin bazı alanları yeniden programlanabilmesine rağmen bu alanlarda yeni anahtarların depolanması büyük bir güvenlik riski yaratmaktaydı. Fakat bu elektronik karşı tedbir gerçekleştirildiği zaman diğer korsan EuroCrypt-M kartları da piyasaya çıkmaya başlamıştı.

4.4.2 Hoo Lee Fook kartı

Hoo Lee Fook kartının 8752 versiyonu, ticari amaçlı uygulanabilecek bir hack işlemi değildir. Çünkü orijinal kod çözücünün içinin açılmasını ve çok karmaşık bir takım işlemlerin yapılmasını gerektiriyordu. Bunun sonucunda, PIC16C54 bazlı Hoo Lee Fook kartı (Şekil 4.15) tasarlanmıştır. Burada, PIC16C54 mikrokontrolörünün sadece bir defa programlanabilen versiyonu kullanılmıştı.

PIC16C54, üç ay kullanıldıktan sonra bunun yerini PIC16C84 almıştır. PIC16C84'ün en büyük avantajı, tekrar programlanabilir olmasıdır. Sky ve News Datacom kanalları, korsan kartlara elektronik karşı tedbirler gerçekleştirmeye başladıkları zaman bu önemli bir faktör olmuştu. Piyasada, PIC16C84 kartının birkaç versiyonu görüldü. Temelde bu değişiklik, akıllı kart konnektör padlerine bağlanan veri hattı için farklı pinlerin kullanılmasından ibaretti.



Şekil 4.15 Orijinal Ho Lee Fook kartı [1]

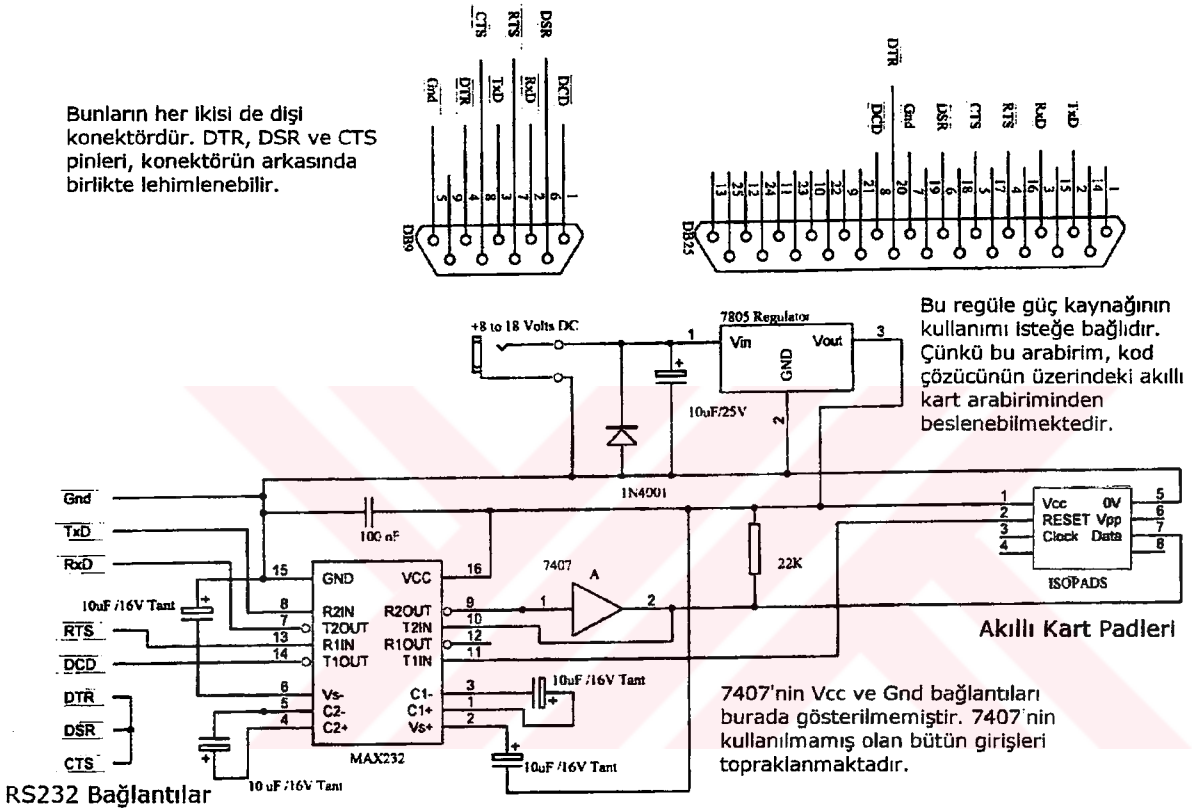
1993 yılının sonlarına doğru, News Datacom tarafından gerçekleştirilen karşı tedbirlerin peryodu arttırılmıştı [1]. Fakat alınan bu tedbirler sadece birkaç gün etkili olabiliyordu. Çünkü bilgisayar korsanları artık korsan kartları tekrar programlayabiliyordu. Daha sonra bazı bilgisayar korsanları, karta bir EEPROM ilave ederek bu karşı tedbir kodlarını depoladılar ve bu kodların kullanıcı tarafından seçilebilmesini sağladılar. Bu seçme işlemi, bir tuş takımı üzerinden gerçekleştiriliyordu.

4.4.3 Season arabirimi

Season programı, Markus Kuhn tarafından 1994 yılında geliştirilmiştir [1]. Bu program, orijinal bir Sky akıllı kartının bir bilgisayar ile emüle edilmesine izin vermektedir. Bilgisayarın seri portu, Season arabirimi adı verilen bu arabirim üzerinden kod çözücüye

bağlanmaktadır.

Şekil 4.16'da gösterilmiş olan bu arabirim, MAX232 RS232-TTL seviye konvertör mikroçipini baz almaktadır. Bu mikroçip, bilgisayar ile kod çözücü arasında akan veriyi RS232 seri portu ve kod çözücüdeki TTL kart arabiriminin her ikisinin de kullanabileceği düzeye dönüştürüyordu. Bu arabirim, korsan bilgisayar emülatörü piyasasının dönüm noktasıydı. Piyasada bu arabirimin ticari amaçlı birkaç değişik modeli mevcuttu. Bu modeller, temel arabirim tasarımını kullanmış olsa da bunlara değişik isimler verilmişti.



Şekil 4.16 Season arabiriminin devre diyagramı [1]

Bu arabirimin en iyi özelliği, seri üretiminin kolay olmasıydı. Ayrıca, seri bir arabirim ile bilgisayarların hemen hemen hepsinde çalışmaktaydı. Bu arabirim, uygun konnektör kablo kullanılarak bir Apple MAC'te de çalışmaktadır.

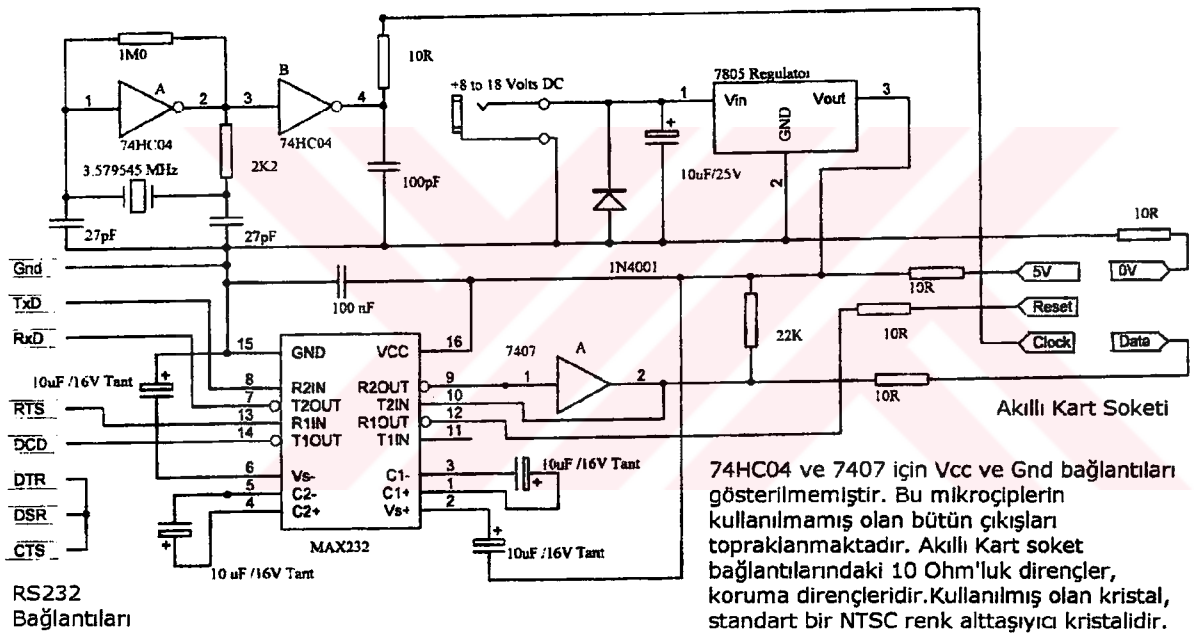
VideoCrypt Sky 10 serisi kart için çalışan bir Season tipi hack işlemi yoktu. Fakat D2-MAC EuroCrypt sisteminin, mevcut bir bilgisayar emülatör programı ile kodunun çözülerek izlenmesi mümkündür [1].

4.4.4 Phoenix arabirimi

Phoenix arabirimi, Season arabiriminin gelişmiş bir modelidir. Şekil 4.17'de gösterilmiş olan bu arabirim, uygun bir yazılım kullanılarak bilgisayarın seri portundan bir VideoCrypt kod çözücüsünün emüle edilmesini sağlamaktadır. Daha sonra bu bilgisayar, veri paketlerini gönderebilmekte ve alabilmektedir.

Phoenix ve Season arabirimleri arasındaki başlıca fark, Phoenix arabirimindeki RESET hattının bilgisayar tarafından kontrol edilmesidir. Ayrıca, karta clock sinyalini sağlamak için kristal kontrollü bir osilatör vardır ve kart bağlantılarında pull-up dirençler kullanılmıştır [1].

DSS Phoenix programı ile birlikte kullanılmış olan Phoenix arabiriminin Amerikan versiyonu, düzey konvertörü kullanmamakta ve kartı doğrudan seri porta bağlamaktadır. Karta clock sinyalini sağlayan 74HC00 bazlı bir osilatör entegre devresidir.

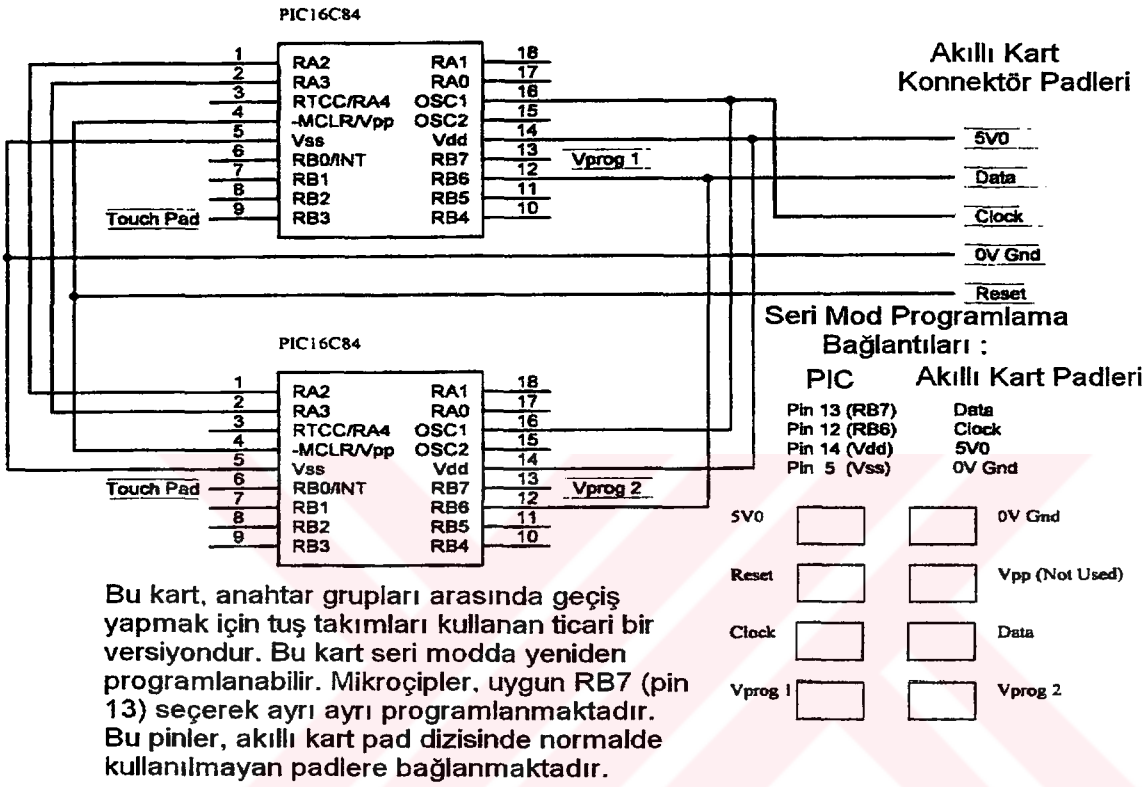


Şekil 4.17 Phoenix arabiriminin devre diyagramı [1]

4.4.5 D2-MAC EuroCrypt kartları

Korsan EuroCrypt kartlarının geliştirilmesi, PIC16C57 ile başlamıştır. Bu mikroçipin seçilmesinin nedeni, PIC16C54'ten daha fazla kapasiteye sahip olmasıydı. PicBuster bilgisi, geniş bir kitleye yayılmamıştı. Kanallar tarafından uygulanmış olan elektronik karşı tedbirlerden dolayı, kolay bir şekilde yeniden programlanabilen mikroçiplerin kullanılması

gerekiyordu. Bunun sonucunda, iki adet PIC16C84 mikroçipine sahip D2-MAC kartları (Şekil 4.18) çıkmıştır. Bu kartların, seri programlama modu kullanılarak tekrar programlanması amaçlanmıştır. Bunun sonucunda, akıllı kart konnektör padi düzeninin tamamı kullanılmıştır. Genellikle kartların büyük bir kısmı, Vpp padi bağlanmaksızın bu padlerin sadece beş tanesini kullanmıştır. Ayrıca, iki daha düşük pad PIC16C84'teki RB7 pinlerine bağlanmıştır. Bu, herbir PIC16C84'ün programlanabilmesi için ayrı ayrı seçilebilmesini sağlamaktadır [1].



Şekil 4.18 İki adet PIC16C84 mikrokontrolörüne sahip D2-MAC kartı [1]

Bu kartların yeniden programlanması, Henk Schaer programlayıcısı veya David Tait programlayıcısı gibi PIC programlayıcıları ile kolay bir şekilde gerçekleştirilebilmektedir. Bu işlem için sadece, konfigüre edilebilen bir kart soketi gerekmektedir. Bilgisayar korsanlarının büyük bir kısmı bu kartı deneme amacıyla, bir Genesis bloke edicisinden söktükleri kart soketini kullanıyorlardı. Daha sonra, uygun pinlere lehimlenmiş kablolar PIC programlayıcıya bağlanabiliyordu [1].

Önceki tasarımlarda tuş takımı kullanılmıştı. Bu padler, kullanıcının kanalların anahtarlar grupları arasında geçiş yapabilmesini sağlıyordu. Bu tasarımlar, ticari amaçlı tasarımlardı. Daha sonra, PicBuster bilgisi yayıldığı zaman bu kartın diğer versiyonları üretilmiştir. Bu versiyonlar, tuş takımına sahip değillerdi. Çünkü bilgisayar korsanlarının programlamadaki ustalığı ve bilgisi bu kartı terfi edilebilir yapmaya yeterliydi.

EuroCrypt-M ve EuroCrypt-S sistemlerinin çalışma biçimi öğrenildiği zaman bilgisayar korsanları, bu sistemlerin kodlarını çıkarabilecek düzeye geldiler ve böylece gerekli rutinler, tek bir PIC16C84'ün içine dahil edilebilir hale geldi. Bu durum, DES algoritmasının uygulamasını optimize ederek ve kritik olmayan rutinleri atarak gerçekleştirildi. Bu yüzden, tek PIC'li uygulamaların büyük bir kısmı yüksek kalitede görüntü rutinlerine sahip değildir.

Bu kartlar yeniden programlanabilir olduğu için sürekli olarak kullanımda kalabildiler. D2-MAC EuroCrypt'in esas kodunun uygulanmasından sonra, ikinci bir PIC16C84'e ihtiyaç kalmadı ve bu yüzden bu ikinci PIC16C84 mikroçipi, kartın devre yapısından çıkarıldı [1].

4.4.6 Bloke edici ve aktif hale getirici kartlar

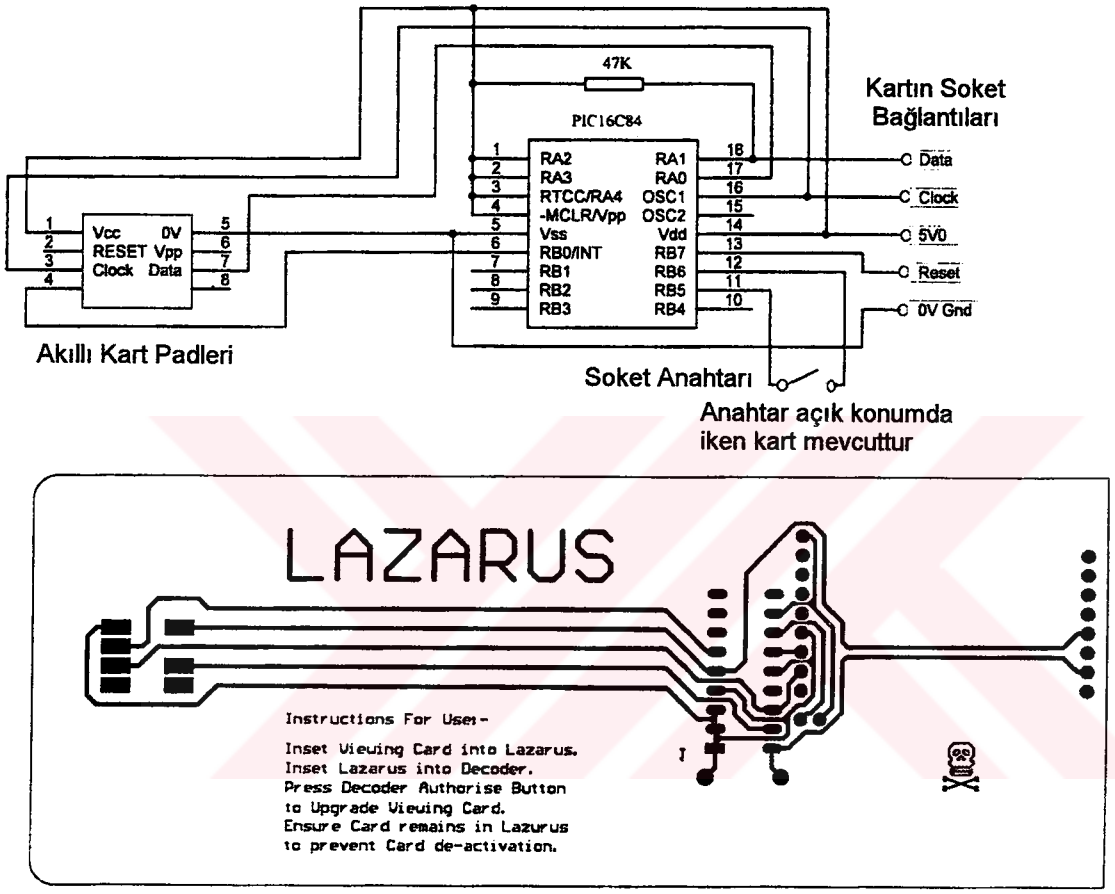
Sky ve News Datacom kanalları için 09 serisi akıllı kart, tam bir felakete neden olmuştur. Bunun sebebi, sistemin güvenilirliğinin tamamen kaybolmuş olmasıydı. Bunun meydana gelmesini sağlayan en önemli şey, bloke edici ve aktif hale getirici kartlardır. Bu kart tek başına, Sky ve News Datacom kanallarının kendi erişim kontrol sistemleri üzerindeki kontrollerini kaybetmelerine neden olmuştur [1].

Bloke edici ve aktif hale getirici kart, Phoenix programını baz almaktadır. İlk başta Sky Quickstart kartlarını aktif hale getirmek için Phoenix programı kullanılıyor ve daha sonra da korsan kart müşterisine bir bloke edici veriliyordu. Bu bloke edici, içindeki kartın seri numarası ile ilgili bir kapatma paketi olup olmadığını Sky kanalının yayınından gelen veri akışını kontrol ederek görmekteydi. Eğer böyle bir paket bulursa, bu kapatma paketinin korsan karta ulaşmasını engelliyordu. Bloke edici teorisi, korsan KENtucky Fried Chip mikroçipini baz almıştır [1].

1994 yılının sonlarına doğru Sky kanalı, yaklaşık bir milyon korsan kartı kapatmaya çalışmıştı. Fakat bu kartların büyük bir kısmı, bloke edici ve aktif hale getirici kartla beraber kullanılmış olduğu için kapatılamamıştır. Sky kanalının bu Quickstart kartları, artık bilgisayar korsanları tarafından satılır hale gelmiştir [1].

Büyük ölçüde modifiye edilmesi gereken orijinal kart mevcutken, aktif hale getirici program olan Phoenix ve bloke edicinin ayrı parçalar olması mantıklı değildi. Bunun sonucunda, kombine bloke edici ve aktif hale getirici kartlar ortaya çıktı. Bu kombine kart, seri üretilmişti. Lazarus, Genesis, Gemini ve SunBlocker gibi birçok ismi vardır. Şekil 4.19'da gösterilmiş olan Lazarus kartının devre diyagramı ve baskılı devre kartı şablonudur. Diğer versiyonların devre diyagramları bu firmaların internet sitelerinden temin edilebilir.

Sky ve News Datacom, bu olağandışı hack işleminin üstesinden gelebilmek için bir takım çalışmalar yapmıştır. Bunun sonunda, nanokomutlar (nanocommands) kullanmaya karar verilmiştir. Bu nanokomutlar, yetki verme paketinde gizlenmişti ve bu bloke edici aygıt bu nanokomutları sadece bir seri numarası gibi görmekteydi ve bu yüzden bu nanokomutların karta ulaşmasına izin vermişti. Bu nanokomutları alan korsan kartların çalışması bu şekilde engellenmiştir. Bununla birlikte, bu elektronik karşı tedbir uygulandıktan hemen sonra ilk sabit 09 serisi korsan kart piyasada mevcuttu [1].



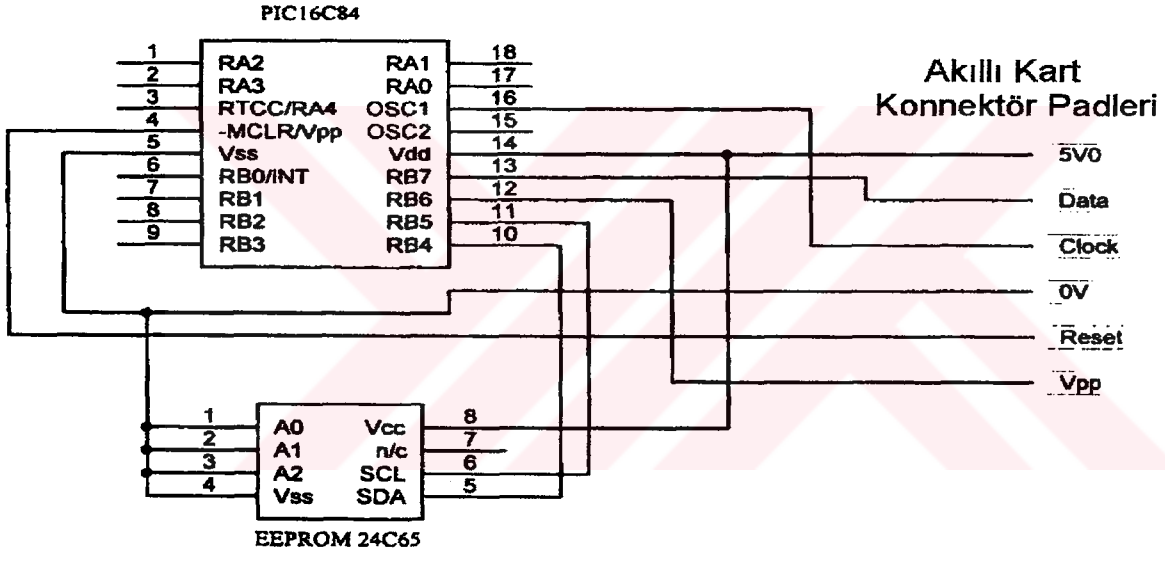
Şekil 4.19 Lazarus kartının devre diyagramı ve baskılı devre kartı şablonu [1]

4.4.7 09 serisi PIC16C84 korsan kartlar

News Datacom, 07 serisi kartlarda meydana gelen korsanlık probleminden sonra 09 serisi kartta büyük değişiklikler gerçekleştirmiştir. Bu yeni kartın algoritması öncekinden farklıdır ve çalışma şekli son derece karmaşıktır. Bir akıllı kartın havadan yeniden programlanabilme yeteneği, bir sistem için çok tehlikeli olabilecek bir özelliktir. Fakat buna rağmen News Datacom bunu kullanmaya karar vermişti. Tabiki bunu kullanmasının bazı nedenleri vardı. VideoCrypt sistemi, yeni abonelerin yükü altında ezilmekteydi. Başlangıçta, VideoCrypt

sisteminin iki milyon abonenin üzerinde kullanıcısının olabileceğinin düşünülmediği açıkça görülmekteydi [1]. Bu yüzden bu yeni kartın abone yönetim merkezi tarafından daha kontrol edilebilir ve erişilebilir yapmak için bazı metodlar gerekmekteydi. Buna ilaveten, herhangi bir korsan cihazı engellemek için bazı özellikler gerekliydi.

Ayrıca News Datacom, güvenlik konusunda bir adım daha ileri gitmişti. Kartın adres bölümünün tamamını, karma (hash) algoritmaların giriş verisi olarak okunabilir yapmıştır. Bunun sonucunda, her bir korsan akıllı kartın bu karma algoritmayı kullanmak için orijinal bir Sky kartının kopyasına sahip olması gerekli hale gelmiştir. Bu durum, 09 serisi akıllı kartın sonunu hazırlamıştır. Bilgisayar korsanları, bu karma fonksiyonun ana uygulamasına ve denetim işlemlerine sahip olduğunda ve birkaç nanokomut bilgisi ve bir Phoenix arabirimi ile Sky kartının adres bölümünü okuyabilmekteydi. Bu hack işlemine Vampire Hack adı verilmiştir [1].

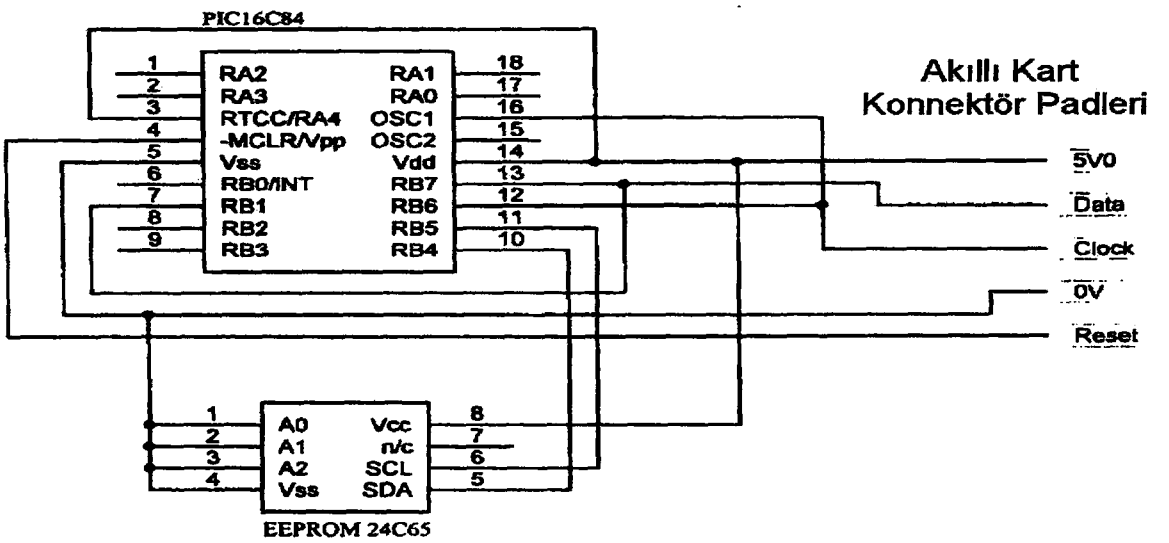


Şekil 4.20 09 serisi Sky akıllı kartı çalışma şekli için devre diyagramı [1]

İlk başta korsan kartlar, iki PIC16C84 ve bir 24C65 mikroçipine sahipti. Daha sonra, bir PIC16C84 ve bir 24C65'e sahip daha kararlı modelleri üretildi. 24C65 mikroçipi, orijinal Sky kartının bellek kopyasına sahipti. Bunu, Sky abone yönetim sisteminin tamamen çökmesi takip etti. Bunun başlıca nedeni, 09 serisi kartları hack edebilmesi için gerekli olan bilgilerin geniş çapta erişilebilir olmasıydı. İsteyen herkes kaynak kodunu, bilgisayar için Season tipi kart emülatörünü ve PIC kartlar için kaynak kodunu bu konu ile ilgili olan internet sitelerinden ve BBS'lerden temin edebilmekteydi.

Şekil 4.20 ve Şekil 4.21'de gösterilmiş olan olan devreler, en yaygın olarak kullanılmış olan devrelerdir. Bu devrelerde, veri bağlantısı için PIC16C84 mikroçipinin farklı portlarının

kullanılması gibi daha akıllıca varyasyonlar kullanılmıştır. Sky kanalı 31.10.1995 tarihinde 10 serisi akıllı kartına geçtiği zaman bu kartlar korsan D2-MAC kartına dönüştürülmüştür [1].



Şekil 4.21 07 serisi Sky akıllı kartı çalışma şekli için devre diyagramı [1]

4.4.8 COP8782 kartı

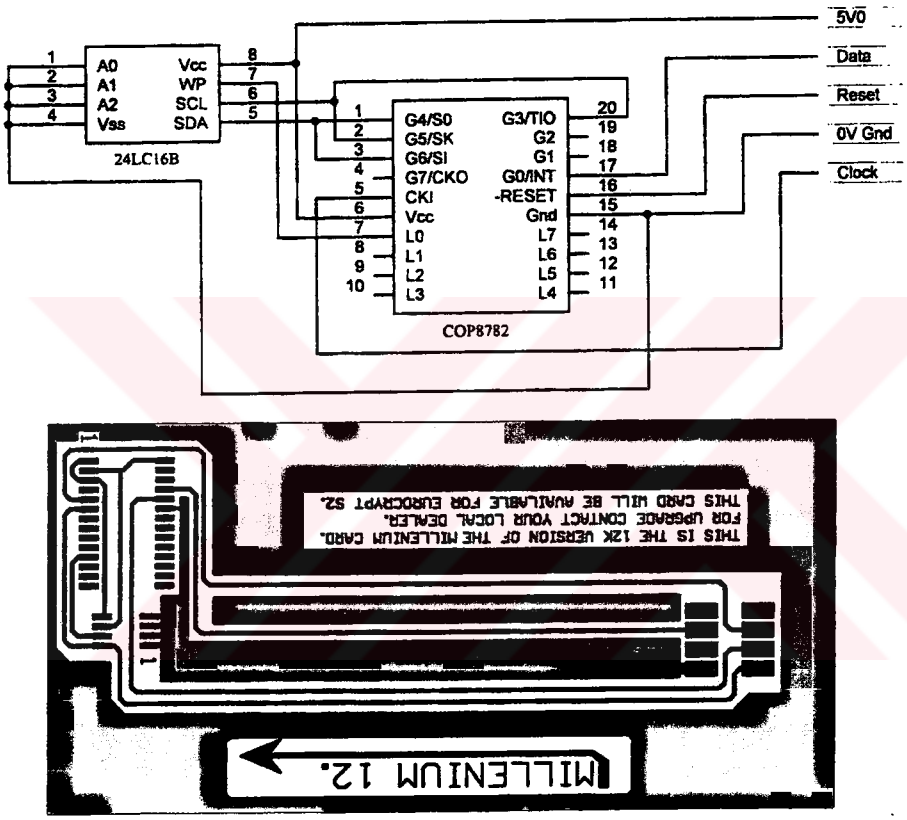
28.09.1995 tarihinde Avrupa'daki korsan kod çözücü endüstrisi bir kaos yaşamıştır [1]. Çünkü, FilmNet, TV1000 ve TV3 akıllı kartlarında kullanılmakta olan anahtarlar bu kanallar tarafından değiştirilmiştir. Bu yüzden, PIC16C84 bazlı korsan kartlar bundan sonra çalışmamıştır. Buna rağmen Battery kartlar, birkaç saat içinde bu yeni anahtarlar için terfi edilebilmiştir. Ayrıca, MACcess emülatörlerini kullanmakta olan diğer korsan kartlar da çalışmamıştır [1].

Kanalların gerçekleştirmiş olduğu bu elektronik karşı tedbirden birkaç gün sonra yeni korsan kartlar piyasaya çıkmıştır. Bu yeni kartlar FilmNet, TV1000 ve diğer D2-MAC EuroCrypt sistemi kullanan kanalların kodunu çözme yeteneğine sahipti. Bu kartlar (Şekil 4.22), National Semiconductor COP8782 mikrokontrolörünü ve bir 24LC16B EEPROM'unu baz almaktaydı.

Kaos, korsan kod çözücü endüstrisinin karşılaştığı yeni bir şey değildi. Kod değiştirildiğinde veya kanal tarafından hack işlemine elektronik karşı tedbirler alındığında, bu duruma hemen bir çözüm bulunabiliyordu. FilmNet ve TV1000 kanallarının anahtarlarını değiştirmesi durumu da bundan farklı değildi. Bazı korsan kart satıcıları, yatırımlarını korumak için yeni bir mikrokontrolöre (COP8782) geçmişlerdir.

İlk başta sadece birkaç şirket bu yeni kodu kartlarında kullanmıştı. Daha sonra bu yeni kod, diğer şirketlere de satılmıştır. Bu durumdaki yanlışlık, bu yeni kod satılırken güvenliksiz PIC16C84 mikroçipine yerleştirilmişti ve bu mikroçipten kod okunduğu zaman bu kod üzerinde hiçbir dağıtım kontrolü yoktu. Fakat COP8782 mikroçipi kullanıldığı zaman bu durum değişmiştir [1].

Korsan kod çözücü endüstrisinde, kodlaması okunan mikroçipler listesine eklenen diğer bir kart da COP8782 bazlı akıllı kartlar oldu. Daha sonra National Semiconductor, mikroçipin okunmasını zorlaştırmak için COP8782 mikroçiplerinde bazı değişiklikler gerçekleştirmiştir.



Şekil 4.22 COP8782 Millenium 12 kartının devre diyagramı ve baskılı devre bordu [1]

Korsan COP8782 mikroçipi, ana program ve küçük bir kod çözme rutini içermektedir. Bu yeni anahtar kodları, kodlanmış formatta EEPROM'un içinde saklanmıştır. Bu yüzden EEPROM içeriğinin kodunun çözülmesi yerine COP8782 mikrokontrolörü hedef alınmıştır ve bu başarıyla sonuçlanmıştır [1].

Bu rekabetçi korsan piyasaya güvenli anahtar dağıtım teknikleri sağladığı için COP8782 mikroçipine geçiş çok önemliydi. EEPROM'un içeriği DES algoritmasına benzer bir algoritma ile kodlanmıştır. Bu kod çözme anahtarı, üreticiden üreticiye değişiyordu. Yani, bir

üreticinin EEPROM terfisi diğer bir üreticinin kartında çalışmamaktaydı.

Fakat bu tip bir sistemin de hack edilmesi mümkündü. Bu yüzden, D2-MAC EuroCrypt sistemi tamamen tehlikeye altındaydı. Bir sistemin elektronik karşı tedbirler kullanma yeteneğinin olması alışılmış bir durumdur. Bunun en iyi örneği VideoCrypt 09 sistemidir. News Datacom, korsan bir battery kartındaki belleğin bir kısmını silmeyi içeren çok başarılı elektronik karşı tedbirler gerçekleştirebilmekteydi. Fakat D2-MAC EuroCrypt sistemi, bu özelliklerin hiçbirine sahip değildi [1]. EuroCrypt sisteminin tasarımcıları, kartın hack edilebilme olasılığını gözardı ediyorlardı. Bunun sonucunda, gerçekleştirdikleri elektronik karşı tedbirler sadece anahtar değiştirmekle sınırlı kalıyordu. Ayrıca, EuroCrypt sisteminin teknik özelliklerinin şirket tarafından yayımlanması da bilgisayar korsanlarının bu sistemin özelliklerini tamamen çözmesine yardımcı olmuştu.

Seçilmiş olan COP8782 sıradan bir mikrokontrolör değildir. Kullanılmış olan tip, sadece bir defa programlanabilen versiyondur ve bu yüzden yeniden programlanamamaktadır. Bu seçimin sebebi, bunun PIC16C84'ten daha güvenli bir mikroçip olması ve kısmen de olsa korsan EuroCrypt kartların çalışması için yakalanması gereken verinin sadece anahtar değişimi olmasıdır.

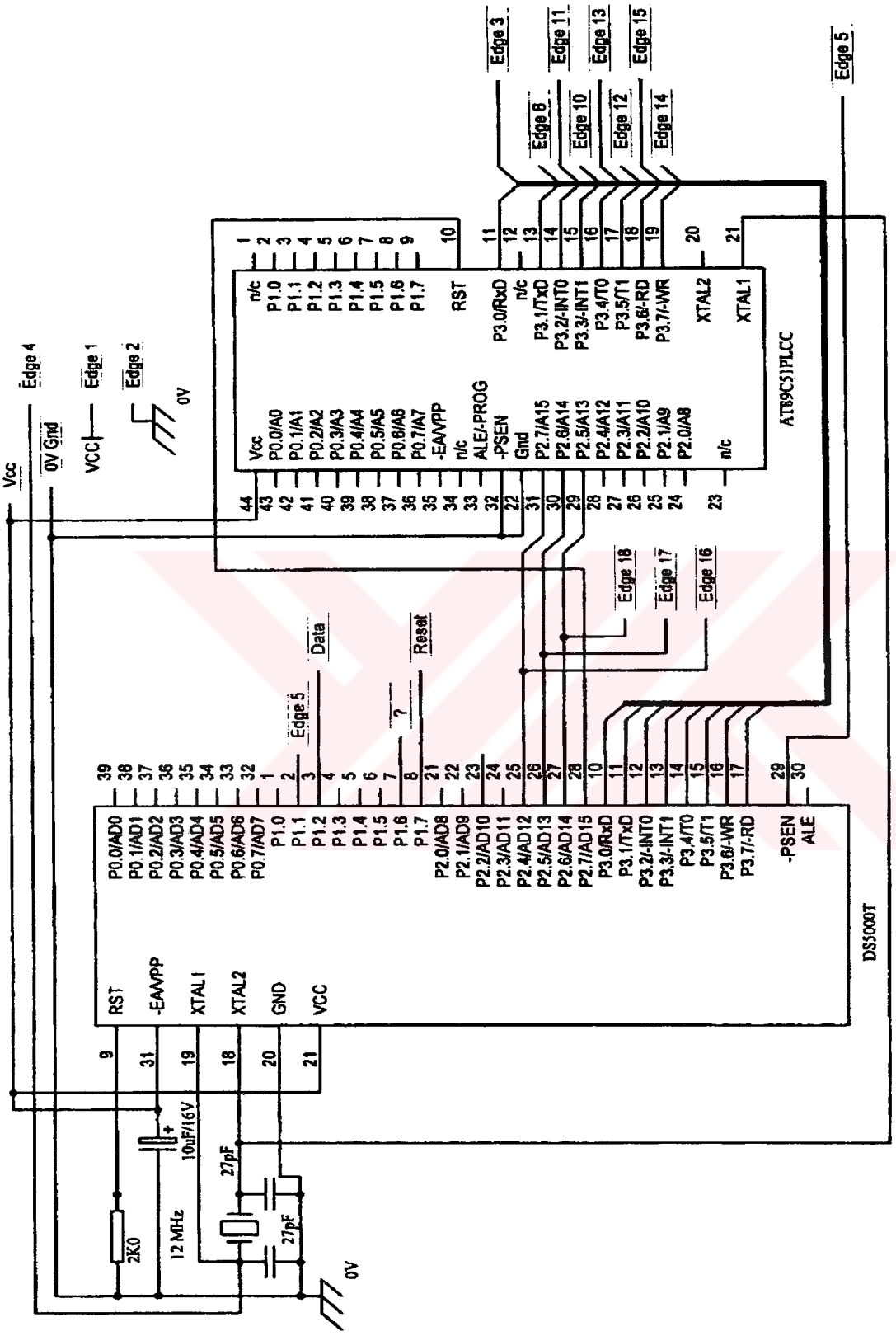
COP8782 kartlarda anahtarların değiştirilmesi, EEPROM'ların yeniden programlanması gibi basit bir durumdur. Yeni anahtarların, korsan kart üzerindeki COP8782'de kullanılmış olan üretici anahtarı ile kodlanması gerekmektedir. Bu yeniden programlama, bir PIC16C84 programlayıcısı kullanılarak gerçekleştirilebilmektedir. 26C16 ve 26C65 EEPROM'larını programlamak için gerekli olan programlar, bu konu ile ilgili internet sitelerinden ve BBS'lerden temin edilebilmektedir.

4.4.9 Battery kartlar

Avrupa'daki bilgisayar korsanları, birbirlerinin tasarımlarından ve bilgilerinden faydalanmaktaydı. Bu yüzden, büyük korsan üreticiler daha güvenli mikrokontrolörler kullanmaya yöneldiler ve korsan akıllı kart endüstrisinin başlangıç noktası olan PIC16C84'ün kullanımına son verilmişlerdir.

Seçilmiş olan güvenli mikrokontrolör Dallas 5002FP'ydi. Bu mikroçip, 8051 tipi bir mikrokontrolördür. Kullanmış olduğu bazı güvenlik elemanları sayesinde bu mikroçip Avrupa'da kullanılmış olan orijinal akıllı kartlardan bile daha güvenliydi. Bu mikroçipteki adres yolu ve veri, DES algoritmasına benzeyen bir algoritma ile kodlanmıştı. Bazı 8051

mikrokontrolörlerinden bu kodun, mikrokontrolörü aldatarak kolayca okunabilmesine rağmen Dallas 5002FP'de böyle bir problem yoktu [1].



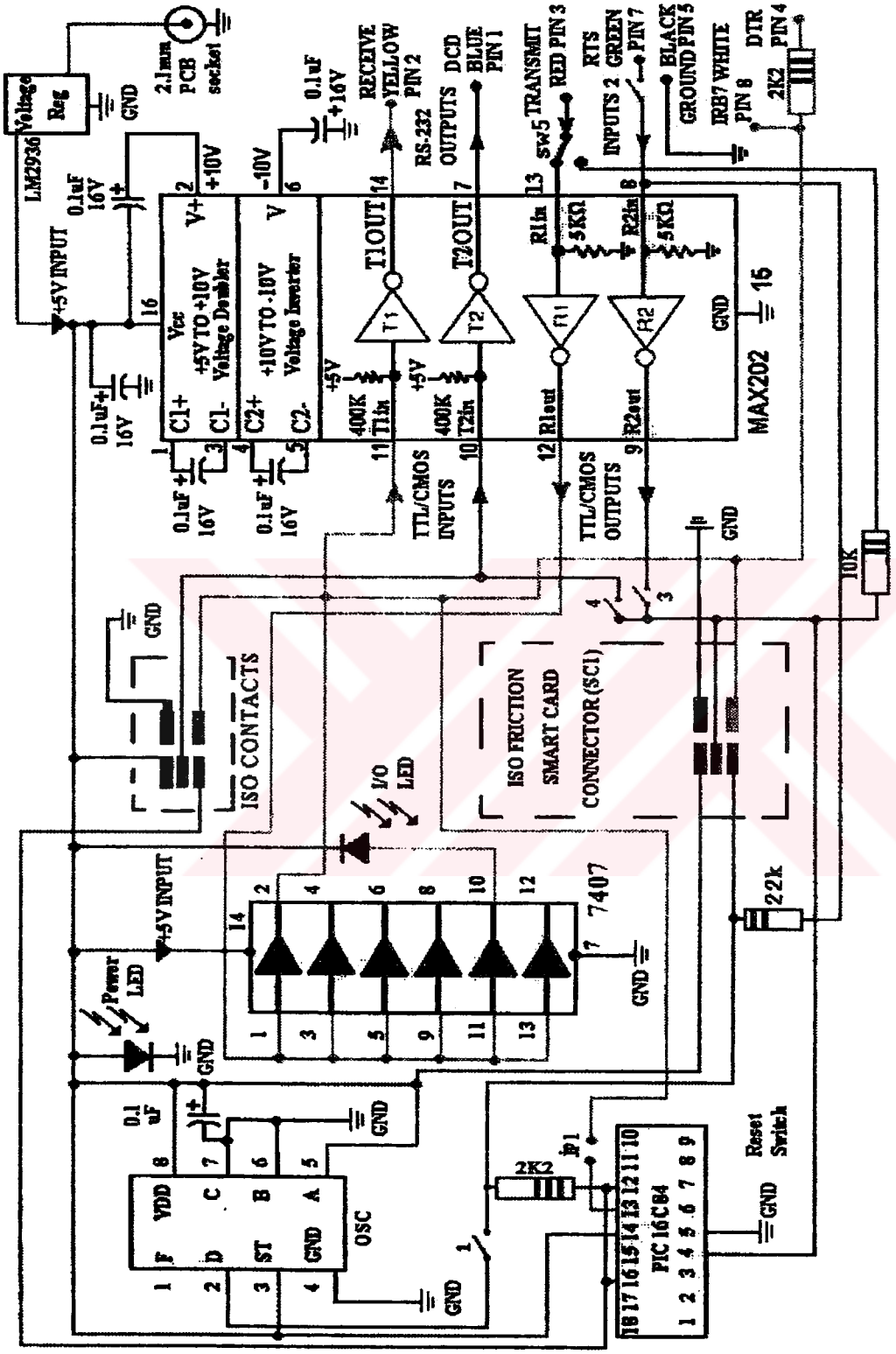
Şekil 4.23 Dallas 5002FP Battery kartının bir varyantının devre diyagramı [1]

Avrupa'da kullanılmış olan 32 kb RAM mikroçipli Battery kartlar, Dallas 5002FP ile büyük benzerliklere sahip bir tasarım kullanmaktaydı. Daha yeni bir tasarım, 128 kb'lık bir RAM mikroçipi kullanan Cardtronics A0 Amiga tasarımıdır. Megatek ve Cardtronics modelleri, Sky 10 serisi kartı emüle etmek için terfi edilebiliyordu. Fakat orijinal Sky kartındaki ASIC'i emüle etmek için ilave bir ASIC bordu gerekmekteydi. Avrupa'daki battery kartlarında bir tuş takımı vardı. Bu şekilde kart kullanıcısı, devre kartının üzerindeki tuşlar ile veya bir uzaktan kumanda ile terfi kodlarını girebiliyordu. Battery kartlarının Amerika'daki gelişimi, Avrupa'daki bu durum ile ortak bazı noktalara sahiptir.

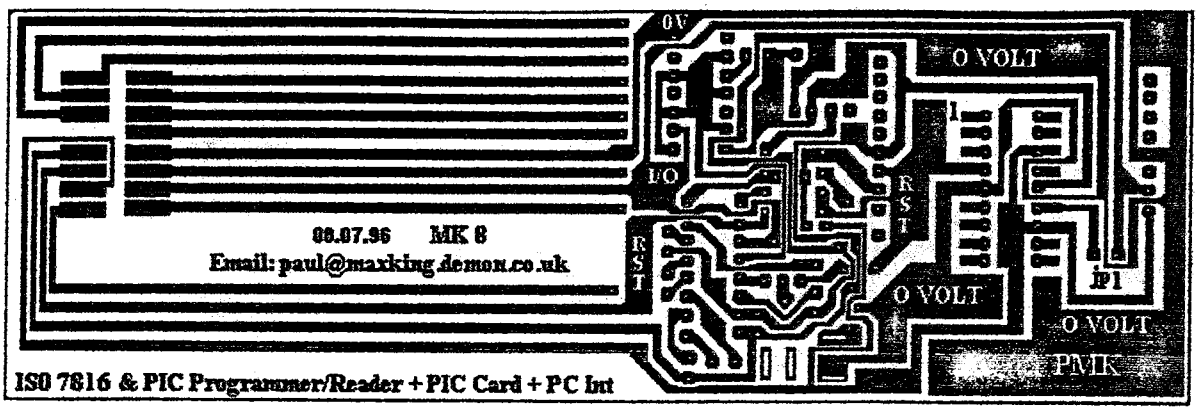
İlk korsan battery kartı Dallas 5002FP'yi baz almıştı. Korsan battery kartı tasarımcıları arasında bazı görüş farklılıkları vardı. Bu yüzden piyasada birkaç farklı kart tasarımı ortaya çıkmıştır. Bu yeni tasarımın bazıları Dallas 5002FP'yi kullanmamıştır. Bunun sebeplerinden biri, DirecTv ve News Datacom şirketlerinde güvenlik üzerine çalışan kişilerin Dallas 5002FP mikroçipinin kimlere satıldığını izlemesidir. Bunun diğer bir sebebi de, Dallas 5002FP mikroçipinin büyük miktarlarda Avrupa'daki korsan piyasa tarafından satın alınmasıdır. Şekil 4.23'te gösterilmiş olan devre, yeni DSS Battery kartlarından biridir. Bu kart, bir Dallas 5000T ve bir ATMEL AT89C51 mikroçipi kullanmaktadır. Programlama, bir kenar (edge) konnektörü aracılığıyla yapılmaktadır.

4.4.10 MK8 arabirimi

Paul Maxwell-King tarafından ticari amaçlı olarak gerçekleştirilmiş olan MK8 arabirimi (Şekil 4.24) Season arabiriminin, Phoenix arabiriminin ve bir PIC programlayıcısının entegre edilmiş halidir. Bu arabirimi kullanmak için gerekli olan yazılım, bu konu ile ilgili internet sitelerinde ve BBS'lerde mevcuttur. ISO standartlarına uygun olan bu cihaz, bir Pace MSS1000 alıcı entegre edilmiş kod çözücüsünde (satellite decoder) kullanılabilmektedir.

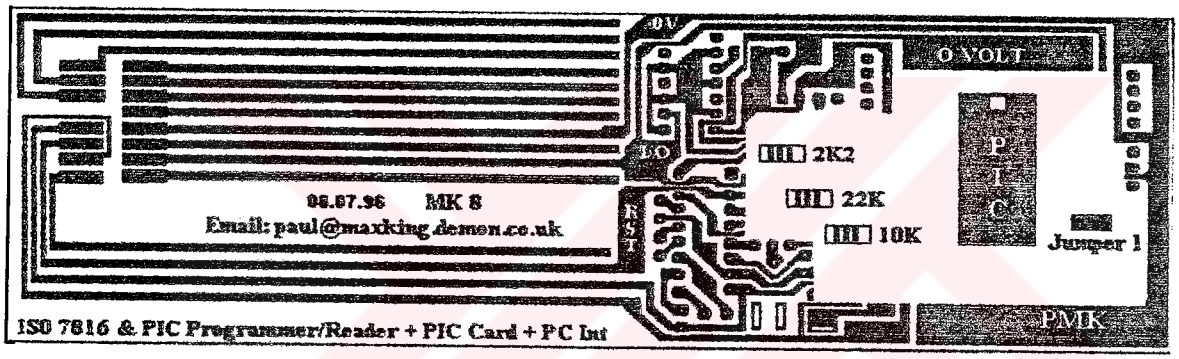


Şekil 4.24 MK8 arabiriminin devre diyagramı [1]

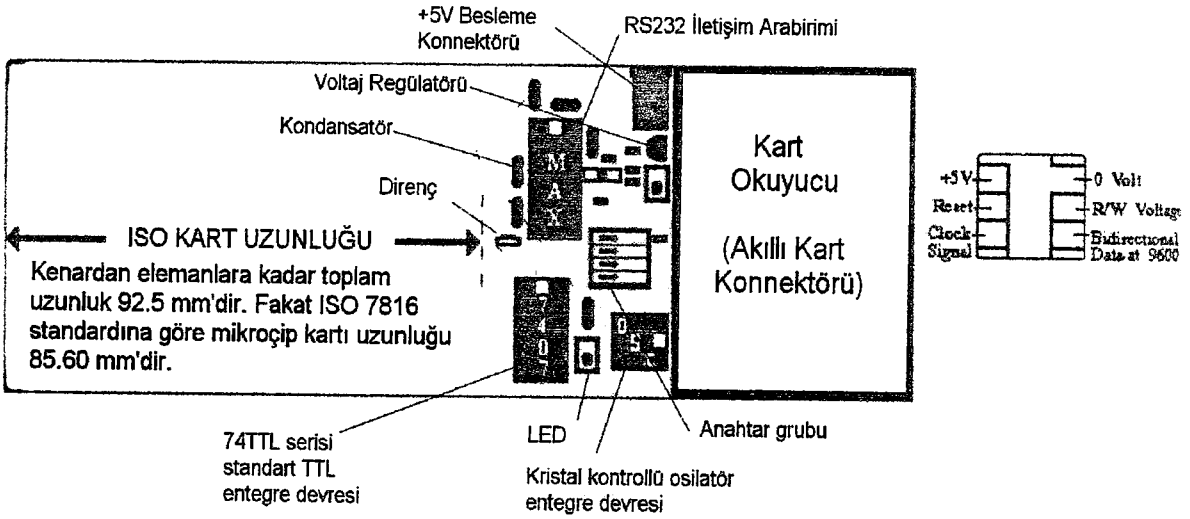


Şekil 4.25 MK8 arabiriminin baskılı devre kartının alttan görünüşü [1]

PIC16C84 mikroçipi, baskılı devre kartının alt kısmına (Şekil 4.26) monte edilmiştir. Bu PIC mikroçipinin 4'üncü pini resetlemek için, 5'inci pini topraklamak için, 12'inci pini (RB6) clock frekansı için, 13'üncü pini (RB7) veri için, 14'üncü pini +5 V besleme gerilimi (V_{dd}) için ve 16'ıncı pini ise clock sinyali için kullanılmaktadır.



Şekil 4.26 MK8 arabiriminin baskılı devre kartının alttan görünüşünde PIC'nin konumu [1]



Şekil 4.27 MK8 arabiriminin devre yapısının üstten görünüşü [1]

5. KARIŞTIRICI SİSTEMLERİN KODLAMA YAPISI

Bu bölümde, kriptoloji ve erişim kontrolü hakkında temel bilgiler verilmiştir. Kriptoloji, yüksek derecede uzmanlık ve kuvvetli matematik bilgisi gerektirir. Kriptanaliz ve kriptografi isimli iki alt bölümü vardır. Kriptanaliz, hack etme işleminde çok etkilidir. Kriptografi ise kod sistemlerinin geliştirilmesidir [1].

Erişim kontrolü, yetki verilmemiş kullanıcıların sisteme erişiminin reddedilmesidir. Bu, oldukça negatif bir tanım gibi görünebilir. Fakat bir erişim kontrol sisteminin, bir sisteme saldırı olma ihtimali düşünülerek tasarlandığı unutulmamalıdır. Bilgisayar korsanlarının sistemi hack edebilmesi için bu sistemin üstesinden gelmesi gereklidir. Fakat bir kriptosistemin, bu saldırılara karşı koymak için sadece çalışmasını doğru biçimde sürdürmesi yeterlidir.

Bir karıştırıcı sistemde kullanılmış olan bir erişim kontrol sisteminin, hack edilmeye karşı güvenli olması veya en azından hack edilmesinin çok masraflı olması gerekir. Bu yüzden bu karıştırıcı sistemde, iyi bir kriptografik sistemin kullanılması şarttır. İyi bir kriptosistem gerekli olmasına rağmen, güvenliği sağlayan unsur bu değildir. Kod çözücünün ve akıllı kartın teknolojisi güvenliği sağlayan temel unsurlardır.

Son yıllarda gerçekleştirilmiş olan akıllı kart bazlı hack işlemlerinin tamamı, orijinal akıllı karttaki algoritmaların ve anahtarların çıkarılması ve bunların korsan akıllı kartlarda emüle edilmesi prensibine dayanmaktadır. Çünkü akıllı kart teknolojisi bir takım kusurlara sahiptir. Genellikle elde edilmesi şart olan algoritmalar ve anahtarlar başka metodlarla hack edilmiştir. EuroCrypt-M sistemi, DES algoritması kullandığı için bu gruba dahil değildir [1].

VideoCrypt sisteminde gerçekleştirilmiş olan 07 serisi için Ho Lee Fook hack işlemi, Sky ve News Datacom kanalları için çok büyük problem olmuştur ve bu durum, 09 ve 10 serisi Ho Lee Fook kartlarına kadar devam etmiştir. Bilgisayar korsanlarının VideoCrypt 07 ve 09 serisi orijinal akıllı kartları hack etmek için kullanmış oldukları algoritmalar detaylı bir şekilde bu bölümde incelenmiştir.

Bir karıştırıcı sistemin bu sistemi kullanan kanal tarafından açıklanan teknik özelliklerine güvenmek potansiyel bir tehlikedir. Çünkü bu sistem özellikleri, bilgisayar korsanlarının saldırıya açık sistem modelleri geliştirmesini neden olmaktadır. Kanal tarafından açıklanmış olan teknik özelliklerin kullanıldığı bazı durumlarda, aslında bu özelliklerin tamamı kullanılmamıştır. Örneğin EuroCrypt-M sisteminde DES algoritması, başlangıç permütasyonu ve ters başlangıç permütasyonu çıkarılarak kullanılmıştır.

5.1 Kriptografinin Temelleri

5.1.1 Kodlama ve anahtar dağıtımı

Yalın metin olarak adlandırılan orijinal verinin kodlanması ve şifreli metin olarak adlandırılan kodlanmış veriye dönüştürülmesi prosedürüne "Kodlama Algoritması" veya "Anahtar" adı verilmektedir. Bu algoritmanın en basit formülü (5.1) eşiliğinde verilmiştir. Bu formüldeki *f* algoritmadır.

$$f(Yalın\ Metin + Anahtar) = Şifreli\ Metin \tag{5.1}$$

Bir kodlama sisteminin güvenliği, bu algoritmanın lineer olmamasına bağlıdır. Eğer bu algoritmadaki yalın metin ile şifreli metin arasında görülebilir bir ilişki varsa, o zaman bu sistemin hack edilebilme olasılığı yüksektir. Eğer bu ilişki lineer olmadığı için hemen fark edilemeyecek bir yapıya sahipse, o zaman bu algoritma yeteri kadar güvenlidir.

Bir sinyalin kodlanması kavramı aşırı derecede basittir. Yerine koyma (substitution) ve permütasyon adı verilen iki temel işlem vardır. Bunlar genellikle, sistemin güvenliğini arttırmak için birlikte kullanılmaktadır.

Yerine koyma işlemi, sinyalin bir elemanının başka bir elemanının yerini almasıdır. Örneğin, DDSO bu işleme göre 2456 olabilir. Bu örnekte harfler sayıların yerine geçmiştir. Bilgisayarda kullanılan ASCII kodları, aslında bir yerine koyma kodlama sistemidir. Herbir harf bir sayıya atanmıştır. Daha sonra bu sayılar, ikili (binary) eşdeğerleriyle bilgisayarda depolanabilmektedir.

Permütasyon işlemi, bir sistemdeki bitlerin başka bir sırayla karıştırılmasıdır. Örneğin, ABCDEF bu işleme göre BACDEF şekline çevrilebilir. Temel biçiminde bu sistem, kırılabilecek en basit sistemdir. Her lisanda belirli harflerin istatistiksel olarak gerçekleşme oranı daha fazladır. İngilizce'de en çok kullanılan harfler A, E, T, N'dir. Daha sonra TH, ST ve EE gibi harf çiftlerinin istatistiksel olarak gerçekleşme oranı yüksektir.

Bu temel teknikler, veri akışını güvenli bir biçimde kodlamak için birlikte kullanıldığı zaman bu kombinasyon, "Bileşke Şifre" olarak adlandırılmaktadır. Verinin bir veya daha fazla sabit bloğu bazen bir bileşke şifre kullanılarak kodlanmaktadır. Bu uygulama, "Blok Bileşke Şifre" olarak adlandırılmaktadır. DES algoritması bir blok bileşke şifredir.

Bir kodlama algoritmasındaki anahtarın görevi, kilitteki bir anahtarın görevi ile aynıdır. Bu algoritma, bir kilit gibi düşünülebilir. Anahtar bir yönde döndürüldüğünde veriyi kilitliyor

veya kodluyor, diğer yönde döndürüldüğünde ise verinin kilidini açıyor veya kodunu çözüyor.

En basit algoritma dijital EXOR fonksiyonunu kullanmaktadır. İki dijital bit bu fonksiyonda karşılaştırıldığı zaman sadece bitlerden biri yüksek olduğunda çıkış yüksek olmaktadır. Eğer bitlerin her ikiside yüksekse veya bitlerin her ikiside düşükse, o zaman çıkış düşük olmaktadır.

1) EXOR fonksiyonu kullanılarak kodlamaya bir örnek

Bu örnekte CAT sözcüğü, anahtar olan DOG sözcüğü ile kodlanmıştır. ASCII kodu kullanılarak bu harfler, bir sayı dizisi ile gösterilebilmektedir (Çizelge 5.1). Böylece CAT sözcüğü 67, 65, 84 ve DOG sözcüğü ise 68, 79, 71 olmaktadır. Eğer bu sayılar binary formlarına çevrilmişse, EXOR fonksiyonu uygulanabilir. Burada CAT sözcüğü yalın metin, DOG sözcüğü ise anahtardır.

Çizelge 5.1 EXOR fonksiyonu kullanılarak kodlama için verilmiş olan bir örnek [1]

CAT (Veri)	0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 0 0 1 1 0 0
DOG (Anahtar)	0 1 0 0 0 1 0 0 0 1 0 0 1 1 1 1 0 1 0 0 0 1 1 1
Çıkış	0 0 0 0 0 1 1 1 0 0 0 0 1 1 1 0 0 0 0 0 1 0 1 1
CAT	676584
DOG	687971
Şifreli Metin	071411

Aynı EXOR fonksiyonu kullanılarak bu anahtar, şifreli metinden yalın metne dönüştürülür.

2) EXOR fonksiyonu kullanılarak kod çözmeye bir örnek

Çizelge 5.2 EXOR fonksiyonu kullanılarak kod çözme için verilmiş olan bir örnek [1]

Çıkış (Şifreli)	0 0 0 0 0 1 1 1 0 0 0 0 1 1 1 0 0 0 0 0 1 0 1 1
DOG (Anahtar)	0 1 0 0 0 1 0 0 0 1 0 0 1 1 1 1 0 1 0 0 0 1 1 1
CAT (Veri)	0 1 0 0 0 0 1 1 0 1 0 0 0 0 0 1 0 1 0 0 1 1 0 0

Karşılaştırma yapılarak görüleceği gibi şifreli metin, anahtar ile EXOR'lanarak tekrar yalın metin haline dönüştürülmüştür (Çizelge 5.2). Sistemin çalışmasını sağlamak için göndericinin ve alıcının bir anahtara sahip olması gereklidir. Bu, bir veri akışını kodlamanın aşırı derecede basit bir metodu olmasına rağmen, televizyon kanallarının kullandığı sistemlerde genellikle anahtar uzunluğu çok büyük olduğu için bu sistemler, hack edilmeye karşı dayanıklıdır ve güvenlidir. Bununla birlikte, basit bir EXOR şifresi çok tehlikelidir.

Karıştırıcı sistemlerdeki problem, kodlanacak olan bilginin yalın İngilizce veya herhangi bir

bir lisan olmamasıdır. Bu bilgi çekirdek bilgisi, kanal yetki verme verisi veya sıralama verisidir. Aslında bu veri türü, tamamen ikili (binary) veya onaltılı (hexadecimal) akışıdır. Kripto algoritmaları bu veriyi kodlamakta ve bu verinin kodunu çözmektedir.

Bu bölümde, kripto algoritmalara bazı örnekler verilmiştir. Piyasadaki karıştırıcı sistemlerin büyük bir kısmı bu algoritmaları burada bahsedildiği gibi doğrudan kullanmamaktadır. Bu algoritmalarda değişiklikler yaparak bilgisayar korsanlarının işini güçleştirmektedirler. Bazı durumlarda bu değişiklikler, kod çözücünün veya akıllı kartın veriyi işlemesini sağlamak için gereklidir. Diğer durumlarda ise bu değişiklikler, algoritmayı daha güvenli yapmaktadır [1].

5.2 DES Algoritması

Son birkaç yıldır, DES algoritması üzerine yoğun çalışmalar yapılmıştır. Bu algoritmanın başlangıçta akademisyenler ve savunma uzmanları tarafından analiz edilmesine rağmen, VideoCipher sisteminin hack edilmesinden sonra bilgisayar korsanlarının da ilgisini çekmiştir. Bununla birlikte, bu algoritmanın Avrupa'daki en önemli uygulaması, EuroCrypt-M sisteminin bir parçası olarak kullanılmıştır [1]. Hesap yapma yeteneği bakımından 1985 ve 1996 yıllarındaki algoritmaların arasındaki fark çok büyüktür. 1985 yılında DES algoritması çok iyi bir algoritmaydı. Fakat 1996 yılında ise hassas uygulamalar için yeterince güçlü bir algoritma değildi. Genellikle bu algoritma, RSA algoritması gibi genel anahtar (public key) bazlı algoritmalar ile değiştirilmiştir

DES algoritmasının ilk formu 1971 yılında IBM tarafından yaratılmıştır [1]. Bu algoritmaya Lucifer ismi verilmişti ve Lloyds isimli bir firmaya satılmıştı. Mevcut olan bu algoritma, çok az kişinin bu algoritmayı hack edebilecek bilgisayar gücüne sahip olmasına rağmen aşırı derecede güvenli değildi. 1974 yılında bu algoritma güçlendirilmiştir. Lucifer adı verilmiş olan bu algoritma 128 bitlik bir anahtara sahiptir. A.B.D. Ulusal Standartlar Bürosu (US National Bureau of Standards) gizli olmayan hükümet verileri için kullanılabilecek standart bir kodlama algoritmasına gereksinim duymuştur. Ulusal Standartlar Bürosu'na sunulmuş olan versiyon 64 bite indirilmiş bir anahtara sahipti.

Ulusal Güvenlik Ajansı (National Security Agency), Amerikan savunmasının elektronik gözü ve kulağıdır [1]. Merkezi İstihbarat Ajansı (Central Intelligence Agency), doğruluk ve analiz çalışmaları ile ilgilenirken Ulusal Güvenlik Ajansı ilgi çeken bütün elektronik konuları izlemektedir. 128 bit anahtarlı bir DES algoritmasını hack etmek daha uzun zaman almaktadır. Fakat bunun 56 bit anahtarlı versiyonları, birkaç saat içinde hack edilebiliyordu.

Ulusal Güvenlik Ajansı, algoritmanın belirli elemanlarının yeniden yaratılmasını istediğini IBM firmasına bildirdi ve DES algoritmasının bu son formunda anahtar zayıflatıldı ve algoritmanın diğer bölümleri kuvvetlendirildi. Bu, Ulusal Güvenlik Ajansı'nın gerekli olduğu durumlarda DES algoritmasını hack edebilmesi için gerekliydi [1]. Bu, Ulusal Güvenlik Ajansı için normal bir girişimdi. Çünkü herhangi bir düşmanın eline geçmesi mümkün olan hack edilemez bir şifreleme sistemini sağlamak akıllıca olmazdı [1]. Ulusal Standartlar Bürosu, değiştirilmiş olan bu Lucifer algoritmasının DES olarak kullanılmasını 15.06.1977 tarihinde onaylamıştır [1]. Bu, Federal Information Processing Standards Publications 46 (FIPS PUB 46)'da belgelenmiştir.

VideoCipher II karıştırıcı sistemi, dijital ses verisini kodlamak için DES algoritmasını baz almıştır. Bunun sonucunda Amerika sınırları dışından çok içinde, bunu hack etme denemeleri için daha fazla bilgisayar zamanı ve beyin gücü gerekti. Bazı söylentilere göre bu durum, A.B.D. hükümet departmanlarını rahatsız etmişti [1]. Bu algoritma, genel bir çözüm bulunarak tam anlamıyla hiç bir zaman hack edilememiştir. DES algoritmasının nasıl hack edileceğine dair birkaç makale mevcuttur. Fakat, bu hack işlemleri çok fazla zaman gerektirdiği için kullanışsızdır. Karıştırıcı sistem algoritmalarının büyük bir kısmında olduğu gibi DES algoritmasının anahtarı aylık, haftalık veya günlük olarak değişmekteydi.

Avrupa'da DES algoritmasının kullanımı yaygın değildir. France Telecom'un EuroCrypt-M sisteminde bu algoritma, karma fonksiyon olarak kullanılmıştır. 1987 yılında, bu algoritmanın kriptografik olarak güvenli olduğu düşünülmekteydi ve bu nedenle France Telecom bu algoritmayı sisteminin merkezi olarak kullanmıştı [1].

DES algoritmasının birkaç uygulama metodu mevcuttur. Bu bölümde, bu metodlardan biri olan Electronic Code Book modu incelenmiştir. Bu metodda, 64 bitlik bir yalın metin bloğundan ve 64 bitlik bir anahtardan şifreli metin üretilmektedir. Bu versiyon, karıştırıcı sistem uygulamalarında en yaygın olarak kullanılmış olan metodlardan biridir. Çoğunlukla, bu algoritmanın yazılımda daha hızlı çalışması için baştaki ve sondaki permütasyonlar çıkarılmaktadır. Bu algoritma, EuroCrypt-M sisteminde de bu şekilde kullanılmıştır [1].

Yerine koyma ve permütasyon olmak üzere iki temel kodlama biçimi vardır. Permütasyon biçiminde, sadece dizideki bitlerin yerleri değişmektedir. Fakat bu bitler aynı değerlerini (1 veya 0) korumaktadır. Bazı durumlarda, bu tekniği tanımlamak için sözcük yer değiştirmesi kullanılmıştır. Yerine koyma biçiminde ise, bitlerin değerleri değişmektedir. Bu kodlama biçimlerinin her ikisinide kullanan kodlama tasarımı, genellikle bir bileşke şifre ile

ilgilidir. Giriş ve çıkışlar bitlerin bloklarında olduğu için DES algoritma biçimi, bir blok bileşke şifre ile ilgilidir.

5.2.1 Electronic Code Book modu

5.2.1.1 Anahtar üretimi

DES algoritmasının ilk aşaması anahtarların üretimidir. Bu anahtarlar, 56 bit genişliğindeki anahtar sözcükten üretilmektedir. 8, 16, 24, 32, 40, 48, 56 ve 64 bitleri parite bitleridir ve anahtar üretim prosedüründe kullanılmamaktadır. Çünkü bu prosedür tek paritededir.

Parite bitlerinden daha küçük olan anahtar sözcük, 1 satır x 56 sütunluk bir permütasyonu beslemektedir. Daha sonra bu permütasyon, 1 satır x 28 sütunluk daha küçük iki permütasyona ayrılmaktadır. Üst permütasyon C_0 olarak ve alt permütasyon ise D_0 olarak kullanılmaktadır. Bu permütasyon, Çizelge 5.3'te permütasyon seçimi 1 (PC-1) olarak gösterilmiştir. C_0 permütasyonunun ilk biti 57, ikinci biti 49 ve son biti ise 36 bitleridir. D_0 permütasyonunun ilk biti 63 biti ve son biti ise 4 bitidir.

Çizelge 5.3 Permütasyon seçimi - 1 [1]

PC-1
57 49 41 33 25 17 09
01 58 50 42 34 26 18
10 02 59 51 43 35 27
19 11 03 60 52 44 36
63 55 47 39 31 23 15
07 62 54 46 38 30 22
14 06 61 53 45 37 29
21 13 05 28 20 12 04

Bu anahtarları elde etmek için C_0 ve D_0'ın bitleri, bu prosedür aracılığıyla bir veya iki bit sola kaydırılmaktadır. C_0'a uygulanmış olan bir sola kaydırma, 57 bitinin sona gitmesiyle sonuçlanmaktadır. Bu yüzden, yeni birinci bit 49 biti olacaktır ve yeni sonuncu bit ise 57 biti olacaktır.

Bu sola kaydırma işlemi, göründüğünden daha az karmaşıktır. Ayrıca bu işlem, yazılımda veya donanımda kolayca gerçekleştirilmektedir. Bu sola kaydırma fonksiyonu, assembler düzeyi programlama dillerinin büyük bir kısmında ortak bir fonksiyon olarak mevcuttur. Ayrıca bu fonksiyon, C++ gibi bazı üst düzey programlama dillerinde de mevcuttur.

Anahtarlar, herbir bloğu C_n ve D_n alarak ve bunları PC-2'ye (permütasyon seçimi 2) girerek

bu bloklardan üretilmektedir. Bu bir 1 satır x 48 sütun permütasyondur. Anahtar uzunluğu 48 bit genişliğindedir. Bu permütasyondaki sayılar, [C_n, D_n] genişletilmiş bloğundaki bitlerin bağıl pozisyonlarını kapsamaktadır. C_n bloğunun ilk biti, PC-2'nin ilk biti ve son biti ise PC-2'deki 28 biti olacaktır. D_n bloğunun ilk biti, PC-2'deki 29 biti ve son biti ise PC-2'deki 56 biti olacaktır.

Çizelge 5.4a Permütasyon seçimi - 2 [1]

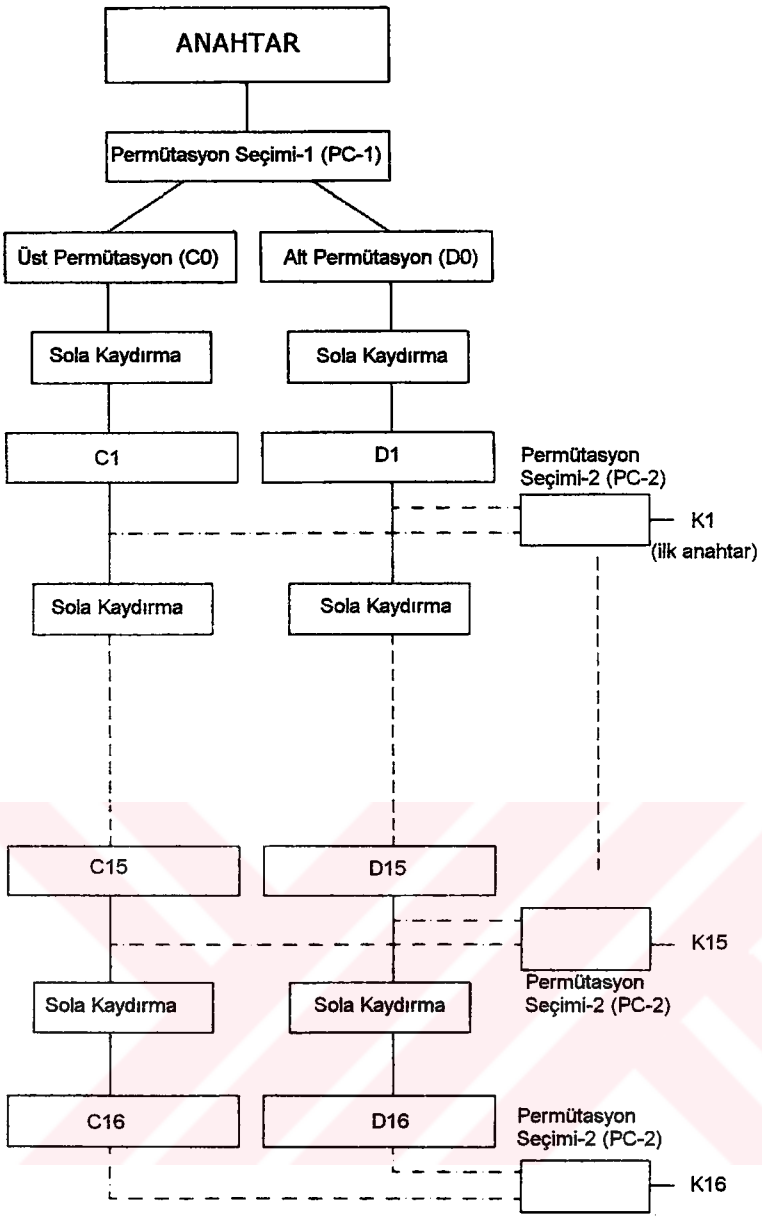
PC-2	C_0	D_0
14 17 11 24 01 05	57 49 41 33 25 17 09	63 55 47 39 31 23 15
03 28 15 06 21 10	01 58 50 42 34 26 18	07 62 54 46 38 30 22
23 19 12 04 26 08	10 02 59 51 43 35 27	14 06 61 53 45 37 29
16 07 27 20 13 02	19 11 03 60 52 44 36	21 13 05 28 20 12 04
41 52 31 37 47 55		
30 40 51 45 33 48		
44 49 39 56 34 53		
46 42 50 36 29 32		

Çizelge 5.4b Sola kaydırma tablosu [1]

Sola Kaydırma Tablosu			
Adım	Adım	Adım	Adım
01 1	05 2	09 1	13 2
02 2	06 2	10 2	14 2
03 2	07 2	11 2	15 2
04 2	08 2	12 2	16 1

Anahtar üretme işlemi, makina kodu düzeyinde hızlı olmaktadır. Ayrıca, bu işlem için yapılmış olan devre yapısı kullanarak da hızlıdır. İşte bu hız unsuru, bazı bilgisayar korsanlarının bunun bir paralel saldırı kullanılarak hack edilebileceğini düşünmelerine yol açmıştır.

Bilham Shamir'in "Differential Cryptanalysis of DES" ve Matsui'nin "Linear Cryptanalysis of DES" adındaki diğer saldırıları, bu uygulamanın sonucunda oluşmaya başlamıştır. Weiner tarafından yazılmış olan "DES Cracking Engine" isimli makalede, DES algoritmasını kırmak için gerekli olan aygıtın çok küçük bir yatırımla yapılabileceği belirtilmiştir [1]. Teknolojideki ilerlemeler sonucunda bu algoritma, herhangi bir hassas uygulama için güvenilir değildir. Bu algoritmayı hassas bir uygulamada kullanmayı düşünen birinin bu konuyu bir kere daha düşünmesi gerekir.



Şekil 5.1 DES anahtar üretiminin blok diyagramı [1]

5.2.1.2 DES kodlama rutini

DES kodlama rutini, karmaşık ve lineer olmayan bir rutin olduğu için güvenlidir. Giriş verisi veya yalın metin ile çıkış verisi veya şifreli metin arasında görülebilir bir ilişkinin olmaması gereklidir. Giriş bloğu veya yalın metin, 64 bit genişliğindedir. Bu blok ilk önce, içine ters permütasyon olarak adlandırılan 1 satır x 64 sütun permütasyonu sokularak permütasyona tabi tutulmaktadır. Daha sonra bu permütasyon, iki 32 bitlik bloğa ayrılmaktadır. Bu bloklar, L_0 ve R_0 olarak adlandırılmaktadır (Çizelge 5.5). L_0, ilk 32 elemanı ve R_0 ise ikinci 32 elemanı içermektedir.

Çizelge 5.5 Giriş bloğunun içine sokulan permütasyon blokları

L_0	R_0
58 50 42 34 26 18 10 02	57 49 41 33 25 17 09 01
60 52 44 36 28 20 12 04	59 51 43 35 27 19 11 03
62 54 46 38 30 22 14 06	61 53 45 37 29 21 13 05
64 56 48 40 32 24 16 08	63 55 47 39 31 23 15 07

Bu rutinin temel adım işlemi, bir modül kümesi olarak düşünülebilmektedir. L_0 ve R_0 ile başlayarak, R_0 ve K_1 ilk anahtarı f kodlama/kod çözme fonksiyonu modülüne sokulmaktadır. Kodlama/kod çözme fonksiyonu modülünün çıkışı, L_0 ile EXOR'lanmaktadır. EXOR işleminin çıkışı, yeni R_1 bloğunu vermektedir. R_0 bloğu da yeni L_1 bloğu olmaktadır. Bu döngü, L_{15} ve R_{15} bloklarına kadar bu şekilde devam etmektedir.

L_{16} ve R_{16} blokları, ön çıkış (preoutput) blokları adı verilmektedir. Bunların dizisi [R_{16}, L_{16}] aralığıdır. R_{16}, f kodlama/kod çözme fonksiyonu modülünün çıkışı ile L_{15}'in EXOR'lanmasıdır. Kodlama fonksiyonu modül girişleri R_{15} ve K_{15} 'tir. Ön çıkış bloğu, ters başlangıç permütasyonu içine sokulmaktadır (Çizelge 5.6). Ters başlangıç permütasyonu, çıkış bloğunu vermektedir. Bu blok, şifreli metindir ve 64 bit genişliğindedir.

Çizelge 5.6 Başlangıç permütasyonu ve çıkış bloğunu veren ters başlangıç permütasyonu

Başlangıç Permütasyonu	Ters Başlangıç Permütasyonu
58 50 42 34 26 18 10 02	40 08 48 16 56 24 64 32
60 52 44 36 28 20 12 04	39 07 47 15 55 23 63 31
62 54 46 38 30 22 14 06	38 06 46 14 54 22 62 30
64 56 48 40 32 24 16 08	37 05 45 13 53 21 61 29
57 49 41 33 25 17 09 01	36 04 44 12 52 20 60 28
59 51 43 35 27 19 11 03	35 03 43 11 51 19 59 27
61 53 45 37 29 21 13 05	34 02 42 10 50 18 58 26
63 55 47 39 31 23 15 07	33 01 41 09 49 17 57 25

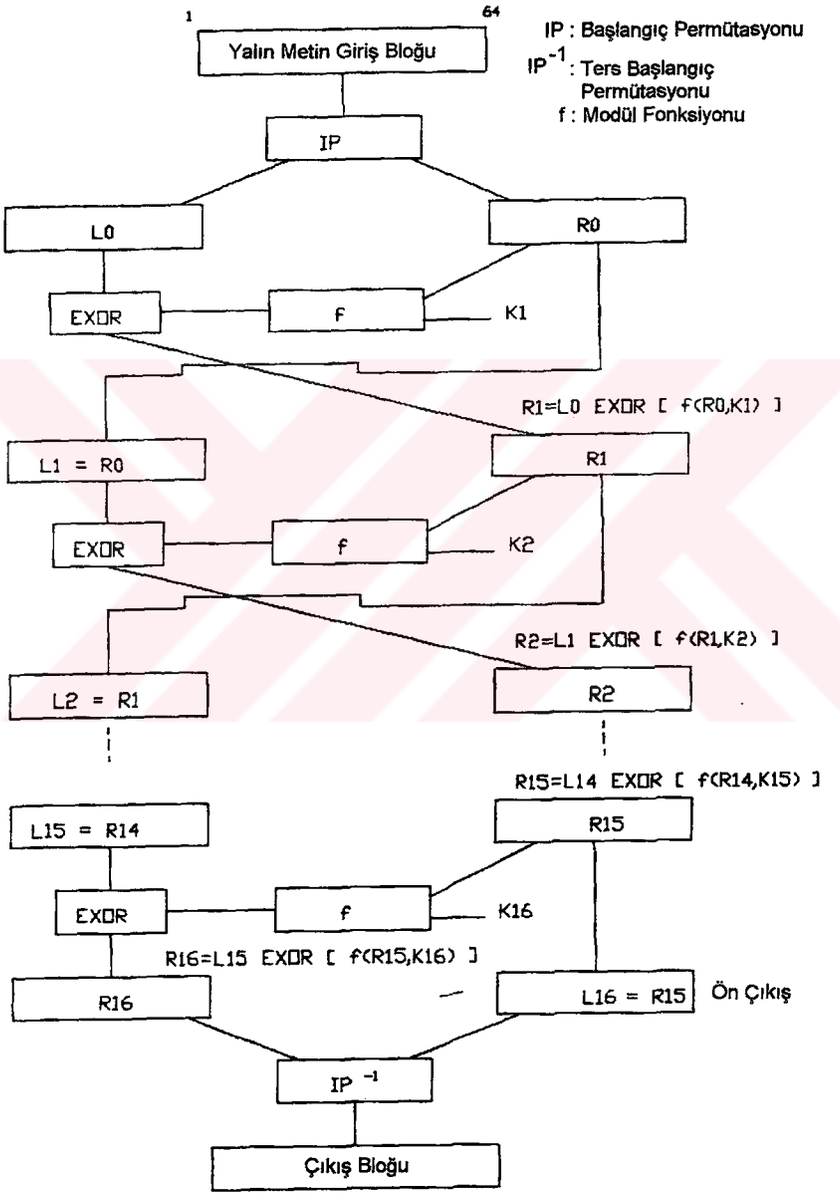
5.2.1.3 DES kodlama/kod çözme fonksiyonu

Bu fonksiyon modülünün çalışma şekli oldukça basit olmasına rağmen karmaşık görünmektedir. Fakat, bu işlemin bir insan beyni için değil bir bilgisayar için optimize edildiği unutulmamalıdır.

R bloğu 32 bit genişliğindedir. Bu bloğun 48 bit genişliğinde bir bloğa genişletilmesi gerekmektedir. Bu iş için kullanılmış olan permütasyona E-Bit Seçme Tablosu (E-Bit Selection Table) adı verilmektedir. Buradaki sayılar, R bloğundaki bit konumlarına işaret

etmektadir.

R bloğundan E ile üretilmiş olan 48 bit genişlikli blok, daha sonra 48 bit genişlikli bloğu üretmek için anahtar ile EXOR'lamaktadır. Bu blok, sekiz adet 6 bit genişlikli bölüme ayrılmaktadır. Bu 6 bit genişlikli bölümler S_1'den S_8'e kadar sekiz seçme fonksiyon modülüne girilmektedir. Bu modüller, 6 bit giriş bölümü için bir 4 bit blok seçer. Ayrıca bu modüller, 4 satır x 16 sütunluk matristir. İkili (binary) sayılarla uğraştığımız için bir 0 satırına ve bir 0 sütununa sahip olmamız gereklidir.



Şekil 5.2 DES kodlama rutininin blok diyagramı [1]

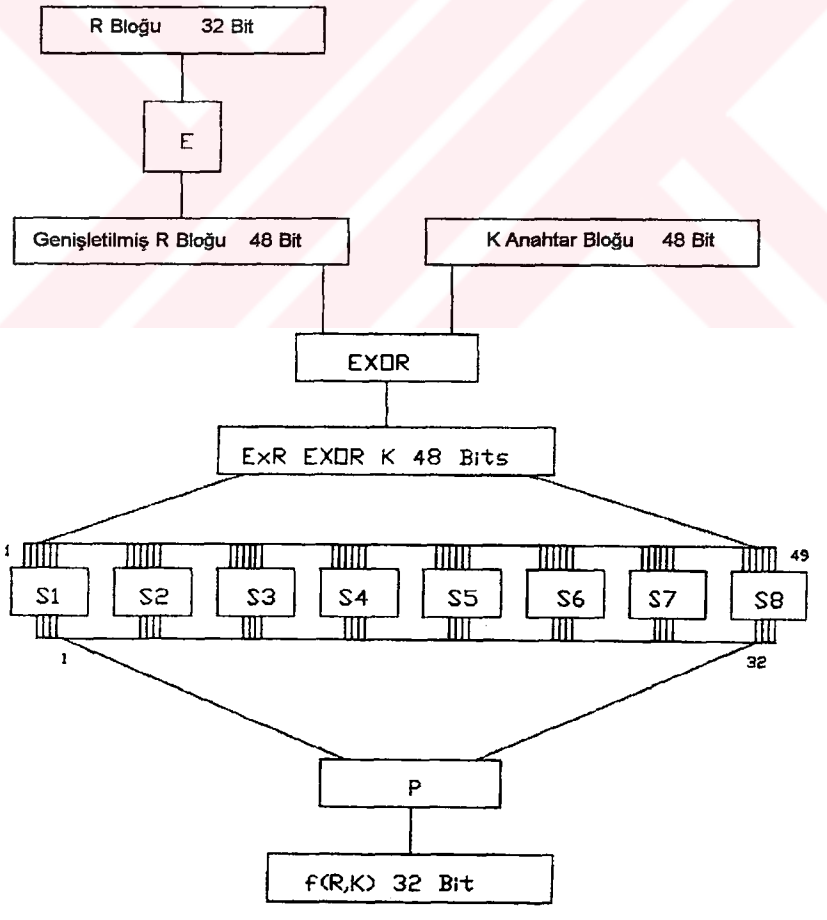
Bu 6 bit giriş bölümünün ilk ve son bitleri, satırı tanımlamak için kullanılmaktadır. Muhtemel kombinasyonlar 00, 01, 02 ve 03'tür. Bunlar, onluk (decimal) bazda 0, 1, 2 ve 3'e karşılık

gelmektedir. Bu 6 bit giriş bölümünün kalan 4 biti, sütunu tanımlamak için kullanılmaktadır. Bu bitler, 0000 ile 1111 arasında veya onluk bazda 0 ile 15 arasında değişmektedir.

Bu kavramı örnekle açıklamak için, S_1 için giriş bölümü olarak 010111'i kullanalım. İlk ve son bitler satırı belirtmektedir. Bu yüzden, satır 01'dir veya satır 1'dir. Kalan bitler ise sütunu belirtmektedir. Bu yüzden, sütun 1011'dir veya onluk bazda 11'dir. Satır sayısı 1 ve kolon sayısı 11'dir. S_1 permütasyonunda bu koordinatlardaki sayıların değerlerini kontrol ederek, 4 bitlik sayıyı elde ederiz. Bu konumdaki bu sayının değeri 11'dir veya ikilik bazda 1011'dir.

Bu çalışma şekli, sekiz adet 6 bit giriş bölümü ve bunların kendi seçme fonksiyon modülleri veya matrisleri için başarılmaktadır. Bunun sonucu, 32 bit genişlikli bir bloktur.

S_1 ile S_8 arasındaki seçme modüllerinden gelen 32 bit genişlikli çıkış, 1 satır x 32 sütunluk P permütasyonuna girilmektedir. Bu permütasyon, Permütasyon Fonksiyonu (P) olarak adlandırılmaktadır. Bu sayılar, seçme modülünden gelen 32 bit genişlikli çıkıştaki bitlerin konumunu göstermektedir. Bu sayılar, soldan sağa doğru akmaktadır.



Şekil 5.3 DES kodlama/kod çözme fonksiyonunun blok diyagramı [1]

Çizelge 5.7 Seçme modülleri, seçme tablosu ve P permütasyonu

Seçme modülleri (S-Boxes)	E-Bit Seçme Tablosu
S_1	32 01 02 03 04 05
14 04 13 01 02 15 11 08 03 10 06 12 05 09 00 07	04 05 06 07 08 09
00 15 07 04 14 02 13 01 10 06 12 11 09 05 03 08	08 09 10 11 12 13
04 01 14 08 13 06 02 11 15 12 09 07 03 10 05 00	12 13 14 15 16 17
15 12 08 02 04 09 01 07 05 11 03 14 10 00 06 13	16 17 18 19 20 21
S_2	20 21 22 23 24 25
15 01 08 14 06 11 03 04 09 07 02 13 12 00 05 10	24 25 26 27 28 29
03 13 04 07 15 02 08 14 12 00 01 10 06 09 11 05	28 29 30 31 32 01
00 14 07 11 10 04 13 01 05 08 12 06 09 03 02 15	
13 08 10 01 03 15 04 02 11 06 07 12 00 05 14 09	
S_3	
10 00 09 14 06 03 15 05 01 13 12 07 11 04 02 08	
13 07 00 09 03 04 06 10 02 08 05 14 12 11 15 01	
13 06 04 09 08 15 03 00 11 01 02 12 05 10 14 07	
01 10 13 00 06 09 08 07 04 15 14 03 11 05 02 12	
S_4	
07 13 14 03 00 06 09 10 01 02 08 05 11 12 04 15	
13 08 11 05 06 15 00 03 04 07 02 12 01 10 14 09	
10 06 09 00 12 11 07 13 15 01 03 14 05 02 08 04	
03 15 00 06 10 01 13 08 09 04 05 11 12 07 02 14	
S_5	
02 12 04 01 07 10 11 06 08 05 03 15 13 00 14 09	
14 11 02 12 04 07 13 01 05 00 15 10 03 09 08 06	
04 02 01 11 10 13 07 08 15 09 12 05 06 03 00 14	
11 08 12 07 01 14 02 13 06 15 00 09 10 04 05 03	
S_6	
12 01 10 15 09 02 06 08 00 13 03 04 14 07 05 11	
10 15 04 02 07 12 09 05 06 01 13 14 00 11 03 08	
09 14 15 05 02 08 12 03 07 00 04 10 01 13 11 06	
04 03 02 12 09 05 15 10 11 14 01 04 06 00 08 13	
S_7	
04 11 02 14 15 00 08 13 03 12 09 07 05 10 06 01	
13 00 11 07 04 09 01 10 14 03 05 12 02 15 08 06	P Permütasyonu
01 04 11 13 12 03 07 14 10 15 06 08 00 05 09 02	16 07 20 21
06 11 13 08 01 04 10 07 09 05 00 15 14 02 03 12	29 12 28 17
S_8	01 05 23 26
13 02 08 04 06 15 11 01 10 09 03 14 05 00 12 07	05 18 31 10
01 15 13 08 10 03 07 04 12 05 06 11 00 14 09 02	02 08 24 14
07 11 04 01 09 12 14 02 00 06 10 13 15 03 05 08	32 27 03 09
02 01 14 07 04 10 08 13 15 12 09 00 03 05 06 11	19 13 30 06

5.2.1.4 DES kod çözme rutini

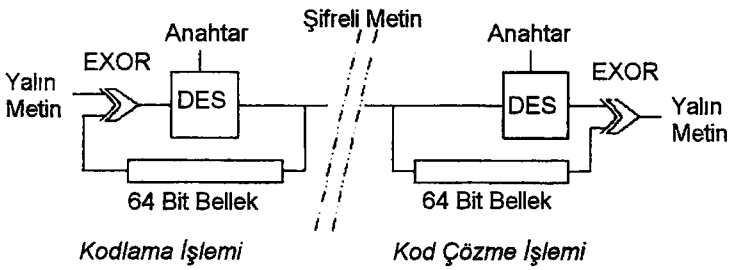
Burada, kod çözmek için de ayrı bir algoritma kullanılmaktadır. Fakat, anahtar uygulama sırası tersine çevrilmiştir. Onaltıncı anahtar olan K_{16} ilk bölgede kullanılmakta, ilk anahtar olan K_1 ise son bölgede kullanılmaktadır. Diğer anahtarların mevcut olması için gerekli olan birkaç anahtar vardır. Bu anahtarlar, anahtar üretme rutininin ilk adımından sonra bütün sıfırları veya birleri veya değişimli olarak sıfır ve bir üretmektedir [1].

Diğer DES algoritma modları, Şifreli Blok Zincirleme (CBC: Cipher Block Chaining), Şifreli Geribesleme (CFB: Cipher Feedback) ve Çıkış Geribeslemesi (OFB: Output Feedback)'dir. Bu modlar, temel Electronic Code Book modundan daha güvenlidir [1].

Bu modlar daha güvenli olmasına rağmen karıştırıcı sistemlerde çok fazla kullanılmamaktadır. Bunun başlıca nedeni, DES uygulamalarının büyük bir kısmının yazılım bazlı olması ve bu modların mikrokontrolörlerin aşırı yüklenmesine yol açmasıdır. Diğer bir sebep ise, Electronic Code Book modunun iletim bakımından daha sağlam olmasıdır. Bir sistemde anahtar değişimleri arasındaki sürenin uzunluğu, bu sistemin tehlikelere karşı daha sağlam olduğunu gösterir.

5.2.2 Şifreli blok zincirleme modu

Şifreli Blok Zincirleme modunun prensibi (Şekil 5.4) basittir. Herbir 64 bit yalın metin giriş bloğu, önceki 64 bit şifreli metin bloğu ile EXOR'lanmaktadır. Yüzeysel olarak bakıldığında bu çok mükemmel gibi görünmektedir. Fakat problemler, başlangıç bloğunda bulunmaktadır ve gerçekte herbir çıkış bloğu önceki blokların tamamının bir fonksiyonudur. İlk bloktan önce gelen şifreli blok olmadığı için bir başlatma değişkeninin veya bloğunun kullanılması gerekmektedir.



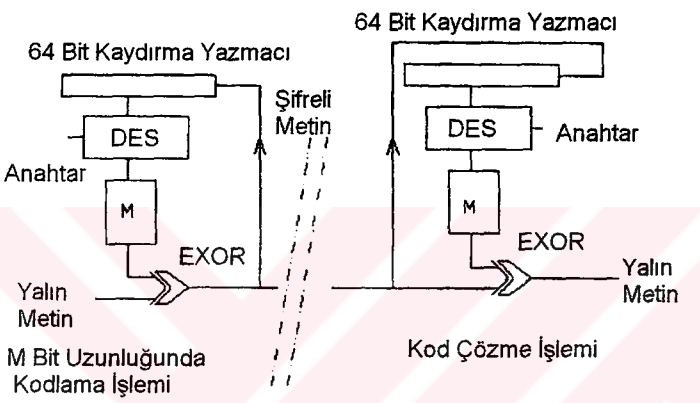
Şekil 5.4 Şifreli blok zincirleme modu [1]

Sonraki blokların tamamı önceki blokların fonksiyonları olduğu için bir bloktaki bir hata sonraki blokların tamamında hatalara yol açmaktadır. Buna hata genişlemesi adı

verilmektedir. Kodlanmış seste bu hata hışırtı sesi olarak ortaya çıkar. Kodlanmış veride ise, verinin tamamının yeniden iletilmesini gerektirir. Hata kontrolü, yalın metinden ziyade şifreli metinde gerçekleştirilmektedir.

5.2.3 Şifreli geribesleme modu

Şifreli Geribesleme modu (Şekil 5.5), kullanılmış olan yalın metnin sürekli olarak 64 bit bir tam bloktan daha az olması durumunda kullanılmaktadır. Tam bir bloğa ulaşmak için yalın metnin, rasgele veri ile dolmuş olması gerekmektedir. Kullanılmış olan bit sayısı 64'ten az olduğu için bu tekniğe M bit Şifreli Geribesleme adı verilmiştir. M, 1 ile 64 arasındaki herhangi bir sayıdır.



Şekil 5.5 Şifreli geribesleme modu [1]

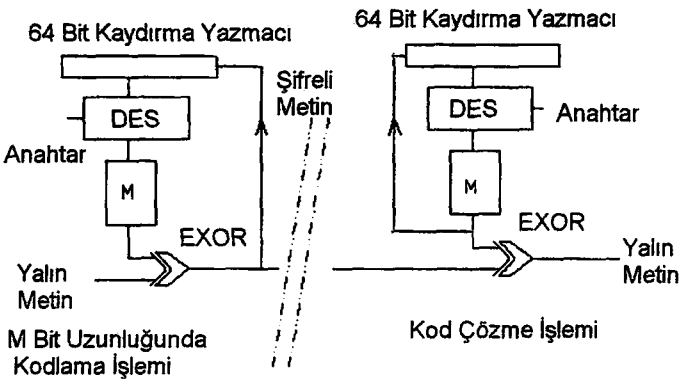
Bu modda, DES algoritmasının girişi şifreli metnin önceki 64 bitidir. Bu DES algoritmasının girişi, iletimin başlangıcında bir ilk değere sahip olan bir kaydırma yazmacında (shift register) tutulmaktadır. M bit yalın metin, DES algoritmasının çıkışının en soldaki bitleriyle EXOR'lanmaktadır. Daha sonra ortaya çıkan bu şifreli metin, kaydırma yazmacını geri beslemektedir.

5.2.4 Çıkış geribeslemesi modu

Çıkış Geribeslemesi modu (Şekil 5.6), DES algoritmasının çıkışını DES giriş kaydırma yazmacına geribesleme olarak kullanmaktadır. Buna M Bit Çıkış Geribeslemesi adı verilmektedir. M, 1 ile 64 arasındaki herhangi bir sayıdır.

Bu modda, DES algoritmasının çıkışı ile M bit yalın metin EXOR'lanmaktadır. Eğer televizyon alıcısı ve vericisi arasındaki senkronizasyon kaybolursa, kaydırma yazmacına yeni bir başlangıç değerinin girilmesi gerekir. Fakat bu başlangıç değerlerinin kodlaması gerekli

değildir [1].



Şekil 5.6 Çıkış geribeslemesi modu [1]

5.3 RSA Algoritması

RSA algoritması, büyük sayıları çarpanlarına ayırmanın zor olmasına güvenmektedir. Matematiksel olarak bu, en basit algoritmalardan biridir. Hesaplama bakımından ise, bir kaç probleme yol açabilmektedir. Bu problemlerin üstesinden gelinebilir. Fakat bu algoritma, DES algoritmasına kıyasla daha yavaştır.

RSA kripto sistemi, bir genel anahtar sistemidir. Bu, bir anahtarın veriyi kodlamak için ve diğer bir anahtarın da verinin kodunu çözmek için kullanıldığı anlamına gelir. Kodlama anahtarı, bir tamsayı çiftidir (N, P). Kod çözme anantarı da bir tamsayı çiftidir (N, S). S tamsayısı gizli tutulmaktadır. N ve P tamsayıları gizli değildir. Bu, matematiksel tanımıdır. Bu kısımda S tamsayısına gizli anahtar, P tamsayısına genel anahtar ve N tamsayısına da adres adı verilmiştir.

Bu algoritmada modülo aritmetik kullanılmaktadır. Aşağıda verilmiş olan örnekte, modülo aritmetiğin nasıl yapıldığı gösterilmiştir. Bu örnekte modüller, N'in en yakın tamsayı katının bölünmesinden arta kalan miktardır.

N=5 değeri verilmiş olsun.

17 Mod 5 = ?

5 . 3 = 15

17 - 15 = 2

17 Mod 5 = 2

Bu sistemde dört temel eleman vardır. İlk iki eleman asal sayılardır. Asal sayılar, sadece bire ve kendisine bölünebilen sayılardır. Aşağıdaki örnekte bu asal sayılar X ve Y olarak adlandırılmıştır.

Bu sistemin üçüncü ve dördüncü elemanları gizli ve genel anahtarlardır. Bu gizli anahtar, bir asal sayıdır. Genel anahtar ise (5.2) eşitliği kullanılarak seçilmektedir. Aşağıdaki örnekte, gizli anahtar S olarak, genel anahtar ise P olarak adlandırılmıştır.

Ayrıca, X ve Y asal sayılarının sonucu da gizli değildir. Bu, bir abonenin telefon numarası gibidir. Bu örnekte, bu sonuç N olarak adlandırılmıştır [1].

X = Asal Sayı 1 S = Gizli Anahtar = Asal Sayı

Y = Asal Sayı 2 P = Genel Anahtar

N = X . Y P seçildiği için;

P . S Mod ((X - 1) . (Y - 1)) = 1

$$P = (((X - 1) . (Y - 1)) + 1) / S \quad (5.2)$$

Kodlarken:

$$\text{Şifreli Metin} = (\text{Yalın Metin})^{P} \text{ Mod } N \quad (5.3)$$

Kod çözerken:

$$\text{Yalın Metin} = (\text{Şifreli Metin})^{S} \text{ Mod } N \quad (5.4)$$

Yukarıda görüldüğü gibi bu basit bir teoridir [1]. Yalın metinden şifreli metini elde etmek (5.3) için yalın metnin P'inci kuvvetinin modülo N'ini almak gereklidir. Şifreli metinden yalın metni yeniden elde etmek (5.4) için şifreli metnin S'inci kuvvetinin modülo N'ini almak gereklidir.

5.3.1 RSA algoritmasına basit bir örnek

X = 47 (Asal Sayı 1) S = 97 (Gizli Anahtar, Asal Sayı)

Y = 79 (Asal Sayı 2) P = ((47 - 1) x (79 - 1))/97 = 37

N = 47 x 79 = 3713

Yalın Metin = AT

Bunu basit bir sayısal koda dönüştürmek için alfabedeki herbir harf, 1'den 26'ya kadar bir sayıya atanmaktadır. Bundan dolayı AT, 120'ye karşılık gelmektedir.

Kodlarken (5.3), 120'nin 37'inci kuvvetinin modülo 3713'ünü üretmek gerekir.

Şifreli Metin = 120^{37} Mod 3713

Şifreli Metin = 1404

Yalın metin olan 120'nin 37'inci kuvvetinin modülo 3713'ünü üretmek için kullanılmış olan bu metot tekrarlanan kare alma ve çarpım ile üst alma (Exponentiation By Repeated Squaring And Multiplication) olarak bilinmektedir. Bu, çok güzel matematiksel bir kısa yoludur. Fakat bu, bu uygulamada kullanılabilecek olan tek algoritma değildir.

RSA'yı mikrokontrolör yazılımında gerçekleştirmek için kullanılabilecek olan birkaç güzel algoritma vardır. Bu örnekte tekrarlanan kare alma ve çarpım ile üst almanın kullanılmış olmasının sebebi, bunun kolayca anlaşılabilir olması ve yüksek düzeyli programlama dillerinde büyük zorluklarla karşılaşılmadan uygulanabilir olmasıdır. Tekrarlanan kare alma ve çarpım ile üst alma algoritması aşağıda gösterilmiştir.

M^H Mod N 'i elde etmek için;

Adım 1: H'ı binary formatında göster (H_n-H_0)

Adım 2: C = 1 yapın

$C = C^2 = 1C$ Mod N

$C = C^2 = MC$ Mod N

H_n daima 1 olmaktadır.

Adım 3: i = n yap (n, binary H'taki basamakların sayısıdır)

Adım 4: C^2, N ile bölündüğü zaman kalanı C'ye ata

Adım 5: Eğer $H_i = 1$ ise o zaman CM, N ile bölündükten sonra kalanı C'ye ata

Adım 6: i'yi 1 azalt (i-1)

Adım 7: Eğer i = 1 ise dur, eğer değilse Adım 4'e git

Bunu örnekteki sayılara uygularsak;

M = 120, H = 37 ve N = 3713, Binary H = 100101

Adım 1: C = 1

C = 120C Mod 3713 = 120 Mod 3713 => 1

i = 6

$C = 120^2$ Mod 3713 = 3261 Mod 3713 => 0

i = 5

$C = 3261^2$ Mod 3713 = 89 Mod 3713 => 0

i = 4

$C = 89^2$ Mod 3713 = 495 Mod 3713

(495 . 120) Mod 3713 = 3705 Mod 3713 => 1

i = 3

$C = 3705^2$ Mod 3713 = 64 Mod 3713 => 0

i = 2

$C = 64^2$ Mod 3713 = 383 Mod 3713

(383 . 120) Mod 3713 = 1404 => 1

i = 1

Bu yüzden 120^{37} Mod 3713 = 1404 olur.

Şifreli metnin kodunu çözerken (5.4) 1404'ün 97'inci kuvvetinin modülo 3713'ünü alırız.

Yalın Metin = 1404^{97} Mod 3713

Bu durumda M = 1404, H = 97 ve N = 3713, Binary H = 1100001

1404C Mod 3713 = 1404 Mod 3713 => 1

$C = 1404^2$ Mod 3713 = 3326 Mod 3713

(3326 x 1404) Mod 3713 = 2463 Mod 3713 => 1

$C = 2463^2 \text{ Mod } 3713 = 3040 \text{ Mod } 3713 \quad \Rightarrow 0$

$C = 3040^2 \text{ Mod } 3713 = 3656 \text{ Mod } 3713 \quad \Rightarrow 0$

$C = 3656^2 \text{ Mod } 3713 = 3249 \text{ Mod } 3713 \quad \Rightarrow 0$

$C = 3249^2 \text{ Mod } 3713 = 3655 \text{ Mod } 3713 \quad \Rightarrow 0$

$C = 3655^2 \text{ Mod } 3713 = 3364 \text{ Mod } 3713$

$(3354 \,.\, 1404) \text{ Mod } 3713 = 120 \quad \Rightarrow 1$

Bu yüzden Yalın Metin = 120 olur.

Tekrarlanan kare alma ve çarpım ile üst alma algoritmasının kullanımı, RSA algoritmasını uygulama işlemlerinin tamamının kolayca bilgisayara yüklenmesine olanak tanır. Bu uygulama için çok basit bir BASIC programı yazılabilir.

RSA algoritmasının güvenliğindeki temel unsur, kullanılmış olan asal sayıların boyutudur. Genellikle bu sayılar, yüz basamaktan daha uzundur. Bu bölümde verilmiş olan örnekte, sonucu görebilmek için küçük asal sayılar kullanılmıştır. Bir bilgisayar programının N adresini çarpanlarına ayırması bir saniyeden daha kısa zaman almaktadır. X ve Y asal sayıları bilindiği zaman S gizli anahtarının değeri, P genel anahtarını elde etmek için kullanılan formül yeniden düzenlenerek hesaplanabilmektedir. Bu durumda, S ile bölünmek yerine P ile bölünür.

5.4 Doğruluğu Kanıtlama ve Gerçekleme

Kripto sistemlerde doğruluğu kanıtlama (authentication) önemlidir. Kod çözücü veya akıllı kartın, aldığı veri paketinin gerçekten headend tarafından gönderildiğinin, araya girmeye çalışan bir bilgisayar korsanı tarafından gönderilmediğinin doğruluğunu kanıtlama yeteneğine sahip olması gereklidir. Kod çözücüdeki bu doğruluğunu kanıtlama prosedürüne uğramadan geçmenin (bypass) mümkün olmaması gereklidir [1].

Doğruluğunu kanıtlamanın önemi, olmaması durumunda başa gelen durumlar görüldükten sonra anlaşılmıştır ve son birkaç yıldır üzerinde durulan bir konu haline gelmiştir. Bunun en iyi örneği, VideoCrypt sistemindeki akıllı kartın bütün kanallar için aktif duruma gelmesini sağlayan Phoenix isimli hack işlemi olmuştur. Bu hack işleminin meydana gelmesinin sebebi, gereği gibi doğruluğu kanıtlanmış mesajın akıllı karta gönderilmesi ve akıllı kartın bu mesajı gerçek olarak kabul ederek normalde olması gerektiği gibi davranmasının mümkün olmasıydı.

Eğer bilgisayar korsanı, doğruluğunu kanıtlama prosedürüne uğramadan geçebiliyorsa güvenlik bakımından bu bir felaket anlamına gelir. Çünkü bunun anlamı, bilgisayar korsanının kod çözücüye giden her şey üzerinde kontrole sahip olduğudur. Bunun en iyi örneği VideoCipher-II sisteminde görülmektedir. VideoCipher-II sistemi, hiyerarşik bir anahtar kümesini baz almaktaydı. Aylık bir anahtar, oturum anahtarının kodunu çözmekteydi. Bu aylık anahtar her bir yetki verilmiş kod çözücüye, bu kod çözücünün kendine ait anahtarı kodlama anahtarı olarak kullanarak kodlanmış bir formda iletilmektedir. Geçerli bir anahtarla bu aylık anahtarın kodu çözülebilmektedir. Bir düzelticide kullanılmış olan anahtarın gerçek düzelticinin anahtarı olmaması önemli değildir. Sadece başka bir düzelticiden elde edilmiş olması yeterlidir. Bu durum, VideoCipher-II sistemi için tam bir felaket olmuştur ve bundan sonra sistem bir daha tamamen geri kazanılamamıştır [1].

5.4.1 Kontrol işlemleri

Bir kontrol işlemi, bir veri paketinin doğruluğunu kanıtlamanın ilk düzeyidir. Bu esasen, veri paketinin bozulmamış (tam) olmasını garantiye almaktadır [1]. Bununla birlikte bu kontrol işlemi, veri paketinin karıştırılmamış olduğunu doğrulamamaktadır

Bir kontrol işlemi, veri paketindeki diğer baytların bazı basit matematiksel işlemlere tabi tutuldukları zaman elde edilen bir değerdir. Akıllı kart veya kod çözücünün, aynı matematiksel işlemi gerçekleştirmesi ve bu kontrol işlemi ile aynı sonuca ulaşması gerekir.

Kontrol işlemlerinin en sık raslanan formu Modülo Aritmetik kontrol işlemi ve Periyodik Fazlalık Kontrolü (CRC)'dür [1]. Bu formlardan Modülo Aritmetik kontrol işlemi daha hızlı gerçekleştirilmektedir. Bu formların en basiti olan Modülo Aritmetik kontrol işlemi, sadece paketteki baytların toplamını N'in bir katına getirmesi gereken bir değerdir. Mod N işleminin sonucunun geçerli bir paket için sıfır olması gereklidir. Fakat böyle basit bir test, bir paketin geçerli olduğunu saptayamamaktadır. Buna rağmen, paketteki baytların sırası değişmişse olumlu bir sonuç vermektedir. Bu kontrol işlemi tipi VideoCrypt sisteminde kullanılmış olan 74h paketinde doğruluğunu kanıtlamanın ilk düzeyi olarak kullanılmıştır [1].

Periyodik Fazlalık Kontrolü diğerinden daha karmaşıktır. Veri, bir polinom olarak gösterilmektedir. Daha sonra bu polinom, küçük bir sabit polinom ile bölünmektedir. Bu bölme işleminin sonucu, Periyodik Fazlalık Kontrolü'dür. Daha sonra bu Periyodik Fazlalık Kontrolü verisi, veri paketine ilave edilmektedir.

Alıcı uçtaki kod çözücü, bu paketin tümünü bu küçük sabit polinom ile bölmektedir. Eğer bu

paket geçerliyse, bu bölme işleminin sonucun sıfır olması gerekir. Fakat burada bazı zayıf noktalar mevcuttur. Eğer bu küçük sabit polinom bir bilgisayar korsanı tarafından saptanabilirse, uygun bir biçimde kontrol işleminden geçirilmiş paketlerin yaratılması mümkündür.

5.4.2 Kripto imzalar

Önceki metodlar, doğruluğunu ispatlama işleminin ilk düzeyini oluşturmak için yeterince iyi olsa da sonuçta bunlar yeterince güvenli değildir. Bunları hack etmek, uygun bir şekilde inşa edilmiş bir kripto imzayı hack etmekten daha kolaydır. Teorik olarak, bir imza sisteminin hack edilmesi daha zordur ve kod çözücüyü yetki verilmemiş bir veri paketi ile kandıran bilgisayar korsanlarına karşı savunmanın son hattını oluşturmaktadır.

Karıştırıcı sistemlerdeki en yaygın tercih, imzanın üretilmesi için algoritma olarak asıl temel algoritmayı kullanmaktır. Çoğunlukla bu imza Karma İmza (Hash Signature) veya Karma Kontrol İşlemi (Hash Checksum) olarak adlandırılmaktadır. Bu algoritmanın bu biçimde kullanılması daha ekonomiktir.

Karıştırıcı sistemlerde imzaların kullanılmasının iki yöntemi mevcuttur. Bunlardan birincisi ve en açığı, pakete eklenmiş olan farklı bir imzaya sahip olmaktır. İkincisi ise, çekirdeği üretmek için kullanılmış olan mesajın bir parçası olan bir imzaya sahip olmaktır.

EuroCrypt-M sisteminde, anahtar üretme paketine 8 baytlık bir kontrol işlemi eklenmiştir. Bu kontrol işlemi, DES'in modifiye edilmiş bir versiyonunun üzerinden dört defa işleme sokulmaktadır. 07 ve 09 serisi VideoCrypt sisteminde bu imza, çekirdek üretme verisinin bir parçasını oluşturmaktadır. Paketin ilk 27 baytı, karma fonksiyon üzerinden işleme sokulmaktadır. Daha sonra, bu karma imzanın 4 baytı karma fonksiyon üzerinden iki kere işleme sokulmaktadır. Herbir turun (cycle) sonucunun, imza baytına eşit olması gereklidir.

5.4.2.1 RSA kripto imzası

RSA'daki imza işlemi oldukça basittir. Verici, bir mesajı alır ve bu mesajın gizli anahtarı (S) kuvvetininin modülo N'ini oluşturur [1].

Daha sonra alıcı, vericinin genel anahtarını (P) şifreli metnin P'inci kuvvetinin modülo N'ini oluşturmak için kullanır. Bunun sonucu, yalın metin mesajıdır. Bu mesaj, bilginin rasgele bir parçası veya tarih veya kanal numarası gibi bir bölümü de olabilmektedir. Bu sırada verici ve alıcı arasında gerçek bir bilgi transferi olmayacaktır.

Verici: yayımlanmış olan veri = N, P

Mesaj = Yalın Metin

Kodlarken;

Şifreli Metin = $(\text{Yalın Metin})^P$ Mod N

Kod çözerken;

Alıcı: Mesajı başlangıçtaki değerine getirmek için vericinin N ve P değerlerini kullanır.

Yalın Metin = $(\text{Şifreli Metin})^P$ Mod N

Bundan başka veri imza metodları da mevcuttur. Bu RSA imza metodu, çok fazla hesap yapma gücü olmayan uygulamalar için kullanışlıdır. Bununla birlikte, 8 bit işlemci yönetimine sahip olan akıllı kart uygulamaları için, daha az çevrim harcayan diğer algoritmaların kullanılması gereklidir.

5.5 Fiat-Shamir Zero Knowledge Test

VideoCrypt dökümanlarına göre Fiat-Shamir Zero Knowledge Test (Sıfır Bilgi Testi), VideoCrypt erişim kontrol sistemindeki bilgi paketlerinin geçerli olduğunun ve bu paketlere müdahale edilmemiş olduğunun doğruluğunu kanıtlamak için kullanılmıştır [1].

VideoCrypt sistemini kullanımında, kod çözücünün akıllı kart arabirimi mikrokontrolöründe Sıfır Bilgi Testi'nin gerçekleştirilmesinde bir kusur vardı. Bu kusurdan dolayı kod çözücü, korsan bir akıllı kartı reddetmemekteydi. Bu kusur giderildikten sonra korsan 07 Ho Lee Fook kartı çalışmadı.

Fiat-Shamir algoritması, modülo kare köklerinin elde edilmesinin ve çarpanlarına ayrılmasının zorluğuna güvenmektedir. Esas itibarıyla R aramalı (taramalı) tablosu, akıllı kartın dışına hiçbir zaman gönderilmemekteydi. Teorik olarak, kart seri numarasının kartın dışına gönderildiği düşünülmektedir.

D2-MAC uygulamasında, N modülleri 64 baytlık bir sayıdır. Bu, modüller için kullanılabilecek olan 2^513-1 sayısını vermektedir. Bu modül, R aramalı tablosunun boyutunu sınırlayan bir faktördür. Eğer bu modül R aramalı tablosundan büyükse, o zaman R Mod N işleminin sonucu sıfır olur. Aramalı tablo R'nin bir katı olduğu zaman R Mod N işleminin sonucunun sıfır olduğu gerçeği, bir hack etme saldırısı için bu meselenin ana

noktası olduğu düşünülmektedir.

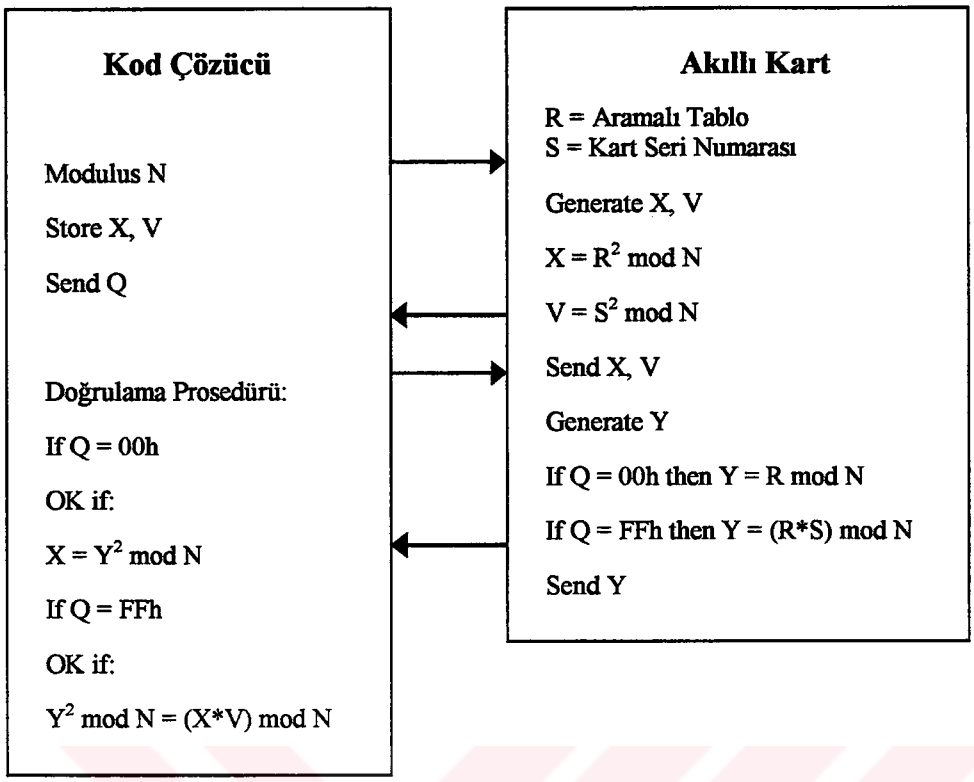
Fiat Shamir Sıfır Bilgi Testi'nin lehine olan nokta, içerdiği sayıların çok büyük olmasıdır. Çarpanlara ayırma algoritması yavaş olduğu için R aramalı tablosunun ortaya çıkarılma şansı iyi değildi. Aramalı tablonun ve modüllerin boyutlarının azaltılması, potansiyel bir zayıflıktır. Paralel çalışan bir kaç bilgisayarın bu aramalı tabloyu Brute Force Attack'da elde edildiği şekilde üretme şansı vardır [1].

Sıfır Bilgi Testi sadece, daha önce bahsettiğimiz doğruluğu kanıtlama rutinlerinden biridir. Bu uygulamada, akıllı kart kanalın kodunu çözme işlemini gerçekleştirmeden önce akıllı kartın doğruluğunu kanıtlamak için kullanılmıştır. D2-MAC sistemi, farklı bir güvenlik yaklaşımına yönelmişti. Halbuki VideoCrypt sistemindeki en değerli yaklaşım bu algoritmadır. D2-MAC sisteminde ise en değerli yaklaşım anahtar tablolarıdır.

Fiat Shamir Sıfır Bilgi Testi algoritmasındaki problem, karıştırıcı bir sistemde kullanıldığı zaman kartın güvenliği kadar kod çözücünün güvenliğine de bağlı olmasıdır. Bu bakımdan bu algoritma zayıftır. Kod çözücü Sıfır Bilgi Testi'ni kartın bir geçerli kart olup olmadığını kontrol etmek için kullanmaktadır. Bunun için ilk baypas, korsan kart yazılımı sıfırlardan oluşan bir cevap vermesi için ayarlamaktır.

Genellikle kart arabirimi mikrokontrolörü, kartın Sıfır Bilgi Testi yanıtını kontrol etmesi gereken elemandır. Ayrıca bu, akıllı kart - kod çözücü trafiğini de kontrol etmektedir (Şekil 5.7). Bu yüzden, eğer bu mikrokontrolördeki program yeniden yazılabilirse, Sıfır Bilgi Testi paketinin tamamını reddedecek ve bu Sıfır Bilgi Testi karta bir daha asla ulaşamayacaktır. Bunun sonucunda, kart kendisini kod çözücüye ispatlamak zorunda olmayacaktır [1].

Fakat sistem tasarımcıları, Sıfır Bilgi Testi algoritmasını çekirdek üretim verisinin içinde oluşturarak bu hack işlemine karşı tedbir alabilmektedir. Bu şekilde Sıfır Bilgi Testi verisi ikinci bir fonksiyona sahip olacaktı. Ayrıca, Sıfır Bilgi Testi'ni içeren paket kart için gerekli olacaktı. Aksi taktirde bu kart, çekirdeği üretecek bir veriye sahip olamayacaktı.



Şekil 5.7 Fiat Shamir Zero Knowledge Test'inde akıllı kart-kod çözücü trafiği [1]

5.5.1 Karma fonksiyonlar ve mesaj özetleri

Bir karma (hash) fonksiyon, bir veri bloğundan sabit uzunlukta bir çıkış üretmektedir. Girişin uzunluğu sabit veya değişken olabilmektedir. Genellikle bu karma çıkışa, karma değer adı verilmektedir. Aslında bu karma fonksiyon, bir veri bloğunun parmak izi olarak adlandırılabilen değeri üretmektedir. Bu fonksiyonun tersine çevrilmesi zor olduğu zaman bu mesaj özeti (digest) olarak adlandırılabilir.

Karma fonksiyonun tersine çevrilmesinin (reverse) oldukça zor olması gerekir. Yani çıkış verisinden giriş verisinin yeniden inşa edilmesinin mümkün olmaması gereklidir. Diğer bir faktör ise, akıllı kart kullanımı gibi bir uygulamada karma fonksiyon için kullanılmış olan gerçek algoritmanın bilinmemesinin gerekli olduğudur. Çünkü, eğer tek bir algoritma kullanılmışsa bu algoritma keşfedildiğinde sistemin güvenliği tehlikeye düşebilir. Genellikle bu karma fonksiyon, adresleme verisinin ve abone verisinin geçerli olduğunu ve değiştirilmediğini ispatlamak için kullanılmaktadır.

5.6 Tekyönlü Fonksiyonlar

Teknik olarak bir tekyönlü fonksiyon, tersine çevrilmesi eğer mümkün değilse aşırı derecede zor bir fonksiyondur. Bu prosedür, isminden de anlaşıldığı gibi sadece tek yönde işlemektedir. Tekyönlü fonksiyondaki problem, bu kavramın temel ilkelerinin kusurlu olmasıdır [1].

Tekyönlü fonksiyonlar, tersine çevrilmesi mümkün değilse çok zordur. Bu karmaşık düzeyi gerçekleştirmek için kullanılabilecek birkaç metot mevcuttur. Birinci metot, çok karmaşık bir algoritma veya denklem tasarlanmasıdır. Eğer elektronik olarak çok fazla işlem gücü mevcutsa, bu metot çok iyidir. Bu metot, kişisel bilgisayarlar veya buna benzer uygulamalar için çok uygundur [1].

İkinci metot, basit bir rutini birkaç kez kullanmaktır. Bu rutin oldukça kısa olabilir. Fakat çok fazla tekrar ettiği için tersine çevrilmesi aşırı derecede zordur. Bu, bir akıllı kartta çok kolay gerçekleştirilebilir. Bu, sadece bir döngü hazırlamadan ibarettir. Bu metodun basitliği ve mükemmelliği, bunu bir akıllı kart uygulaması için ideal yapmaktadır. Akıllı kartların büyük bir kısmı 8 bit işlemci kullanmaktadır. Ayrıca, bu işlemciler oldukça yavaş clock hızlarında çalışmaktadır.

Tekyönlü fonksiyonun çekirdeğindeki (belleğindeki) rutin en zayıf noktadır. Eğer bu rutin doğru bir şekilde tasarlanmamışsa, bu rutinin bir kaç kez kullanılması hiç bir önem taşımaz. Çünkü karşılaştırma yaparak bunu hack etmenin bir yolu bulunabilir [1].

Teorik olarak, tekyönlü fonksiyonun çıkışındaki bitlerin birbirleriyle görünür bir ilişkiye sahip olmaması gereklidir. Fakat uygulamalarda, bilgisayar korsanları için birkaç açık nokta verilebilmektedir. Bu açıklardan biri işlemci sözcük uzunluğudur.

8 bit işlemciler ile 16 bit genişlikli yazmaçlara (registers) sahip olmak mümkündür. Bu şekilde bu rutinin çıkışı 16 bit genişlikte olabilmektedir. Akıllı kart üzerinde çok sınırlı bir RAM bulunduğu için bellek kullanımı bakımından bu uygulama oldukça kötüdür. Her seferinde bir 8 bit çıkış kullanılması, güzel olmaktan ve uygulama kolaylığından çok uzaktır.

İkinci metotta bu rutin birkaç kez uygulanmaktadır. Tipik bir prosedür, akıllı kart modelinde tek bir bayt olması gereken çıkış bloğunun içeriğinin rutin çıkışı ile EXOR'lanmasıdır. Çıkış bloğu, rutinin önceki çıkışlarının hepsinin toplanmasıdır. Çıkış bloğunun başlangıç durumu sıfırdır. Matematiksel tabirle çıkış bloğu, rutin çıkışlarının tamamının modülo 2 toplamıdır. Fakat, bu model oldukça basittir ve de zayıftır. Çünkü tekrarlama sırasında aynı anahtarlar kullanılmaktadır. Bu durum, bütün zinciri oldukça lineer yapmaktadır [1].

K_0 ve K_n arasındaki anahtarlar, tekrarlanan bir bazda seçilmiştir. Bu yüzden, bunun bir örneğinin geliştirilebilme riski vardır. Anahtarlar, sabitler haline gelmektedir. Bir potansiyel kriptanalistin büyük miktarda şifreli metne ve bunlara karşılık gelen yalın metne sahip olacağı unutulmamalıdır. Bu nedenle, olabildiğince çok lineer olmamayı sağlayacak elemanın bu modele dahil edilmesi çok iyi olacaktır. İlk adım olarak, anahtarların seçimini non-lineer yapılması gerekir.

Uygulama, akıllı kart bazlı olduğu için anahtar tabloları için mevcut bellek çok sınırlıdır. Anahtarları seçmek için bir aramalı tablo rutini kullanılarak, orijinalinin bir kaç katı büyüklüğünde sanal bir anahtar tablosu yaratılabilmektedir. Bu aramalı tablo rutini, bunu hack etme işlemini daha zor hale getirecektir.

Bu tip bir görüş için verilebilecek en iyi örnek, DES algoritmasındaki anahtar üretme rutinidir [1]. DES algoritması, tek bir 56 bit anahtardan on altı adet 48 bit anahtar üretmektedir. Bu, DES algoritmasındaki her bir döngünün, bu döngünün kendi anahtarı ile gerçekleşmesini sağlamaktadır.

Bu model terfi edildiğinde bile bu işlem oldukça lineer kalmaktadır. Çıkışın her bir bloğu için bu zincir tekrarlanır. f fonksiyonu, anahtar tablosundan ve bilinen bir değişken olan giriş verisinden gelen girişleri kullanmaktadır. Giriş verisi bilinen bir faktör olduğu için, bir kriptanalist tarafından bir saldırı yolu olarak kullanılabilir.

Bilgisayar programlaması bakımından bu çok karmaşık bir modeldir. Zincir, her çıkış bloğu için tekrarlanmaktadır. Birçok çıkış bloğu gerektiren bir durumda (örneğin bir 8 bayt genişlik) her bir çıkış bloğu için bir zincir (chain) kullanmak işlemci zamanını gereksiz yere harcamaktadır. Ayrıca bu durum, her bir çıkış bloğunu kendisine özel yapmaktadır. Böylece bir kriptanalist için mevcut olan bilgi miktarını 8 ile çarpmaktadır. Eğer çıkış bloğu sayısının tamamı tek bir çıkış oluşturuyorsa, o zaman her şey biraz daha fazla karışık hale gelecektir.

DES algoritması, bu tahminler için kullanılabilir. Kodlama ve kod çözme döngülerinde, önceki döngünün çıkışının bir kısmı sonraki döngünün girişi olarak kullanılır. Bu prosedürü kullanan bir şifreye "Fiestel Şifresi" adı verilmektedir [1]. Bu, algoritmanın kırılmasının karmaşıklığını arttırdığı için mükemmel bir metottur. Her bir döngünün çıkışı önceki bütün döngülerin çıkışlarının bir ürünüdür.

Sonraki çıkış bloğunu üretmek için f fonksiyonundaki her bir çıkış bloğunu beslemek bu programı, basit bir EXOR denkleminden lineer olmayan bir şekle dönüştürür.

Tekyönlü fonsiyonlar hakkındaki bu düşüncelerin pek çoğu VideoCrypt 07 Ho Lee Fook algoritmasında görülebilmektedir.

5.7 Yalancı Rasgele Sayı Üreteçleri ve Yalancı Rasgele İkili Dizi Üreteçleri

Rasgele bir sayı, olası bir sayılar kümesinden rasgele seçilmiş olan bir sayıdır. Seçilecek olan bir sonraki sayının önceden tahmin edilmesi imkansızdır. Bu tür bir sayı, piyango biletleri ve buna benzer uygulamalar için çok kullanışlıdır. Sinyal güvenliği uygulamaları, senkronize çalışacak iki veya daha fazla rasgele sayı üretecini gerektirmektedir. Bu üreteçler bu şekilde rasgele sayılar üretemiyecekleri için bu durum imkansızdır. Bu yüzden Yalancı Rasgele Sayı Üreteçleri kullanılmaktadır [1].

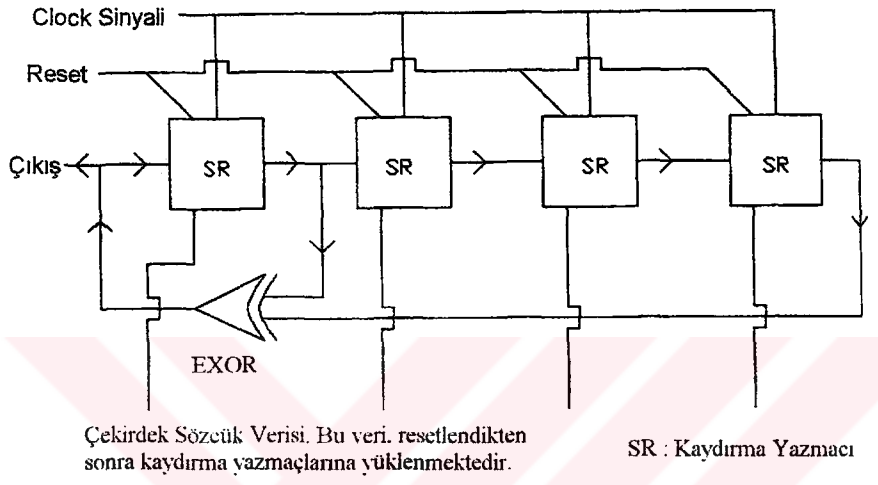
Bir Yalancı Rasgele Sayı Üreteci, rasgele seçilmiş olarak görünen bir dizi sayı üretir. Aslında bu üreteç, bu bir dizi sayıyı matematiksel bir denklem kullanarak üretmektedir. Bir Yalancı Rasgele Sayı Üreteci, bir sayı ile belirli bir maksimum basamak sayısı arasında ilişki kurar. Yani, Yalancı Rasgele Sayı Üretecinin çıkışı, paralel bazdaki bir veri ile EXOR'lanmıştır. Eğer Yalancı Rasgele Sayı Üreteçlerini üretmek mümkünse bir Yalancı Rasgele İkili Dizi Üretecini üretmek daha kolay olacaktır [1].

Güvenlik uygulamalarında, bir Yalancı Rasgele Sayı Üreteci yerine bir Yalancı Rasgele İkili Dizi Üreteci kullanılmaktadır. Bu Yalancı Rasgele İkili Dizi Üreteci, 1 bit gerişlikli bir çıkış üretir. Bu çıkış, veri akışı ile bit yönünde EXOR'lanabilir. Donanım bakımından bir Yalancı Rasgele İkili Dizi Üreteci, bir kaç kaydırma yazmacı ve bir EXOR kapısı kullanılarak kolayca gerçekleştirilebilmektedir. Başlangıçta bu kaydırma yazmaçları, bir anahtar veya çekirdek değeri ile doludur. Daha sonra sistem clock'u, bu yazmaçlar aracılığıyla bitleri kaydırır. EXOR kapısına girişlere geribesleme noktası adı verilmektedir [1].

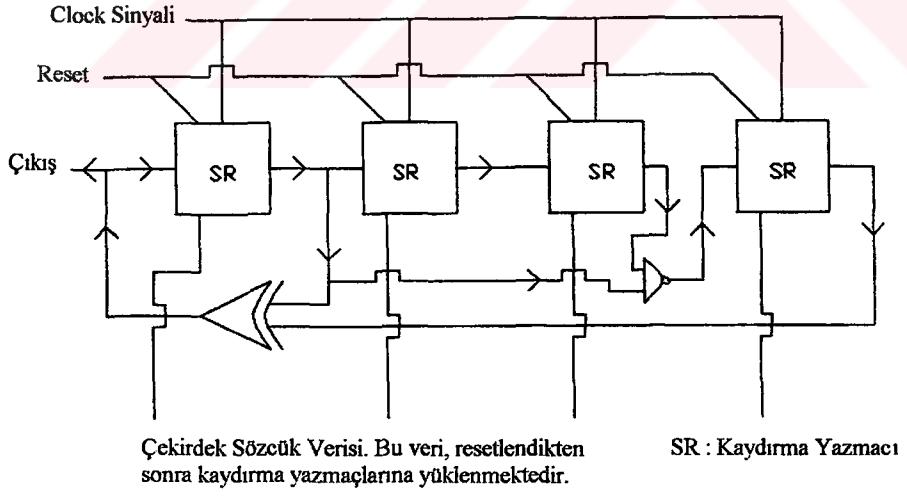
Yalancı Rasgele İkili Dizi Üretecinin çıkışının veri ile EXOR'lanması ile elde edilen veri akışının hack edilmesi daha zordur. Bit sadece 1 veya 0 ve yeni veri akışındaki her bir bit de sadece 1 veya 0 olabildiği için, bilgisayar korsanlarının pek çok şifreli metni ve yalın metni elde etmesi gerekecektir. Bir kaç karmaşık istatistiksel analiz ve matris cebri kullanılarak, Yalancı Rasgele İkili Dizi Üretecinin özellikleri çıkarılabilir. Bu özellikler, kaydırma yazmacının uzunluğu ve Yalancı Rasgele İkili Dizi Üretecinin geribesleme noktalarıdır. Fakat bilgisayar korsanlarının çekirdek sözcüğü de çıkartması gereklidir. Bu çekirdek sözcük (seed word), Yalancı Rasgele İkili Dizi Üreteci başlangıç durumuna getirildiği zaman kaydırma yazmaçlarına yüklenen veridir. Bunların hepsi geribesleme lojiğinin lineer olduğunu

varsaymaktadır. Eğer lineer değilse, o zaman bu iş aşırı derecede zor olacaktır.

Genellikle Yalancı Rasgele İkili Dizi Üreteçleri, dijital ses uygulamalarında sinyalin spektrumunu biçimlendirmek için kullanılmaktadır [1]. Yalancı Rasgele İkili Dizi Üretecinin kullanılması, veri akışının rasgele 1'ler ve 0'lar olarak görünmesini sağlar. Bunun dışındaki veri akışı gürültü olarak adlandırılır. Diziyi hack etmek zaman aldığı için video veya sesin bu işlem süresi için uygun miktarda geciktrilmesi gereklidir. Genellikle bu, ekonomik nedenlerden dolayı uygulanabilir bir hack işlemi değildir.



Şekil 5.8 Lineer geribeslemeli yalancı rasgele ikili dizi üreteci [1]



Şekil 5.9 Non-lineer geribeslemeli yalancı rasgele ikili dizi üreteci [1]

5.8 07 Ho Lee Fook Algoritması

VideoCrypt sisteminin 07 serisi akıllı kartını hack etmek için kullanılmış olan bu algoritma, yapı bakımından oldukça basittir. Sistemin merkezi, bir çekirdek fonksiyonudur. Bu algoritma, 32 baytlık mesaj bloğunu 8 baytlık bir kod çözme anahtarına dönüştürmektedir. Çekirdek fonksiyonunun basit olmasına rağmen bu fonksiyonun 99 defa tekrarlanmasından dolayı, 8 baytlık bir kod çözme anahtarının orijinal 32 baytlık mesaj paketine geri dönüştürülmesinin tasarım prosedürü aşırı derecede zordur.

Bu algoritma, bir mesaj özeti (digest) olmaktan daha çok gerçek bir kodlama sistemidir. Bu algoritma, 32 baytlık paketin bir özetini üretmektedir. Bu paket, kanal kimlik bilgisi, zaman işaretlemesi ve kontrol işlemlerini kapsamaktadır. Bazı bakımlardan bu algoritma, havadan adresleme problemine güzel bir çözümdür. Fakat diğer bakımlardan ise bu algoritma, sistemi tamamen savunmasız bırakmaktadır.

Doğruluk ispatlama, adresleme, kontrol işlemi yapma ve anahtar üretimi için tek bir paket kullanılması, sistemin doğruluk ispatlamanın sadece bir katına sahip olduğu anlamına gelmektedir. Bu yüzden sistem, hack edilmeye oldukça elverişlidir. Bunun sonucunda bir hack edilme olayı gerçekleştikten sonra sistemin geri kazanılması için mevcut seçenekler oldukça azdır. Fiat-Shamir Sıfır Bilgi Testi'nin 8052'de gerçekleştirilebilmesine rağmen burada bu algoritmayı kullanmak mümkün değildir. İlk üretim VideoCrypt düzelticilerinin büyük bir kısmında bir hata mevcuttu [1]. Bu hata, Fiat Shamir Sıfır Bilgi Testi'nin sonuçlarının düzeltici tarafından reddedidiği anlamına gelmektedir.

Kod çözme işlemi, ikinci bir doğruluk ispatlama katı olmaksızın gerçekleşebilmektedir. Bu, VideoCrypt sisteminin erişim kontrol tasarımındaki önemli bir kusura işaret etmektedir. News Datacom'um sistemi hakkında vermiş olduğu bilgilere göre bu sistemde bu tür bir hack işleminin mümkün olmaması gerekiyordu [1].

07 Ho Lee Fook algoritması, 32 baytlık bir m (0-31) mesaj paketini 8 baytlık bir r (0-8) kod çözme anahtarına dönüştürmektedir. Bu, bir mesaj özetidir. Çekirdek fonksiyonu olan f, lineer olmadığı için bu fonksiyonun tersine çevrilmesi çok zordur. Eğer lineer olsaydı, o zaman tersine çevrilmesi çok kolay olacaktı. Bu fonksiyonu tersine çevirmek için bir teşebbüs olduğunda, bunun sonucu belirli bir sonuç olmayacaktı. Bunun aksine birkaç sonuç mevcut olacaktı.

Sky Channel, 10 serisi akıllı kartlarını kullanmaya başladığı için artık bu algoritma artık Sky

kanallarında çalışmamaktaydı. Bununla birlikte, bu algoritma hala Avrupa'da kullanılmakta olan VideoCrypt-II varyantlarında kullanılmaktadır. Fakat bu sistemi kullanan kanallar, farklı anahtar tabloları kullanmaktadır.

07 Ho Lee Fook algoritması, dört aşamada incelenmektedir. Birinci aşama, anahtar seçimi ve PIC16C54 ve PIC16C84 gibi sınırlı belleğe sahip mikrokontrolörlerde kullanmak için anahtarların sıkıştırılması ile ilgilidir. İkinci aşama, çekirdek fonksiyonu incelemektedir. Bu, 07 Ho Lee Fook algoritmasının merkezindeki fonksiyondur. Aslında bu, algoritmadaki başlıca non-lineer fonksiyondur. Bu fonksiyonun tersine çevrilmesi denemeleri sonucunda, aynı sonucu verecek olan birkaç potansiyel giriş elde edilmektedir. Üçüncü aşama ise, kullanılan algoritmanın incelenmesidir. Bu fonksiyon, 99 defa kullanılmıştır. Bu yüzden, algoritmanın tersine çevrilme işlemi aşırı derecede zordur.

5.8.1 Anahtar tabloları ve anahtar yapıları

07 Ho Lee Fook algoritmasındaki anahtar tablosu 256 bayt uzunluğundadır. Bu anahtar tablosunun PIC'lerde kullanıldığı düşünülürse, 256 bayt oldukça büyük bir uzunluktur. Bu mikrokontrolörlerdeki bellek kapasitesi sınırlı olduğu için bu anahtar tablolarının sıkıştırılması gereklidir.

Aslında 256 bayt, çok uygun bir sayıdır. 16 x 16 = 256 olduğu için iki adet 16 bayt dizi ile gösterilebilmektedir. Bu nedenle, herbir diziden bir giriş ilave ederek 256 giriş dizisinin tamamını yeniden üretmek mümkündür. Bu durum için toplama kullanılmaktadır. Ayrıca çarpma, çıkarma veya diğer bir fonksiyonun da kullanılabilmesi mümkündür.

Ho Lee Fook algoritmasının PIC uygulamasında, anahtar tablosu sadece 56 bayt uzunluğundadır (Çizelge 5.7). Yani, bu 56 bayt blokta birden fazla 256 giriş anahtar tablosu depolanmaktadır.

Çizelge 5.7 Ho Lee Fook algoritmasının anahtar tablosu [1]

Ho Lee Fook Anahtar Tablosu (Onluk)	Ho Lee Fook Anahtar Tablosu (Onaltılık)
101 231 113 026 180 136 215 118	65 E7 71 1A B4 88 D7 76
040 208 076 110 134 140 200 067	28 D0 4C 6E 86 8C C8 43
169 236 096 066 005 242 061 028	A9 EC 60 42 05 F2 3D 1C
108 188 175 195 043 181 220 144	6C BC AF C3 2B B5 DC 90
249 005 234 081 070 157 226 096	F9 05 EA 51 46 9D E2 60
112 082 103 038 097 073 066 009	70 52 67 26 61 49 42 09
080 153 144 162 054 014 253 057	50 99 90 A2 36 0E FD 39

56 baytlık tablonun ilk 32 baytı kullanılarak aşağıda görülen anahtar değerlerinin üretilmesi mümkündür.

Onaaltılık (Hexadecimal) formatta:

Anahtar Sütunu = { 65, E7, 71, 1A, B4, 88, D7, 76, 28, D0, 4C, 6E, 86, 8C, C8, 43 }

Anahtar Satırı = { A9, EC, 60, 42, 05, F2, 3D, 1C, 6C, BC, AF, C3, 2B, B5, DC, 90 }

Anahtar Matrisi:

Satır x Sütun

```
0F 91 1B C3 5E 32 81 20 D1 7A F5 18 30 36 72 EC
52 D4 5E 07 A1 75 C4 63 15 BD 39 5B 73 79 B5 30
C5 48 D1 7A 15 E8 38 D6 88 31 AC CE E6 EC 29 A3
A7 2A B3 5C F6 CA 1A B8 6A 13 8E B0 C8 CE 0B 85
6A EC 76 1F B9 8D DC 7B 2D D5 51 73 8B 91 CD 48
58 DA 64 0D A7 7B CA 69 1B C3 3F 61 79 7F BB 36
A2 25 AE 57 F1 C5 15 B3 65 0E 89 AB C3 C9 06 80
81 04 8D 36 D0 A4 F3 92 44 EC 68 8A A2 A8 E4 5F
D1 54 DD 86 21 F4 44 E2 94 3D B8 DA F2 F8 35 AF
22 A4 2E D6 71 45 94 33 E4 8D 09 2B 43 49 85 FF
15 97 21 C9 64 38 87 26 D7 80 FB 1E 36 3C 78 F2
29 AB 35 DD 78 4C 9B 3A EB 94 10 32 4A 50 8C 07
90 13 9C 45 DF B3 03 A1 53 FB 77 99 B1 B7 F3 6E
1B 9D 27 CF 6A 3E 8D 2C DD 86 02 24 3C 42 7E F8
42 C4 4E F6 91 65 B4 53 05 AD 29 4B 63 69 A5 20
F5 78 02 AA 45 19 68 07 B8 61 DC FE 17 1D 59 D3
```

Bu 256 giriş anahtar tablosu, mikrokontrolör belleğinin problem yaratmadığı tek bir dizide saklanabilmektedir. 56 bayt bloğunda birkaç anahtar tablosu saklandığından dolayı herbir giriş için farklı bir 256 bayt anahtar tablosunun saklanması gerekmektedir. Bu basit bir kaydırıcı (offset) olduğu için iyi bir metot değildir. Bu kaydırıcının algoritmada kullanılması durumunda, yeni bir anahtar tablosu yaratacak ve çok fazla zorluk çıkaracaktır.

Bu matrisin adreslenmesi karışık değildir. Satır ve sütun değerleri iki adet 16 bayt dizinin değerleri olduğu için bunların herbiri bir nybble veya bir baytın yarısı olarak adlandırılabilmektedir.

Daha önceden de bahsedildiği gibi 56 bayt blok, bir kaç anahtar tablosu üretmek için kullanılabilmektedir. Bu blok, 07 serisi akıllı kartta üç tablo üretmek için kullanılmıştır. Yukarıdaki örnekte, ilk dört satır iki 16 bayt diziyi sağlamak için kullanılmıştır. Bir 8 kaydırması ve bir 24 kaydırması kullanılarak, başka iki yeni 256 giriş anahtar tablosu

üretilebilmektedir.

Offset = 8

Anahtar Sütunu = { 28, D0, 4C, 6E, 86, 8C, C8, 43, A9, EC, 60, 42, 05, F2, 3D, 1C }

Anahtar Satırı = { 6C, BC, AF, C3, 2B, B5, DC, 90, F9, 05, EA, 51, 46, 9D, E2, 60 }

Offset = 24

Anahtar Sütunu = { 6C, BC, AF, C3, 2B, B5, DC, 90, F9, 05, EA, 51, 46, 9D, E2, 60 }

Anahtar Satırı = { 70, 52, 67, 26, 61, 49, 42, 09, 50, 99, 90, A2, 36, 0E, FD, 39 }

Sırayla 0, 8 ve 24 kaydırmaları kullanılarak, üç anahtar tablosu üretmek için 56 bayt tablo kullanılabilmektedir. Bunların tam genişletilmiş formatında bu tablolar 768 bayt işgal edecektir. Bazı kişiler, 07 kartında kullanılan algoritmaların 06, 07 ve 08 serlerinde de kullanıldığını iddia etmektedir. Fakat 08 kodlarının 07 kartına dahil edilmiş olması mümkün değildir. Gerçekte 07 kartı, 06 ve 07 anahtar tablolarını ve belkide biraz daha fazla algoritma içermektedir. 08 kartı sadece, 07 kartının bazı yeni anahtar tabloları ile modifiye edilmiş halidir. 07 kartının tamamen hack edilmesinden sonra 09 serisi kartın lehine olacak bazı yenilikler gerçekleştirilmiştir [1].

Anahtar tabloları adresleme metodunun DES algoritmasında kullanılmış olan S-Box rutinlerine benzediği görülmektedir. Bununla birlikte, S-Box rutinleri çok dayanıklı olması için tasarlanmıştır. Fakat, anahtar tablolarının mı yoksa non-lineerliğin mi dayanıklı olduğu bilinmemektedir.

Standart sabit kaydırma (offset), anahtar üretiminin çok klasik bir metodudur. Sistem, her bir paket için yalancı rasgele bir kaydırma kullanılarak daha güvenli hale getirilebilmektedir. 07 algoritmasını 09 algoritması ile karşılaştırılınca, çok basit bir uygulama olduğu görülmektedir.

5.8.2 07 Ho Lee Fook algoritmasının çekirdek fonksiyonu

07 Ho Lee Fook algoritması, 32 baytlık bir girişten 8 baytlık bir çıkış üretmektedir. Burada, 8 bayt genişlikli r[0..7] yazmaçları vardır. Herhangi bir zamanda bu fonksiyon, iki yazmaç ile çalışmaktadır.

Çekirdek fonksiyonu *f*, bir bayt genişlikte çalışır. Herbir yazmaç sadece 8 bit genişliğindedir ve elde (carry) biti yoktur. Yani, işlemin tamamı 1 bayt genişliğindedir. Bundan dolayı, toplama ve çarpma gibi işlemler kayıplı olacaktır. İki adet 8 bitlik sayı toplandığı zaman

sonuç 9 bitlik bir sayı olabilmektedir. Bu fonksiyon 8 bitte çalıştığı için bu dokuzuncu bit kaybedilmiştir. 8 bitlik bir sayının iki ile çarpılmının tersine çevrilmesi de, aynı sonucu verecek olan iki olası girişi meydana getirmektedir. Makina kodunda iki ile çarpma işlemi, 8 bitlik yazmaçtaki bitlerin sola doğru bir bit kaydırılmasını gerektirmektedir. Böylece, en soldaki bit sıfır olur.

Çizelge 5.8 Sola kaydırma işlemi için verilmiş olan bir örnek [1]

İkilik düzende	Onaltılık düzende	Onluk düzende
1101 1011	DB	219
(1) 1011 0110	1B6	438
1011 0110	B6	182 (dokuzuncu bit atılmıştır)

Çizelge 5.8'den, iki ile çarpma işleminin sadece bütün bitlerin bir adım sola kaydırılmasından ibaret olduğu görülebilmektedir. İki ile bölme işleminde ise bu bitleri bir adım sağa kaydırmak gereklidir. Dokuzuncu bit atıldığı için iki ile bölme işlemi Çizelge 5.9'da gösterilmiş olan sonucu verecektir.

Çizelge 5.9 Sağa kaydırma işlemi için verilmiş olan bir örnek [1]

İkilik düzende	Onaltılık düzende	Onluk düzende
1011 0110	B6	182
0101 1011	5B	91 (bir bit ile sağa kaydırılır)

Buradaki problem, doğru orijinal değerin 219 mu yoksa 91 mi olduğundan emin olunamamasıdır. Dokuzuncu bit atıldığı için, her iki değer de iki ile çarpıldığı zaman 182 değerini vermektedir [1].

Bit kaybının aynı değişkenleri, sayılardan biri bilindiği zaman da dahil olmak üzere iki adet 8 bitlik sayının toplanması ile uygulanmaktadır. Burada, iki olası başlangıç sayısı mevcuttur.

Çarpma ve toplama işlemlerinin bir dizisini sabit uzunluklu bir yazmaçta birleştirerek, bir tekyönlü fonksiyon olduğundan dolayı tersine çevrilmesi imkansız olmadığı için orijinal başlangıç değerinin ne olduğu konusunda pekçok şüphe olan bir fonksiyon yaratmak mümkündür. Bu, korsan VideoCrypt 07 algoritmasındaki çekirdek fonksiyonunun çalışma şeklidir. Bu algoritma, karmaşık yapısını gizleyen basitliğe sahiptir.

Aşağıdaki C dilinde yazılmış olan kod, çekirdek fonksiyonunun gerçekleştirilmesinin sadece bir kısmıdır. Bu fonksiyona giriş olan bayt, mesaj bloğundan gelen bir bayttır.

```
/* 07 Algoritmasının Çekirdek Fonksiyonu */

void Owf(unsigned char byte)

{

unsigned char acc,kpoint,k1,k2;

/* Anahtarın Üretilmesi */

r[Ppos]^=byte;

kpoint=r[Ppos];

k1=key[Offset+(kpoint>4)];

k2=key[Offset+16+(kpoint&0x0f)];

acc=k1+k2;

acc=~acc;

acc=(acc<1)|(acc>7);

/* Fonksiyonun mesaj baytına, anahtara ve yazmaca uygulanması */

acc+=byte;

acc=(acc<1)|(acc>7); /* sola kaydır */

acc=(acc>4)|(acc<4); /* nybble'ları değiş tokuş et */

Ppos++; /* Ppos'u arttır */

Ppos&=7; /* Bu, Ppos'un değerinin sekizden küçük olmasını sağlar */

r[Ppos]^=acc;

}
```

r[Ppos] bayt genişlik çıkış yazmacıdır. Buradaki Ppos, ilgili yazmacın göstergesidir (pointer). Bu fonksiyondaki ilk adım, mesaj baytı ile geçerli çıkış yazmacı olan r[Ppos]'un içeriğini EXOR'lamaktır. Bu, hem geçerli çıkış yazmacının içeriğini değiştirir hem de kpoint isminde bir anahtar pointer'ı yaratır.

Daha sonra bu kpoint anahtar pointer'ı, iki 16 baytlık diziden baytları seçmek için

kullanılmaktadır. Bu baytlar, birinci diziyi adreslemek için yüksek nybble kullanılarak ve ikinci diziyi adreslemek için ise düşük nybble kullanılarak seçilmektedir. Burada bahsedilmekte olan ofset (offset), 56 bayttan uygun tabloyu seçmek için gerekli olan değerdir.

Dana sonra, iki anahtar baytı ilave edilmektedir. acc olarak adlandırılan sonuç, ters çevrilmekte ve iki ile çarpılmaktadır. Bu iki ile çarpma işlemi, sola kaydırma rutinidir. Daha sonra bu anahtar, mesaj baytına ilave edilmektedir. Bunun sonucu iki ile çarpılmaktadır. Daha sonra, yüksek nybble düşük nybble ile değiştirilmektedir.

Nybble'ları değiş tokuş etme prosedürü, basit olmasına rağmen programlama olmaması bakımından karmaşık görünmektedir (Çizelge 5.10). Temelde bu işlem, bölmek için sağa kaydırma ve çarpmak için sola kaydırma kavramlarının bir uzantısıdır. 16 ile bölmek için bitlerin dört defa sağa kaydırılması gereklidir. Bunun sebebi, $2^4 = 16$ olmasıdır. 16 ile çarmak için ise bitlerin dört defa sola kaydırılması gereklidir. 16 ile bölmenin ve çarpmanın sonuçlarını tek bir sayı olarak bütünleştirmek için OR işlemi gerekmektedir.

Çizelge 5.10 Nybble değiş tokuş işlemi için verilmiş olan bir örnek [1]

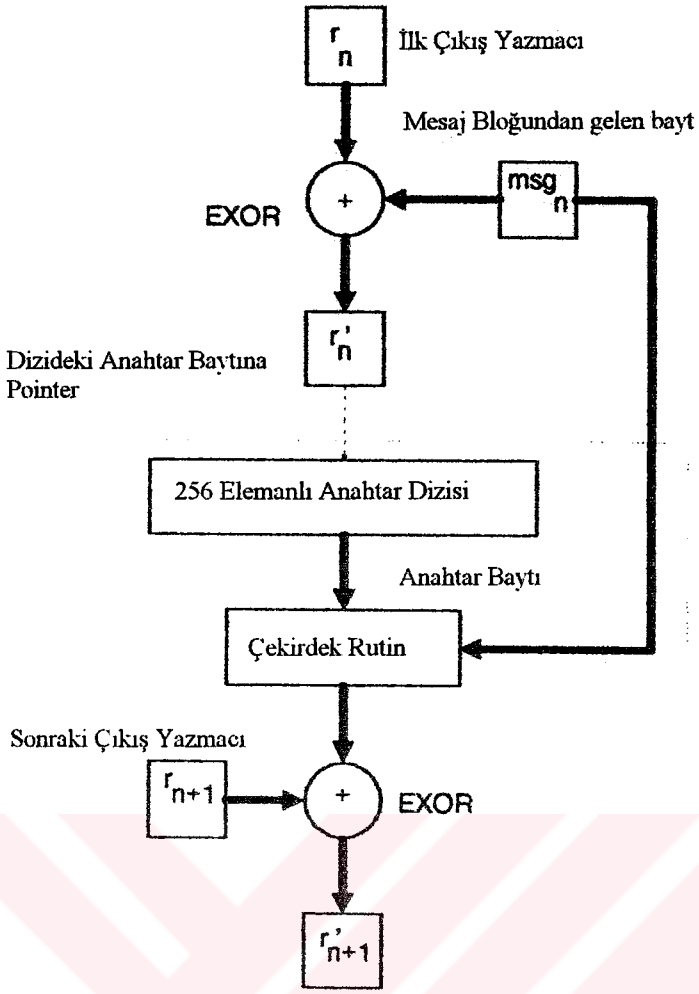
İkilik düzen	Onaltılık düzen	Onluk düzen
1101 1011	DB	219 Orijinal Değer
0000 1101	0D	13 Dört defa sağa kaydırılmış
1011 0000	B0	176 Dört defa sola kaydırılmış

Sonraki prosedür, Ppos pointer'ının değerini artırmaktır. Böylece, sonraki r[Ppos] değerini gösterir. Ppos'un değeri, r[0..7] sekiz çıkış yazmacının sadece birini gösterdiğini görmek için kontrol edilir. Daha sonra acc'nin içeriği r[Ppos] yazmacının içeriği ile EXOR'lanır.

Çekirdek fonksiyonu oldukça açıktır ve C dilinden başka bir programlama diliyle de gerçekleştirilebilmektedir. Buradaki başlıca problem, bayt genişlik yazmaçlarının tanımlanmasıdır. bu durum, yapısal programlama dillerinin çoğunda büyük bir problem olmazken Qbasic programlama dilinde problemlere yol açabilmektedir.

Şekil 5.10'da gösterilmiş olan her durumda her bir yazmacın genişliği tek bir bayttır. Mesaj bloğunun tamamı 32 bayt ve çıkış bloğunun tamamı ise 8 bayt genişliğindedir.

Bu algoritma bu şekilde oldukça lineerdir. Dikkate alınması gereken başlıca durum, iki ile toplama veya çarpma fonksiyonlarının kayıplı olmasıdır. Bu yüzden, bu fonksiyonlardan birinin tersine çevrilmesi durumunda iki olası cevap ortaya çıkmaktadır.



Şekil 5.10 Tek aşamalı Ho Lee Fook algoritmasının blok diyagramı [1]

5.8.3 07 Ho Lee Fook algoritmasının çalışma şekli

Ho Lee Fook algoritmasının sağlamlığı, çekirdek fonksiyonunun 99 defa uygulanması gerçeğine dayanmaktadır. 32 baytlık mesaj bloğu, 8 baytlık çıkış bloğuna dönüştürülmektedir. Uygulanma düzeni Çizelge 5.11'de gösterilmiştir.

Çizelge 5.11 Ho Lee Fook algoritmasının uygulanma düzeni [1]

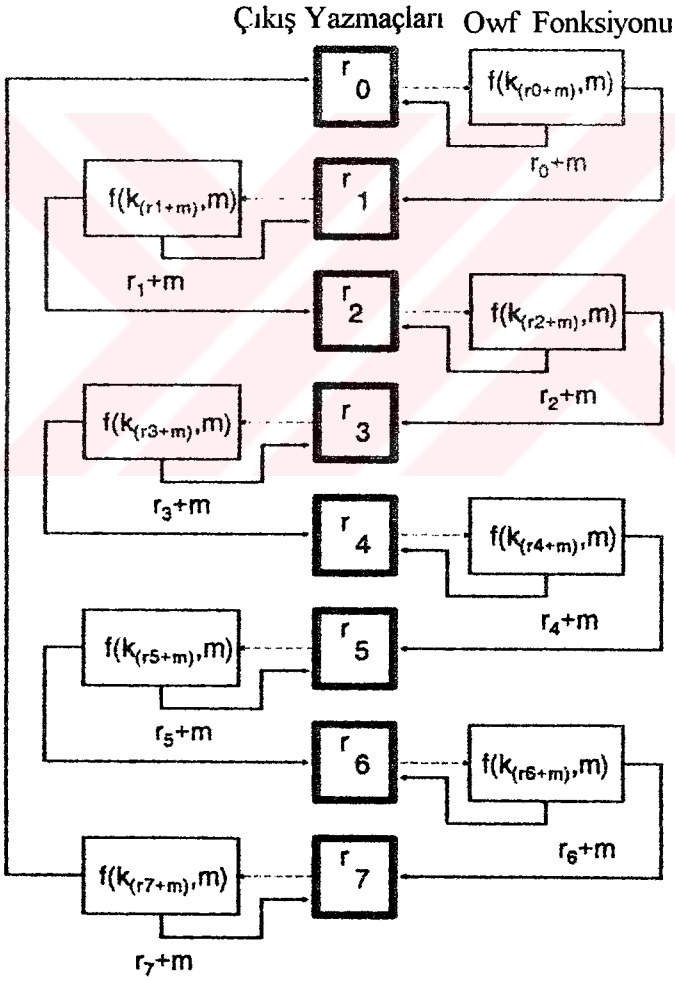
Giriş Baytı	İşlemden geçme sayısı
msg [0...26]	Fonksiyon boyunca bir defa işlemden geçer
0	Fonksiyon boyunca iki defa işlemden geçer
msg [27...29]	Fonksiyon boyunca iki defa işlemden geçer
msg [31]	Fonksiyon boyunca 64 defa işlemden geçer

Otuzikinci bayt olan Bayt 31, algoritmanın tersine çevrilmesini aşırı derecede zor hale getirme amacını taşımaktadır. Çoğunlukla bu bayt, bozucu (destructor) bayt olarak adlandırılmaktadır.

Otuzbirinci bayt olan Bayt 30, çekirdek fonksiyonu boyunca işlemden geçirilmez. Bu bayt, 27, 28, 29 baytları ile birlikte paketin kontrol işlemini sağlamak için kullanılmaktadır.

Algoritmayı 32 bayt mesaj bloğundan 8 bayt çıkış bloğuna dönüştürme durumu, bir mesaj özetine çok benzerdir. Veri akışından tek bir kod çözme anahtarının çıkarılmış olmasının yanısıra, VideoCipher ve EuroCrypt durumlarında olduğu gibi paketin tamamı kodlanmış anahtar olmaktadır.

Eğer baytlardan herhangi biri yanlışsa, o zaman bileşke çıkış bloğu yanlış olacaktır [1]. Bu bakımdan bu çok mükemmeldir. Yetki verme verisi, kanal kimlik bilgisi ve kod çözme bilgisinin doğruluğunu garanti edilmektedir. Orijinal kart, kontrol işleminde başarısız olan herhangi bir paketi kabul etmeyecektir. Yani, kart kimlik bilgisi ve kontrol işlemi rutinlerini bilmeyen bilgisayar korsanları tarafından korsan karta yetki verilemeyecektir.



Şekil 5.11 Ho Lee Fook algoritmasının basitleştirilmiş bir modeli [1]

Fakat, bir bilgisayar korsanı kontrol işlemi prosedürünü, akıllı kartı açma talimatlarını

biliyorsa ve anahtar tablolu geçerli bir algoritmaya sahipse, bu sistem tamamen saldırıya açık olacaktır. Bu durum, Phoenix ve Genesis programları ile nelerin yapıldığını göstermektedir.

Ho Lee Fook algoritmasının basitleştirilmiş bir modelini Şekil 5.11'de gösterilmiştir. Verilmiş olan bu model peryodiktir. Çıkış yazmaçları boyunca mesaj bloğundan baytların dağıtımı, bayt 26'ya kadar lineerdir. Kontrol işlemi için rutin biçimi değişmektedir. Fakat bu biçim, peryodik yapıyı sürdürür.

Herbir durumdaki + işareti, modülo 2 toplamayı veya EXOR'lamayı göstermektedir. r_n+m ise, mesaj baytının yazmacın içerikleri ile EXOR'landığını göstermektedir. Mesaj baytı m ve ilgili çıkış yazmacı r'yi EXOR'lamak ve $f(k_{(r+m)},m)$ fonksiyonunun çıkışının ilgili çıkış yazmacı r ile EXOR'lanması gibi EXOR'lama evrelerinden bazıları bu modelin kolayca anlaşılabilmesi için ihmal edilmiştir.

Çizelge 5.12 Mesaj bloğu baytlarının dağıtımı [1]

Çıkış	Mesaj Baytı
0	00 08 16 24 -- 31 31 31 31 31 31 31 31
1	01 09 17 25 28 31 31 31 31 31 31 31 31
2	02 10 18 26 28 31 31 31 31 31 31 31 31
3	03 11 19 *0 -- 31 31 31 31 31 31 31 31
4	04 12 20 *0 29 31 31 31 31 31 31 31 31
5	05 13 21 -- 29 31 31 31 31 31 31 31 31
6	06 14 22 27 -- 31 31 31 31 31 31 31 31
7	07 15 23 27 31 31 31 31 31 31 31 31 31

Mesaj bloğundan bir baytın yerine 0 değerinin kullanıldığı yer *0'dır. Bu, kontrol işlemi rutininin ilk iki turu (round) için bu şekilde olmaktadır. -- sembolünün olduğu yerlerde yazmaç atlanmaktadır. Ayrıca, bayt 31'in herbir yazmaca kaç defa uygulandığı sayılırsa, herbir yazmaca sekiz defa uygulandığı görülür (Çizelge 5.12).

Ayrıca bu durum, bir yazmaç ile ofset olsa bile çekirdek fonksiyonunun çıkışının uygulamasında tekrarlanmaktadır. Buradaki farklılık, *0 baytlarının işlenmesinin farklı sonuçlar vermemesidir.

Çizelge 5.13'te gösterilmiş olan basit modelde, her bir turda (round) çıkış yazmaçlarının ikisinde değişiklik olduğu görülmektedir. Turun başlangıcındaki yazmaç, kendisiyle EXOR'lanmış bir mesaj baytına sahiptir. Şimdi bu, çekirdek fonksiyonu için anahtar göstergesi olmuştur. Daha sonra, çekirdek fonksiyonunun çıkışı sonraki çıkış yazmacının içerikleriyle EXOR'lanmaktadır.

Çizelge 5.13 Çekirdek fonksiyonu çıkış baytlarının dağıtımı [1]

Çıkış	Dağıtım
0	-- 07 15 23 30 35 42 51 59 67 75 83 91
1	00 08 16 24 -- 36 44 52 60 68 76 84 92
2	01 09 17 25 31 37 45 53 61 69 77 85 93
3	02 10 18 26 32 38 46 54 62 70 78 86 94
4	03 11 19 27 -- 39 47 55 63 71 79 87 95
5	04 12 20 28 33 40 48 56 64 72 80 88 96
6	05 13 21 -- 34 41 49 57 65 73 81 89 97
7	06 14 22 29 -- 42 50 58 66 74 82 90 98

Aşağıda verilmiş olan program, 07 Ho Lee Fook algoritmasının uygulamasını göstermektedir [1]. Fakat bu programda, kanalların gerçekleştirdiği elektronik karşı tedbirler için önemli kontrol işlemleri yapılmamaktadır. Mesaj bloğunun değiştirilmesi, sadece mevcut değerlerin üzerine yazılması ve yeniden derlenmesi durumundan ibarettir. Bu program, Turbo C++ dilinde yazılmış ve derlenmiştir [1].

```
#include <stdio.h>
/* This a model of the Ho Lee Fook Algorithm
as used in the hack on VideoCrypt. */
unsigned char key[56] = {
0x65, 0xe7, 0x71, 0x1a, 0xb4, 0x88, 0xd7, 0x76,
0x28, 0xd0, 0x4c, 0x6e, 0x86, 0x8c, 0xc8, 0x43,
0xa9, 0xec, 0x60, 0x42, 0x05, 0xf2, 0x3d, 0x1c,
0x6c, 0xbc, 0xaf, 0xc3, 0x2b, 0xb5, 0xdc, 0x90,
0xf9, 0x05, 0xea, 0x51 , 0x46, 0x9d, 0xe2, 0x60,
0x70, 0x52, 0x67, 0x26, 0x61, 0x49, 0x42, 0x09,
0x50, 0x99, 0x90, 0xa2, 0x36, 0x0e, 0xfd, 0x39
};
unsigned char r[8]; /* This is the key output */
unsigned char msg[32]= {
0xf8,0x3f,0x6a,0x29,0x51,0x19,0x01,0x8a,
0xâ7,0xbc,0x50,0xeb,0xec,0xed,0xee,0xef,
0xf0,0xf1,0xf2,0xf3,0xf4,0xf5,0xf6,0xf7,
0xf8,0xf9,0xfa,0x8c,0x7a,0x20,0xff,0x41
};
```

```
/* This is the message packet */
int Ppos=0, Offset=0;
/* Core Function */
void Owf(unsigned char byte)
{
unsigned char acc,kpoint,k1,k2;
r[Ppos]^=byte;
kpoint=r[Ppos];
k1=key[Offset+(kpoint>4)];
k2=key[Offset+16+(kpoint&0x0f)];
acc=k1 + k2;
acc=~acc;
acc = (acc<1) | (acc>7);
acc+=byte;
acc = (acc< 1) | (acc>7);
acc = (acc>4) | (acc<4);
Ppos++;
Ppos&=7;
r[P pos]^=acc;
}
void main (void)
{
unsigned char a,b=0;
for(a=0;a<8;a++) r[a]=0; /* initialise key */
if(msg[1]<0x33) /* Calculate Offset */
Offset=0x00;
else if(msg[1]<0x3b)
Offset=0x08;
else
Offset=0x18;
```

```
printf("Offset (in hex) = ");
printf("%X ",Offset)
printf("\n");
for(a=0;a<27;a++)
Owf(msg[a]);
/* Checksumming Routine */
printf("\n * Checksumming Routine * \n ";
printf("Conditions: valid checksum r[a] = msg[Ppos] \n");
printf("If this routine is omitted then the algorithm \n");
printf("will decrypt any msg packet without actually \n");
printf("checking to see if it is valid. \n \n");
for(a=27;a<31;a++)
{
Owf(b);
Owf(b);
b=msg[a];
printf("%X ", msg[a]);
printf("%X ", r[Ppos]);
if(msg[a]!=r[Ppos])
{putchar(7); printf("Invalid Checksum Result \n");}
else printf("Valid Checksum Result \n")
Ppos++; Ppos&=0x07;
}
for(a=0;a<64;a++) Owf(msg[31]); /* Apply Destructor Byte */
printf(" \n Message Block: \n");
for (a=0;a<16;a++)
printf("%X ",msg[a]);
printf("\n");
for (a=16;a<32;a++)
printf("%X ",msg[a]);
printf("\n"); printf(\n");
```

```
printf("The decrypt key is: \n");
for(a=0;a<8;a++) printf("%x ", r[a]);
}
```

5.9 09 Algoritması

20.06.1994 yılında Londra'da Dorchester isimli otelde gerçekleştirilmiş olan açık arttırmada, 09 Sky kodunun çalışan bir kopyası bilgisayar korsanlarına satışa sunulmuştu. Fakat bundan kısa bir süre sonra Sky Channel, bir elektronik karşı tedbir gerçekleştirerek satışa sunulmuş olan bu kodun çalışmasını engel olmuştu. Açık arttırmada satılan bu kod, Sky ve News Datacom karşı tedbir gerçekleştirinceye kadar sadece bir hafta kadar kullanılabilmiştir [1].

07 algoritmasındaki düşüncelerin büyük bir kısmı 09 algoritmasında da görülmektedir. Fakat bu algoritmalar modifiye edililerek daha güvenli hale getirilmişti ve bu yüzden 09 algoritmasının ters mühendisliği oldukça zordur.

09 algoritmasının önemli elemanlarından biri, çekirdek fonksiyonunda çarpma işleminin kullanılmasıdır. Bu, 07 korsan akıllı kart endüstrisinin merkezi olan PIC16C84 mikrokontrolörünü kullanım dışı bırakmak için Sky Channel tarafından gerçekleştirilmiş olan bir saldırıydı [1]. Çünkü, PIC16C84 mikrokontrolöründe çarpma komutu yoktur.

5.9.1 09 kodundaki anahtar tabloları ve anahtar seçimi

09 kodundaki başlangıç anahtar tablosunun büyüklüğü 256 bayttır. Bu büyüklük, 07 kodunda 56 bayttır. 07'deki kod tablosu kavramı 09 kodunda da mevcuttur.

Her bir turda anahtar üretmek için kullanılması gereken kod bölümü, mesaj paketinden elde edilen bir ofset kullanılarak seçilmektedir. Bilinen üç seçim vardır. Seçimlerin ikisi, anahtar üretiminde tek bit 64 baytlık dizi kullanımına izin vermektedir. Diğer seçim ise, iki 64 baytlık dizinin EXOR toplamını kullanmaktadır.

07 kodunda anahtar baytları çiftler halinde kullanılmıştır. İki adet 16 baytlık anahtar dizisi vardır. 09 kodunda bu dizilerin herbiri 64 bayta yükseltilmiştir. Satışa çıkarılmış olan bu yeni versiyondaki seçimlerin büyük bir kısmı tek bir 64 baytlık dizi kullanmasına rağmen, iki dizinin bir kombinasyonu için bir koşul mevcuttu. Bu ikili dizi seçimi 26.06.1994 tarihine kadar kullanılmıştır.

07 kodunda toplama işlemi olan anahtar kombinasyonu fonksiyonu, bunun 09 kodu versiyonunda EXOR ile değiştirilmiştir. Bu değişikliğin nedeni, anahtar baytlarını okuma

girişimlerini engellemektir.

5.9.2 09 kodunun çekirdek fonksiyonu

Bu, algoritmanın genel yapısındaki en büyük değişikliktir. 07 kodu herhangi bir tur (round) boyunca sadece çıkış yazmaçlarının bir çiftinde çalışmasına rağmen 09 kodu, sekiz çıkış yazmacının hepsinde çalışmaktadır. Herbir turdan sonra bu sekiz yazmacın tamamının içeriğinin değişmesinin amacı, 07 versiyonundaki kontrol işlemi baytlarından önce bu baytlara yapılan saldırının 09 algoritmasında çalışmamasını sağlamaktır.

09 çekirdek fonksiyonunun yapısı, dört rutinden oluşmaktadır. Bu rutinlerin ilk üçü aynıdır ve r[2...7] yazmaçlarında çalışmaktadır. Son rutin, önceki rutine benzemesine rağmen birkaç sabit tanıtmaktadır. Bu rutin, r[0] ve r[1] yazmaçlarında çalışmaktadır.

İlk üç aşama, farklı anahtarlar kullanmaktadır. Anahtar baytının göstergesi (pointer), çıkış yazmacının başlangıcını 3Fh ile AND'lenmesi ile elde edilmektedir. Bu, gösterge için sadece 64 olası değerin olmasını sağlar. Bu gösterge değeri, doğru baytı seçmek için eklenmiş bir ofsete sahiptir. Bu ofset, mesaj paketindeki bir bayt kullanılarak ayarlanabilmektedir. Sky Channel'ın saldırmış olduğu bu versiyonda şu seçimler kullanılmıştır:

```
k1 = r[i] & 0x3F;

k = key[k1]^key[k1 + 0x98];
```

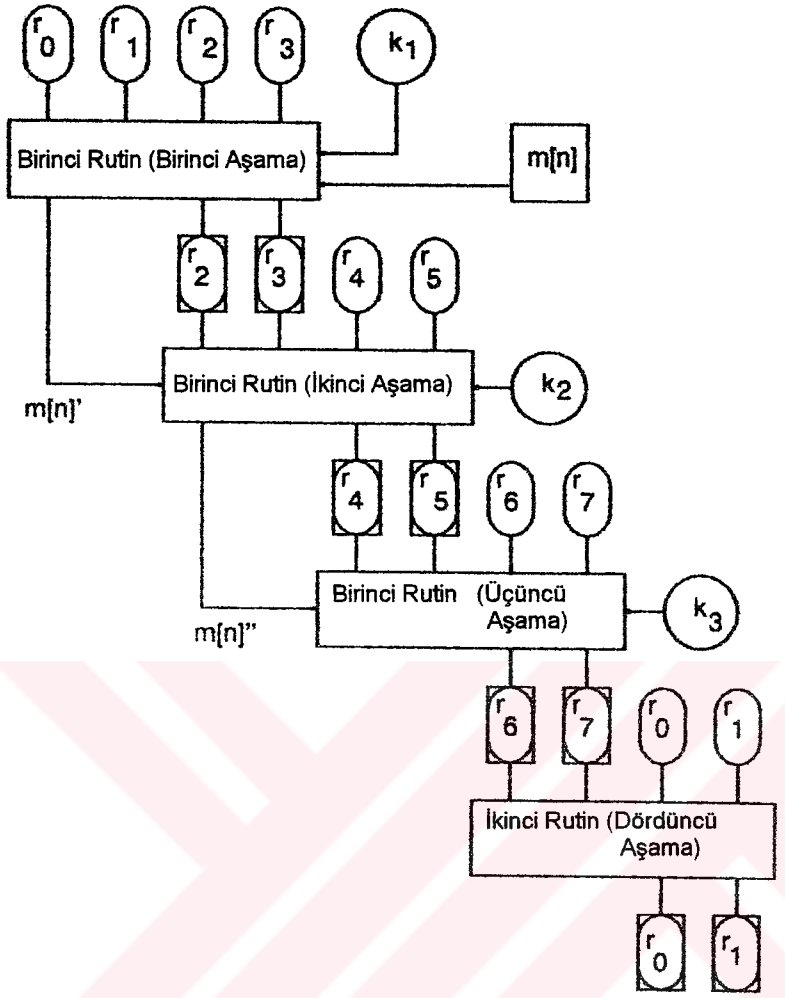
Her iki rutinde de kullanılmış olan işlem çarpma işlemidir. Bu çarpma işleminin sonucu 64 bitlik bir sayıdır. Bu sonuç, daha sonra bu aşama tarafından değiştirilmiş olan iki çıkış yazmacının içerikleri ile birleştirilecek olan iki bayta ayrılmıştır.

Birinci rutindeki çarpma işlemi; mesaj baytı, anahtar baytı ve çıkış yazmaçlarının üçünün bir kombinasyonunda çalışmaktadır. Bu mesaj, ikinci ve üçüncü aşamalar için değiştirilmektedir.

İkinci rutin, r[6] ve r[7] çıkış yazmaçlarının içeriklerini çarpmaktadır. Yüksek bayt ve düşük bayt, r[1] ve r[0] yazmaçları üzerinden dağıtılmaktadır. Daha sonra bu yazmaçların içeriklerine bir sabit eklenir ve ayrıca sonucun bir IF koşulunu sağlayıp sağlayamamasına göre bir arttırılabilmektedir.

Şekil 5.12'de görüldüğü gibi 09 çekirdek fonksiyonu, iki rutine dayanmaktadır. Birinci rutin üç defa ve ikinci rutin ise sadece bir defa kullanılmaktadır. Anahtar baytı k_n sadece ilk üç aşamada uygulanmaktadır. Mesaj baytı m[n] birinci aşamada uygulanmaktadır. Daha sonra bu bayt iki ile çarpılmakta ve bu sonuca bir sabit eklenmektedir. Bu yeni değer m[n]' ikinci

aşamada kullanılmaktadır. Bu işlem, m[n]" yi verinceye kadar tekrarlanmaktadır. Bu değer, üçüncü aşamada kullanılmaktadır.



Şekil 5.12 09 çekirdek fonksiyonunun modeli [1]

Dördüncü aşama, önceki aşamalardan farklı bir rutin kullanmaktadır. Diğerlerinden farklı olan bu rutin, önceki rutin ile benzer olmasına rağmen bir takım sabitleri kullanmamaktadır. Ayrıca bu aşamada, anahtar baytı ve mesaj baytı kullanılmamaktadır.

Herbir aşamada, sadece iki yazmacın içerikleri değişmektedir. Bu yazmaçlar, Şekil 5.12'de gösterilmiş olan diyagramda kutu içine alınmış olan r_n yazmaçlardır [1]. Yuvarlaklaştırılmış kutular, her aşamada kullanılmıştır. Fakat bunların içerikleri gerçek anlamda değişmemiştir.

5.9.3 Dorchester 09 kodunun yapısı

Dorchester 09 kodu ile ilgili şaşırtıcı durum, 07 kodunda olduğu gibi aynı 27-4-1 yapısını kullanmasıdır [1]. İlk 27 baytın herbiri bir defa işlemden geçirilmektedir. Sonraki 4 bayt, paket için kontrol işlemlerini sağlamak için kullanılmaktadır. Son bayt ise 64 defa işlemden

geçirilmektedir.

Kontrol işlemi rutini, 07 için kullanılan ile büyük benzerlik göstermektedir. 09 kodunda, r[7] çıkış yazmacının içeriğinin mesaj baytına karşı kontrol edilmesi ilave edilmiştir. 09 serisi akıllı karta kadar abone yönetim yazılımı, mesaj paketinin bu yapısına bağlıydı. Bu yüzden 09 kartı için, sadece sıralamada bazı küçük değişiklikler yapılabilmiştir.

27.06.1994 tarihinde gerçekleştirilmiş olan elektronik karşı tedbir, Dorchester koduna dayanan algoritmayı çalışmaz hale getirmişti. Zaten bu zamana kadar kullanılmış olan algoritma gerçek algoritmanın geçiş versiyonuydu. Dorchester açık arttırmasında bu kodu satın almış olan bilgisayar korsanları, bu kodun tamamı çok pahalı olduğu için satın alamamıştı [1].

1994 yılı Ekim ayının sonlarına doğru gerçekten başarılı bir korsan 09 kartı ortaya çıktı. Bu kartın kodu, Dorchester kodunun ve orijinal 09 akıllı kartından ters mühendislikle elde edilmiş olan kodun bir kombinasyonuydu.

Aslında kanalın gerçekleştirmiş olduğu bu elektronik karşı tedbir oldukça basitti. Değiştirilmesi gerekli olan şey algoritmanın kendisiydi. News Datacom, 74h paketinin içine altkomutlar (nanokomutlar) entegre etmişti. Bu nanokomutlar, karma fonksiyonun farklı giriş verisi ile veya farklı tekrar sayısında gerçekleştirilmesini sağlamaktadır. Gerçekte bu nanokomutların bazıları oldukça dolambaçlı olduğundan dolayı kart belleğinin yeniden programlanmasına izin vermektedir.

Nanokomutların kullanımı, bilgisayar korsanlarını kriptografik teori bakımından etkisiz hale getirmiştir. Bilgisayar korsanları korsan piyasa için fonksiyonların karttaki uygulanma sürelerinin ölçümü, clock çevrimlerinin hesaplanması ve ayrıca çekilen akımın kontrol edilmesi üzerinde çalışmaktaydı. Bu yüzden piyasada korsan kart mevcut değildi ve kısa bir süre için de olsa sistemi yeniden güvenli olduğu için Sky Channel bu durumdan memnundu.

Aşağıda, 09 Dorchester kodunun çekirdek fonksiyonu verilmiştir [1]. Bu, her bir turdaki cevap yazmaçlarının tamamının içeriğini değiştirdiği için 07 çekirdek fonksiyonundan daha karmaşıktır. Fakat anahtar seçimi 07 ile kıyaslanırsa basitleştirilmiştir.

```
/* The 09 Core Function */
void 0wf09(const unsigned char in, unsigned char *r) {
unsigned char a, b, c, d, key; unsigned short acc;
int i; a=in;
/* Routine 1 - affects r[2], r[3], r[4], r[5], r[6], r[7] */
for (i =0; i <=4; i +=2) { b= r[i] &0x3f;
/*simplified key selection */
key = key09 [b] ^ key09 [b + 0x98] ;
c = a + key - r[i+1] ;
d = (r[i] - r[i+1]) ^ a;
acc = d * c;
/* EXOR 1ow byte of result with r[i+2] */
r[i + 2] ^= (acc & 0xff) ;
/* Add high byte of result to r[i+3] */
r[i + 3] += acc > 8;
acc = (a < 1) | (a > 7) ;
acc += 0x49;

/* Routine 2 - affects r[0], r[1] /*
acc = r[6] * r[7] ;
/* Add low byte of result to r[0] */
a = (acc & 0xff) + r[0] ;
if (a < r[0] ) a++;
r [0] = a + 0x39;
/* Add high byte of result to r[1] */
a = (acc > 8) + r[1] ;
if (a < r[1]) a++;
r [1] = a + 0x8f;
return;
}
```

5.9.3.1 Dorchester kodunun C programlama dilinde yazılmış hali

Elektronik karşı tedbirden sonra kullanılmış olan kod çok daha fazla karmaşıktı. Dorchester kodu, kesinlikle asıl kodun sadece bir geçiş formatıydı. Bu alınmış olan karşı tedbir, nanokomutları baz almaktaydı. Bu paketler, karma fonksiyona girişler olarak kartın adres boşluğundan gelen baytları kullanmış olan alt talimatları taşımaktaydı. Bunun diğer versiyonları karma fonksiyonun son baytta 64 defadan fazla uygulanmasını sağlamaktadır. Bu kart çarpma komutlarına güvendiği için PIC16C84'ü bu uygulamada artık kullanılamaz hale getirmiştir. Çünkü PIC16C84 mikrokontrolöründe çarpma komutları bulunmamaktadır [1].

```
/*
* This is the algorithm and key as used in a PICl6C84
* BSkyB clone card . It worked fine between 1994-05-18
* and 1994-06-27. It still produces the correct signature;
* but not the correct hash result after 1994-06-28.
*
* MK, 1994-06-30
*/
const unsigned char key09[216] = {
0x91, 0x61, 0x9d, 0x53, 0xb3, 0x27, 0xdS, 0xd9,
0x0f, 0x59, 0xa6, 0x6f, 0x73, 0xfb, 0x99, 0x4c,
0xfb, 0x45, 0x54, 0x8e, 0x20, 0x5f, 0xb3, 0xbl,
0x38, 0xd0, 0x6b, 0xa7, 0x40, 0x39, 0xed, 0x2a,
0xda, 0x43, 0x8d, 0x51, 0x92, 0xd6, 0xe3, 0x61,
0x65, 0x8c, 0x71, 0xe6, 0x84, 0x65, 0x87, 0x03,
0x55, 0xbc, 0x64, 0x07, 0xbb, 0x79, 0x9e, 0x40,
0x97, 0x89, 0xc4, 0x14, 0x8f, 0x8b, 0x41, 0x4d,
0x2a, 0xaa, 0xe8, 0xe1, 0x08, 0xcd, 0x82, 0x43,
0x8f, 0x6f, 0x36, 0x9b, 0x72, 0x47, 0xf2, 0xa4,
0x49, 0xdd, 0x8b, 0x6e, 0x26, 0xc6, 0xbf, 0xb7,
0xd8, 0x44, 0xc3, 0x70, 0xa3, 0x4c, 0xb6, 0xb2,
0x37, 0x9b, 0x09, 0xdf, 0x32, 0x28, 0x24, 0x86,
0x8d, 0xSf, 0xe6, 0x4b, 0xSd, 0xd0, 0x2f, 0xdb,
```

```
0xac, 0x2e, 0x78, 0xle, 0xcc, 0x52, 0xcl, 0x61,
0xea, 0x82, 0xca, 0xb3, 0xf4, 0x8f, 0x63, 0x8e,
0x6c, 0xbc, 0xaf, 0xc3, 0x2b, 0xbS, 0xdc, 0x90,
0xf9, 0x05, 0xea, 0x51, 0x46, 0x9d, 0xe2, 0x60, .
0x01, 0x35, 0x59, 0x79, 0x00, 0x00, 0x55, 0x0f,
0x00, 0x00, 0x00, 0x00, 0x10, 0x6e, 0xlc, 0xbd,
0xfe, 0x44, 0xeb, 0x79, 0xf3, 0xab, 0x5d, 0x23,
0xb3, 0x20, 0xd2, 0xe7, 0xfc, 0x00, 0x03, 0x6f,
0xd8, 0xb7, 0xf7, 0xf3, 0x55, 0x72, 0x47, 0xl3,
0x7b, 0x0c, 0x08, 0x01, 0x8a, 0x2c, 0x70, 0x56,
0x0a, 0x85, 0xl8, 0xl4, 0x43, 0xc9, 0x46, 0x64,
0x6c, 0x9a, 0x99, 0x59, 0x0a, 0x6c, 0x40, 0xd5,
0x17, 0xb3, 0x2c, 0x69, 0x41, 0xe8, 0xe7, 0x0e
};
/*****************************************************
Only 64 bytes of this table were used This allowed some
implementations to reduce the key selection routine and
the key storage. This resulted in a significant memory saving in the
PICl6C84 implementations.
***************************************************** /
void kernel_b(const unsigned char in, unsigned char *answ,
const unsigned char sel)
{
unsigned char a, b, c, d;
unsigned short m;
inti;
a=in;
/* Routine 1 */
for (i = 0; i <= 4; i +=2) {
b = answ[i ] & 0x3f;
i f (sel <= 8 ) {
```

```
i f (sel == 2) b = key09[b + 0x40] ;
else {
i f (sel < 2 && b == 0) b = key09 [b + 0x8d] ;
else
b = key09[b] ^ key09[b + 0x98] ;
}
} else
b = key09 [b] ^ key09 [b + 0x98] ; /* only this one is used */
c=a+b-answ[i+1];
d = (answ[i] - answ[i+1]) ^ a;
m=d*c;
answ[i +2] ^=(m&0xff);
answ[i + 3] += m > 8;
a = (a < 1) | (a > 7) ;
a += 0x49 ;
}
/* Routine 2 */
m = answ[6] * answ[7] ;
a = (m & 0xff) + answ[0] ;
i f (a < answ[0] ) a++;
answ[0] = a + 0x39;
a = (m > 8) + answ[1] ;
if (a < answ[1]) a++;
answ[1] = a + 0x8f;
return;
}
int decode_b(const unsigned char *msg, unsigned char *answ)
{
int i, j;
int check = 0;
unsigned char b = 0;
```

```
for (i =0; i < 8; i++) answ[i] =0; /* Clear answer regs */
for (i = 0; i < 27; i++) /* Do Kernel */
kernel_b(msg[i], answ, msg[1]);
/* Hash Checksum */
for [i = 27; i < 31; i++) {
kernel_b(b, answ, msg[1]);
kernel_b(b, answ, msg[1]);
b=msg[i];
if (b != answ[7]) check |= 1;
/* Process Last Byte */
/*******************************************************
This is the point at which the processing changed after the ECM of
27-06-94. Depending on a card command sent in the 74h, the card
would execute a series of nanocommands which handled the
processing differently. The packet would of course have a valid
hash checksum and would look just like any other packet.
*******************************************************/
for (i = 0; i < 64; i++)
kernel_b(msg[31], answ, msg[1]);
answ[7] &= 0x0f;
/* test checksum */
b=0;
for (i = 0; i < 32; i++)
b+=msg[i];
if (b != 0) check | = 2;
return check;
}
```

5.10 EuroCrypt-M Karıştırıcı Sisteminin İncelenmesi

EuroCrypt-M D2-MAC sisteminin uygulamasında bazı hatalar yapılmıştır. Çünkü bu sistem, McCormac Hack işlemine karşı tamamen savunmasızdı ve bu yüzden sistem, ciddi bir şekilde

tehlike altındaydı. Bu yüzden, 1992 yılının sonlarına doğru EuroCrypt-M sistemi hack edilmiştir [1]. Bunun sonuçları, France Telecom ve EuroCrypt-M sistemini kullanmış olan kanallar için tam bir felaket olmuştur. France Telecom, Megasat firmasına karşı yasal işlem başlatmıştı. Çünkü bu firma, EuroCrypt-M sisteminin korsan akıllı kartlarının en önemli üreticilerinden biriydi. Bunun sonucunda, mahkeme kararına göre Megasat firması artık korsan EuroCrypt-M kartları satamayacaktı [1].

5.10.1 Kullanmış olduğu algoritma

EuroCrypt sistemindeki tehlikeli eleman, algoritmadan ziyade anahtardır. Bu sistemin kullanmış olduğu algoritma, DES algoritmasıydı. Bu algoritma, kullanılmış olan yazılım uygulamasında daha hızlı çalışması için modifiye edilmiştir. Bu algoritmadaki başlangıç ve ters başlangıç permütasyonları, EuroCrypt-M uygulamasında kullanılmamıştır.

1992 yılında "Subscription Television Conference" isimli konferansta, EuroCrypt sisteminin bankaların kullandığı algoritmalardan birini kullandığı açıklanmıştı [1]. Bundan sonra, seçilebilecek olan algoritmayı bulmak çok kolaydı. Çünkü bankalar, DES ve RSA algoritmalarını kullanmaktadır.

Bu iki algoritmadan DES algoritması, EuroCrypt-M sistemi için daha uygundu. Çünkü EuroCrypt-M sisteminin akıllı kartı, RSA algoritmasını kontrol sözcüğü üretiminin bir parçası olarak güvenli bir şekilde kullanacak hesap yapma gücüne sahip değildi. Bundan dolayı, bu sistemde kullanılmış olan algoritma ya DES algoritması ya da bunun bir varyantı olmalıydı.

DES algoritmasındaki problem, bu algoritmanın bir donanım uygulamasına yönelik donatılmış olmasıydı. Bu yüzden, bir mikrokontrolör de olsa bunu bir yazılımda gerçekleştirmek zor olabilirdi. EuroCrypt akıllı kartı, 6805 mikrokontrolöründe modellenmiştir ve bu 3.5 MHz'te çalışmaktadır. Bu algoritmada gerçekleştirilecek olan herhangi bir değişiklik, güvenliğini zayıflatmaksızın kod çözme işlemini hızlandırmayı amaçlamıştır.

Bu algoritmada gerçekleştirilmiş olan en belirgin değişiklik, başlangıç permütasyonunun ve ters başlangıç permütasyonunun algoritmadan çıkarılmış olmasıdır. NET_DES.ARC isimli bir bilgisayar programı, bu permütasyonların yazılımda uygulanması durumunda işlemin yavaşlamasına neden olacağını saptamıştı. Bu yüzden bu algoritma, permütasyonlar olmaksızın yazılımda gerçekleştirilmiştir. Bu permütasyonlar uygulamadan çıkarılmış olsa bile, bir karıştırıcı sistemde kullanmak için DES algoritması hala iyi bir algoritmaydı. Fakat,

anahtar yönetme protokolünün iyi olması şarttır.

DES algoritmasının EuroCrypt-M sistemindeki uygulaması, başlangıç ve ters başlangıç permütasyonlarının algoritmanın daha hızlı çalışması için çıkarılmış olduğu Electronic Code Book modudur. Havadan iletilmiş olan çekirdek, sonuca ulaşmak için bu algoritma kullanılarak kodlanmıştır.

Ayrıca DES algoritmasının EuroCrypt-S2 sistemindeki uygulaması da Electronic Code Book modudur [1]. Bu durumda, bu algoritma kullanılarak çekirdeğin kodu çözülmekteydi. Ayrıca bu durumda, başlangıç ve ters başlangıç permütasyonları da kullanılmıştır.

5.10.2 EuroCrypt Phoenix arabirimi

D2-MAC EuroCrypt sistemini geniş bir alana yayılmış olan Phoenix tipi saldırıdan koruyan bir yaklaşım, kritik algoritmanın gerçekleştirilmesinin daha kolay olmasıdır. Bununla birlikte, EuroCrypt kartlarını test etmek için Phoenix progranları geliştirilmiştir. Bu programlara gerçek anlamda ihtiyaç olmadığı için bu programlar yayılmamıştır. Diğer bir yaklaşım ise EuroCrypt sistemindeki anahtar kullanma prosedürlerinin VideoCrypt sisteminde kullanılanlardan farklı olmasıydı.

EuroCrypt sistemindeki kritik eleman, kullanmış olduğu anahtarlardır. Teorik olarak bu algoritmanın tersine çevrilmesi çok zordur. Fakat bu algoritmalar, DES algoritması hack etme cihazları kullanılarak tersine çevrilebilmekteydi. Fakat bu cihazlar, bilgisayar korsanlarının bütçesini çok aşmaktaydı.

EuroCrypt sisteminin tasarımcılarının anahtar kullanma teorileri uygulandığında, bu sistemin hack edilmesi çok zorlaşmıştır. Bununla birlikte, EuroCrypt sistemini kullanmakta olan kanalların kullanmış olduğu akıllı kartların büyük bir kısmı EPROM'du. Bu yüzden, anahtarların sık sık güncellenmesi mümkün değildi.

Bu teknik özelliklerde kullanılmış olan EuroCrypt sisteminin en iyi örneği Cine Cinemas kanalıdır [1]. Bu kanal, anahtarlarını düzenli olarak güncellemekteydi. Fakat buradaki problem, uygun idare anahtarlarının bilgisayar korsanları tarafından biliniyor olmasıydı. Eğer, anahtar güncellemelerini kodlamak için kullanılmış olan bu idare anahtarı bilinmiyor olsaydı, herhangi bir hack işleminin ömrü çok kısa olacaktı [1]. Bütün bunların merkezinde, bu sistemde bir kontrol işlemi yapma rutini kullanılmıştır.

FilmNet, TV1000 ve TV3 kanallarındaki anahtar güncellemeleri ara sıra görülmekteyken,

diğer kanallar daha aktif güncellemeler yapıldığı görülmekteydi. Örneğin Fransız Rendezvous kanalı, anahtarını her bir kaç günde bir güncellemekteydi [1].

FilmNet ve TV1000 kanalları için yeni bir anahtar güncelleme süresinin tasarlanması gerekliydi. Bu kanallar, aylık değişen anahtar programına geri döneceklerdi. Yeni anahtarlar, bir ayın son haftası ve diğer ayın ilk haftası boyunca havadaki yayından düzelticilere indirilebilecekti. Bu anahtar güncelleme programı türü, seksenli yılların ortalarına Amerika'da kullanılmış olan VideoCipher-II sisteminde kullanılan program ile benzerdir. Bu, FilmNet ve TV1000 kanallarının kullanmış olduğu programlardan daha radikal bir programdı. Fakat bu yaklaşımda bir kusur vardır. Eğer anahtarları güncellemek için kullanılmış olan idare anahtarları biliniyorsa, o zaman bilgisayar korsanlarının da kendi korsan kartlarını havadan gönderilen bu sinyallerle güncellemesi mümkündür. Bir veya iki haftalık anahtar güncelleme peryodu, ticari amaçlı bilgisayar korsanlarına problem yaratmak için yeterli değildi. Özellikle battery kartlarının, oldukça uzun olan bu güncelleme peryoduna bağışıklığı vardı.

EuroCrypt sisteminin kontrol işlemi rutinleri bilinmeksizin EuroCrypt Phoenix denemeleri çalıştırılamıyordu. Ticari amaçlı korsan akıllı kart uygulamalarının büyük bir kısmı bu kontrol işlemi rutinini içermekteydi. Buna karşılık, bazı paketleri hatalı kontrol işlemleri içeren elektronik karşı tedbir uygulanması çok kolaydı. Bu kontrol işlemi rutinlerine sahip olmayan korsan kartlar bu paketleri alacak ve böylece düzeltici düzgün bir biçimde kodu çözemeyecekti.

Ayrıca, EuroCrypt sistemindeki kontrol işlemi DES algoritmasını baz almaktadır. Bu, CA88 mesajının baytlarını almakta ve bunları, algoritmaya giriş olarak paketteki kontrol işlemine eşit olması gereken bir sonuç üretmek için kullanmaktaydı. Bu baytlar, 8 baytlık bir tampon ile EXOR'lanmaktadır. Daha sonra bu tampon işleme konmaktadır. Algoritmanın son uygulamasında, kalan baytlar ile tampon EXOR'lanmakta ve 8 bayt kalmamış olsa bile bu tampon işleme sokulmaktadır. Kontrol işlemi rutini için kullanılmış olan algoritma biraz değiştirilmiştir. Bu yüzden, S-Box seçiminin sonuçlarının sıralaması farklıdır. S1 ve S2'den gelen sonuçlar S5 ve S6'dan gelen sonuçlar ile değiş tokuş edilmektedir.

EuroCrypt Phoenix'in gerçekleştirilmesindeki kolaylık, paket yapılarındaki bilginin mevcut olması için hiç bir küçük parça olmamasından kaynaklanmaktadır. Ayrıca kartları aktif hale getirmek veya kapatmak ve anahtarların güncellenmesi de mümkündü.

5.10.3 Megatek kartının güncelleme kodlarının saptanması

Megatek, Cardtronix ve Benedex battery kartlarının ana prensibi, güvenli bir güncellemeye izin verilmesidir. Televizyon kanalının gerçekleştirmiş olduğu güncellemeyi saptamak telefon hattı veya internet üzerinden mümkündür. Bu kartların en gelişmiş modelleri, modem ile güncelleme özelliğine sahiptir. Fakat sistemin tamamı güvenli bir güncelleme metoduna güvenmektedir. Aksi taktirde, herkes bu güncellemeleri aynı anda elde edebilirdi. Ticari açıdan bakıldığında, bu hiçte iyi bir durum olmazdı. Megatek kartlarının güncelleme prosedürü, daha güvenli bir formatla değiştirilmiştir.

FilmNet ve TV1000 anahtarlarının 1995 yılındaki güncellenmesi, korsanları uğraştırmak için bazı materyaller içermekteydi. Dallas 5002FP tarafından adresleme ve veri için kullanılmış olan kodlama algoritmasının tamamını elde etmek için iki adet kodlanmış anahtar yeterli değildir. Fakat asıl hedef bu değildi. Megatek kartında kullanılmış olan algoritmada zayıflıklar vardı. Bu yüzden bu alboritmanın kırılması oldukça kolaydı [1].

Megatek kartları için güncellemeler, alfabetik bir formatta sağlanmıştır. Her bir blok üç harf genişliğindedir. Bunun bir sonucu olarak bu üç harf, sekizli (octal) bir kodu temsil etmektedir.

Çizelge 5.14 Megatek kartının güncellenmesinde harflere karşılık gelen rakamlar [1]

A = 0	E = 4
B = 1	F = 5
C = 2	G = 6
D = 3	H = 7

Bu üç harf blokları, şu şekilde kısımlara ayrılır;

$L_1 . (8^2) + L_2 . (8^1) + L_3 . (8^0)$

Bu yüzden, bu üç harf bloklu koddan onaltılı koda geçiş aşağıda verilenler gibi olmaktadır.

Çizelge 5.15 FilmNet kanalı güncellemesinde kodların onaltılı kodlara çevrilmesi [1]

Alfa-Sekizli kod	Sekizli kod	Onaltılı kod
BEG AGF ACD BCH	146 165 123 127	66 75 53 57
BEG DAC DCH DHG	146 302 327 376	66 C2 D7 FE
BEG BEF DEB CAA	146 145 341 200	66 65 E1 80
BEG AGG DDB CCD	146 066 331 223	66 36 D9 93
BEG AGD AEC BAE	146 063 042 104	66 33 22 44
BEG AAF DBG DDD	146 005 316 333	66 05 CE DB
BEG CBD DFG DAC	146 213 356 302	66 8B EE C2

Çizelge 5.16 TV1000 kanalı güncellemesinde kodların onaltılı kodlara çevrilmesi [1]

Alfa-Sekizli kod	Sekizli kod	Onaltılı kod
BEG BDD BGD CHF	146 133 163 275	66 5B 73 BD
BEG BGA ABC CFB	146 160 012 251	66 70 0A A9
BEG BCD DAF DCC	146 123 305 322	66 53 C5 D2
BEG BHC DGH CDH	146 172 367 237	66 7A F7 9F
BEG CAH CHF CFE	146 207 275 254	66 87 BD AC
BEG DHF CAB AFC	146 375 201 052	66 FD 81 2A
BEG ADH ADH DGE	146 037 037 364	66 1F 1F F4

Bu talimat, WRITE ADDRESS DATA biçiminde görünmektedir. Onaltılı koddaki 66h değeri, yazma talimatıdır (Çizelge 5.15 ve 5.16). Bunu takip eden iki bayt, kodlanmış formattaki adrestir ve son bayt ise anahtardır. FilmNet ve TV1000 kanalları için K_e kodlanmış anahtarlar Çizelge 5.17'de gösterilmiştir.

Çizelge 5.17 FilmNet ve TV1000 kanalları için kodlanmış anahtarlar [1]

FilmNet için K_e	TV1000 için K_e
57 FE 80 93 44 DB C2	BD A9 D2 9F AC 2A F4

Ayrıca, K_p yalın metin anahtarları (Çizelge 5.18) mevcut olduğu için bunları karşılaştırmak da mümkündür. Basit bir EXOR işlemi karakteristikleri göstermektedir (Çizelge 5.19).

Çizelge 5.18 FilmNet ve TV1000 kanalları için yalın metin anahtarları [1]

FilmNet için K_p	TV1000 için K_p
F2 58 27 33 E5 79 61	90 87 FD B7 85 00 DF

Çizelge 5.19 Kodlanmış metin ve yalın metin anahtarlarının karşılaştırılması [1]

FilmNet için K_e EXOR K_p		TV1000 için K_e EXOR K_p	
K_e	57 FE 80 93 44 DB C2	K_e	BD A9 D2 9F AC 2A F4
K_p	F2 58 27 33 E5 79 61	K_p	90 87 FD B7 85 00 DF
	A5 A6 A7 A0 A1 A2 A3		2D 2E 2F 28 29 2A 2B

Yalın metin anahtarı (K_p) ile şifreli metin anahtarı (K_e) EXOR'landığı zaman elde edilen dizi alışılmış olan bir dizi değildir. Yüksek nybble, değişmeyen bir değerdir. Fakat düşük nybble bir artmaktadır. Düşük nybble'ın dizisi bayt 03'te resetleniyor gibi görünmektedir. Aslında, yeni başlangıç değerini vermek için önceki düşük nybble değerinden 7 çıkarıldığı görülmektedir. Bunun nedeni, 0'dan F'e kadar olan sayıların ikilik düzende listelenmesiyle daha iyi anlaşılır (Çizelge 5.20).

Çizelge 5.20 Sayıların ikilik düzende karşılığı [1]

Sayı	İkilik karşılığı
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

İlk önce, kodlanmış anahtarların birinci ve ikinci baytlarının yüksek nybble'ları EXOR'lanması ile değişmeyen bir nybble'ın elde edilebilir gibi görünmekteydi. Bu, FilmNet çifti için mükemmel bir şekilde çalışmıştır. Fakat TV1000 çifti için başarılı olamamıştır.

FilmNet kanalı için: TV1000 kanalı için:

5 EXOR F = 2 B EXOR A = 1

Bunun muhtemel bir nedeni, EXOR'lanması gereken değerlerin her ikisininde dokuzdan büyük olmasıdır. Bu nedenle bu durumda, bu EXOR'lamanın sonucuna bir eklenmesi gereklidir.

Algoritmanın ana hatlarını şu şekilde sıralayabiliriz;

1) Yüksek nybble her zaman değişmeden kalacaktır ve düşük nybble ise diziseldir. Yüksek bitlerin beş tanesi her zaman değişmeden kaldığı için yüksek nybble'ların değişmediğini söylemek doğru olmayabilir. Değişmeyen veri, bunun sayacın veya yazmacın EXOR'lanmış bir formu olduğuna işaret etmektedir. Adaylardan bir tanesi adresleme yazmacıdır.

(sNh) = B1(Nh) EXOR B2(Nh) (If B1(Nh) and B2(Nh) greater than A, add 1)

2) Düşük nybble dizisi, bayt 03'te kesilmektedir. Bu nybble için yaratılmış olan yeni

başlangıç değeri, önceki nybble'ın değerinden yedi çıkarıldığı zaman elde edilen sonuca eşittir.

5.10.3.1 Megatek battery kartının güncelleme programı

Burada verilmiş olan MCATTACK.C isimli programın C kodu, bu konudaki edinilmiş olan fikirleri test etmek için kullanılmış olan deneysel bir koddur. Program uygulamasının başlangıç ve bitiş sürelerinin okunması için bir zamanlama döngüsü dahil edilmiştir. İlk başta, bu kodda bir hata olduğu düşünülmekteydi. Çünkü, program çalışmasına rağmen clock güncellenmemekteydi. Bunun anlamı, anahtarların hesaplanması için geçen sürenin bir bilgisayarın okuyamayacağı kadar hızlı olmasıdır. Bu yüzden Megatek, anahtar güncelleme metodunu değiştirmiştir. Ayrıca Cardtronics güncelleme metodu da farklıdır.

Dallas 5002FP, hack edilmesi çok zor olan mikroçiplerden biri olduğu için Megatek bu mikroçipi kullanmıştır. Fakat bütün bu güvenliğin yanısıra, anahtar güncellemesinin hack edilmesine izin veren küçük bir kusuru vardı.

Diğer battery kartlarının güncelleme prosedürü, bundan daha güvenli gibi görünmektedir. Bir kaynağa göre, bu kartlardan biri için güncelleme kodunu kodlamak için IDEA algoritması kullanılmış.

Fakat, battery kartlarının güncelleme prosedürü bilinen bir yalın metin saldırısı kullanılarak kırılabilmekteydi. Bu durum sadece D2-MAC EuroCrypt anahtarlarında mümkündür. Çünkü Megatek kartında anahtarlar, işlenmemiş formatlarında kullanılmıştı. Bu nedenle, güncelleme kodlamasının altında kodlamanın ikinci düzeyi yoktur. Eğer olsaydı, bu basit saldırı işe yaramayacaktı.

Sky 09 kartı için mevcut olan bütün elektronik karşı tedbir kodlarıyla birlikte bu yaklaşım, Dallas 5002FP mikroçipinin içindeki adres ve veri kodlamasına saldırmayı denemek için umut verici bir yaklaşım gibi görünmektedir. Bu hack işleminin hedefi sadece güncelleme anahtarlarını kırmaktır. Bu hack işleminin gerçekleşmesine yol açan elemanlar güncelleme kodu formatının düzenli bir yapıda olması, kodlama algoritmasının basitliği ve bazı yalın metinlerin mevcut olmasıdır.

```
#include <stdio.h>
#include <dos.h>
/* MCATTACK.C
This program crunches the encryption on the Megatek battery
card updates and generates 256 possible DES keys for any DES
update. The reduction from 2^56 to 2^4 means that all the
possible keys can be tested in 1ess than a second .
Change the values in the ekey and 1 key arrays to the 1ow
and high nybbles of the encrypted key bytes . This is an
experimental piece of code so it is not as elegant as it could be.

Last Rev: 19951020
FilmNet key:
plain text : F2 58 27 33 E5 79 61
cipher text : 57 FE 80 93 44 DB C2
TV1000 key:
plain text : 90 87 FD B7 85 00 DF
cipher text: BD A9 D2 9F AC 2A F4
*/
/*
unsigned char ekey[7]={ 0xb, 0xa, 0xd, 0x9, 0xa, 0x2, 0xf };
unsigned char lkey[7]={ 0xd, 0x9, 0x2, 0xf, 0xc, 0xa, 0x4 };
unsigned char ekey[7]={ 0x3, 0xc, 0x6, 0x3, 0x3, 0x0, 0x8 };
unsigned char lkey[7]={ 0x5, 0x2, 0x5, 0x6, 0x3, 0x5, 0xb };
*/
unsigned char ekey[7]={ 0x5, 0xf, 0x8, 0x9, 0x4, 0xd, 0xc };
unsigned char lkey[7]={ 0x7, 0xe, 0x0, 0x3, 0x4, 0xb, 0x2 };
/*
filmnet col2
unsigned char ekey[7]={ 0x7, 0xc, 0x6, 0x3, 0x3, 0x0, 0x8 };
unsigned char lkey[7]={ 0x5, 0x2, 0x5, 0x6, 0x3, 0xS, 0xb };
```

```
unsigned char ekey[7]={ 0x5, 0x7, 0x5, 0x7, 0x8, 0xf, 0xl };
unsigned char lkey[7]={ 0xb, 0x0, 0x3, 0xa, 0x7, 0xd, 0xf };
*/
unsigned char l,b,c,e,h,ok,q,r,s,t,u,v,w,x,y,z;
/* The global array fill option is used to fill the arrays
*/
unsigned char dkey[7]={0};
unsigned char Harray[16][7]={0};
unsigned char Larray[16][7]={0};
unsigned char Parr0[16][7]={0};
unsigned char Parrl[16][7]={0};
void main(void)
{ /* This is the timing routine that was irrelevant
struct time t;
gettime(&t);
printf("The start time is: %2d:%02d:%02d.%02d\n",
t.ti_hour, t.ti_min, t.ti_sec, t.ti_hund);
*/
/* Fill High Array */
for (c=0; c<=0xf; c++)
{ for (e=0; e<=6; e++)
{ ok=0 ;
ok=c ^ ekey[e] ;
ok=ok<4;
Harray[c][e]=ok;
};
};
/* This section here could be done using a for loop but since
checking the result at each stage was important I used a */
more basic approach. */
for (c=0; c<=0xf; c++){
```

```
x=c;
1=x^lkey[0]; Larray[c][0]=1;
x=x+l;tf (x>0xf) x=x-0xf; .
1=x^lkey[1]; Larray[c][1]=1;
x=x+l; if (x>0xf) x=x-0xf;
1=x^lkey[2]; Larray[c][2]=1;
x=x-7; x&=0x0f; if (x>0xf) x=x+0xf;
1=x^lkey[3]; Larray[c][3]=1;
x=x+l; if (x>0xf) x=x-0xf;
1=x^lkey[4]; Larray[c][4]=1;
x=x+l; if (x>0xf) x=x-0xf;
1= x^lkey[5]; Larray[c] [5]=1 ;
x=x+1; if (x>0xf) x=x-0xf;
1= x^lkey[6]; Larray[c][6]=1;
};
{ printf("High Array Low Array\n");
for (x=0; x<=0xf; x++){printf("\n");
for (y=0; y<7; y++){printf ("%X ",
Harray[x][y]>4);};
printf(" ");
for (z=0; z<7; z++){printf ("%X", Larray[x][z]);};
};
};
for (x=0; x<=0xf ; x++) {
for (y=0; y<7; y++) {
Parr0[x][y]=Harray[x][y]
Larray[5][y];
Parrl[x][y]=Harray[x][y]
Larray[0xd][y];
};
}
```

```
printf("\n*****************************************\n");
printf(" (0x5 Group) Possible Key Arrays (0xd Group)") ;
printf("\n-------------------------------------------------------\n");
printf("Encrypted Key: ") ;
for (x=0;x<7;x++){dkey[x]=(ekey[x]<4)|lkey[x];
printf("%2.2X ", dkey[x]);};
h=((ekey[0]<4)^(ekey[1]<4))>4;
if(ekey[0]>ekey[1]) h=h+1;
printf("\n Potential keys on row %2.2x", h) ;
printf("\n*****************************************\n):
/* for (x=0; x<=0xf; x++){ printf("%2.2x | ", x); */
x=h;{
for (y=0; y<7; y++){
printf("%2.2X ",Parr0[x][y]);
};
printf(" ") ;
for (z=0; z<7; z++){
printf("%2.2X ", Parrl[x] [z]);
};
printf ("\n") ;
};
}; /*Now Wasn't That fun :-)*/
```

6. VİDEO KARIŞTIRICI SİSTEMLER

Video işleyici bir sistem, videoyu dijitalleştiren ve karıştıran bir sistemdir [1]. Anahtar sözcük dijitalleştirmektir. Teorik olarak, dijital bir sistem çok güvenlidir. Fakat uygulamada, sistemin diğer bölgelerindeki kusurlardan dolayı bu sistem de hack edilebilmektedir. Dijital sistemlerin kullanılmasıyla korsanlığın sona ereceğinin düşünülmesi yanlış olur. Bu bölümde incelenmiş olan hack işlemlerinin tamamı bir zamanlar korsanlığa karşı güvenli olduğu düşünülen sistemlerde gerçekleştirilmiştir. Çünkü şu ana kadar değerli televizyon programlarını koruyan hiçbir sistem uzun bir süre güvenli olarak kalamamıştır.

Bu bölümde anlatılmış olan sistemlerin büyük bir kısmının, geçiş sistemleri olarak adlandırılması daha doğru olur. Çünkü bu sistemler, değişmez bir şekilde analog televizyon standartlarını baz almıştır ve dijital kodlama metotlarını sadece güvenliklerini sağlamak için kullanmıştır. Kodlama metodlarının büyük bir kısmı veri akışını korumayı amaçlamaktadır. Çünkü bu veri akışı, yetki verilmiş bir kart veya düzeltici tarafından videonun kodunun çözülmesini sağlamaktadır. Bu geçiş sistemlerinin erişim kontrol bölgelerinin tamamen dijital ve sıkı kodlama kullanıyor olmasına rağmen video, sadece dijital teknikler kullanılarak karıştırılmıştır.

Kodlama ve karıştırma arasındaki fark çok incedir. Video karıştırıcı, tam anlamıyla kodlama sayılmaz. Çünkü videonun değerinden sonra gelmez. Bu, sadece zaman domeninde videonun sırasını değiştirmektedir. Bu tip bir karıştırıcı (kes ve yer değiştir veya satır karıştırma tipi) en basit şekilde, bir mesajdaki harflerin yerlerini değiştiren bir yer değiştirici şifre olarak düşünülebilir. Bu yer değiştirici şifre, harflerin gerçek değerlerini değiştirmeden sadece yerlerini değiştirir.

Fakat video işleyici bir sistem, yer değiştirici bir şifre olarak düşünmek çok aşırı bir basitleştirmedir. Çünkü bu yer değiştirmeyi sağlamak için birçok elektronik devre yapısı kullanmaktadır. Ayrıca bu yüzden, bu sistemler temelde senkronizasyon darbelerini kullanmayı baz alan sistemlerden daha zor hack edilmektedir.

Çoklanmış Analog Bileşen (MAC) sistemi ile bunun varyantları, bu geçiş sistemleri ile gerçek dijital televizyon sistemleri arasında bir yerde bulunur. Bu sistem de videonun yerini değiştirmek için dijital karıştırıcı teknikler kullanmaktadır. Ayrıca bu sistemde, video paketleri sıkıştırılmaktadır ve de dijital ses (audio) kullanılmaktadır.

Fakat DirecTv sistemi, yukarıda bahsedilen sistemlerden hariç tutulmalıdır. Çünkü bu sistem, gerçek bir dijital televizyon sistemidir. Bu sistemde, MPEG 1.5 standardı ve veriyi kodlamak

ve kodlanmış olan bu veriyi iletmek için dijital teknikler kullanılmaktadır. Bu sistem, hack edilmiş olan ilk gerçek dijital televizyon sistemidir. DirecTv sisteminin hack edilmesinin sebebi, Avrupa'da News Datacom kanalında kullanılmış olan bilgi satırlarının aynılarının burada da kullanılmış olmasıdır.

09 Sky kartı, VideoCrypt-II kartı ve DirecTv kartı için kullanılmış olan orijinal akıllı kart aynıydı. Sadece EEPROM'larındaki program biraz farklıydı. Bu yüzden, 09 Sky kartının nasıl hack edildiğini bilen bilgisayar korsanları diğer sistemleri de hack etmek için aynı bilgiyi kullanabilmekteydi. Bu durum, bu sistemlerin hepsinin kullanmış olduğu ortak bir elemanın hack edilmesi durumudur. Bu da, Avrupa'da tek bir karıştırıcı sisteme veya standarda geçilmesinin hiçte akıllıca olmayacağını kanıtlamaktadır.

Avrupa'da kullanılmakta olan sistemlerin tamamı hack edilmiştir. Bu hack işlemlerinin büyük bir kısmı sistemin erişim kontrol bölümünde gerçekleştirilmiştir. Fakat Nagra sistemindeki hack işlemi video karıştırıcıya saldırmayı baz almaktaydı. Bilgisayar korsanları için Nagra sistemindeki problem, korsan bir akıllı kart yapılıp kullanılabilmesi için piyasada yeterli sayıda kod çözücünün bulunmamasıydı. Bu yüzden, uygulanabilecek tek alternatif sistemin video karıştırıcı yaklaşımını hack edecek korsan bir kod çözücü yapmaktı. Bu alternatif hack işleminin, teknik ve ekonomik sebepler yüzünden gerçekleştirilmesi birkaç yıl önce mümkün değildi.

Video işleyici sistemlerin artmasındaki temel unsur, video analog-dijital konverterlerinin ve video dijital-analog konverterlerinin maliyetinin düşük olmasıdır. Bu durum, B-MAC gibi bazı eski video işleyici sistemler için problemler yaratmıştır. Çünkü ekonomik açıdan makul olan bir korsan kod çözücünün yapılması mümkün hale gelmiştir. Bu hack işleminin başarılı olmasını sağlayan zayıf nokta dalga biçimindeki standart geçiş süresiydi.

Bir erişim kontrol sistemi planının tamamı sadece akıllı kartları baz almaktadır. VideoCrypt, EuroCrypt ve DirecTv akıllı kart bazlı sistemlerde hack işlemi gerçekleştikten sonra akıllı kartların korsanlığı önleyeceği düşüncesinin ne kadar yanlış olduğu anlaşılmıştır.

Bu hack işlemleri gerçekleştiği zaman erişim kontrol hizmeti sağlayan şirketler bu tehlikeden haberdar oldu. Bu şirketlerin büyük bir kısmı bankalar ile çalışmaktaydı. Bankacılıkta, bir sistemin hack edilmesi kabul edilebilecek bir durum değildir. Bu düşünce, erişim kontrol hizmeti veren bu şirketler için de geçerlidir. Bu hack işlemlerinin, bu sistemleri kullanan televizyon kanalları üzerindeki etkisi yıkıcı olmuştur ve bazı durumlarda yetersizliklerini haklı göstermek için erişim kontrol hizmeti veren bu şirketlere dava açılmıştı.

Ayrıca Amerika'da, DirecTv sistemi de bilgisayar korsanları tarafından hedef alınmıştır. Çünkü bu sistemin kullanmış olduğu kart, Avrupa'da VideoCrypt sisteminde kullanılmış olan kartın biraz geliştirilmiş modeliydi [1]. Fakat, DirecTv sistemindeki hack etme yolları VideoCrypt sistemindekilerden biraz faklıydı.

Amerika ve Kanada'daki korsan battery kartı kullanıcılarına ve satıcılarına televizyon kanallarının bu saldırısı, korsanlık problemini düzeltmekten çok uzaktı. Bu durum, akıllı kart baz alan sistemlerdeki yeni nesil hack işlemlerini daha çok hızlandırdı. Bu yeni nesil hack işlemleri, son kullanıcının bu kartları çoğaltarak dağıtmasını engellemek için güvenlik elemanlarıyla modifiye edilmiş olan SEASON tipi hack işlemiydi.

6.1 VideoCrypt-I Sistemi

VideoCrypt sistemi, düşük maliyetli güvenli bir karıştırıcı sistem olduğu için iyi bir tasarımdır. Bu sistem, bilgisayar korsanları için sabit bir hedef yerine hareketli bir hedef olan akıllı kartı baz almaktadır. Teorik olarak bu akıllı kart hack edildikten sonra yenisi ile değiştirilebilmektedir.

Fakat bu teori pratikte gerçekleştirilememiştir. 1993 yılı Nisan ayında Sky kanalının akıllı kartı tamamen tehlike altındaydı. Fakat Sky kanalı bu akıllı kartı ekonomik sebeplerden dolayı ancak 18.05.1994 tarihinde yenisiyle değiştirilebilmiştir.

1994 yılı Haziran ayında 09 Sky kartının korsan bir versiyonunun kodu açık arttırmayla satışa sunulmuştur. Bununla birlikte, Ekim ayında ilk kararlı 09 korsan kartı korsan piyasaya çıkmıştır. Bundan sonra orijinal Sky 09 kartının satışları inişe geçmiştir. Bu korsan 09 kartı, 31.10.1995 tarihinde Sky kanalı yeni kartı olan 10 serisi akıllı karta geçinceye kadar kullanımda kalmıştır [1].

Fakat bu yeni Sky 10 kartı da korsanlar tarafından hack edilmiştir. Bu durum, korsanlık teknolojisinin Sky kanalı üzerindeki zaferini göstermektedir. Ho Lee Fook hack işleminden sonra VideoCrypt akıllı kart sisteminin tamamen tehlikede olduğu ortaya çıkmıştır. News Datacom ve Sky kanallarının akıllı kart kullanmaya karar vermeleri onlara pahalıya patlamıştır. Çünkü bilgisayar korsanlarına karşı almış oldukları elektronik karşı tedbirler şaşırtıcı bir hızla yenilgiye uğratılmıştır. Bundan sonra bu kanallar, son çare olarak bilgisayar korsanlarını yasal yollarla engellemeyi denemişlerdir.

VideoCrypt sistemi, seksenli yılların ortasında geliştirilmiş olduğu için artık çok eski bir sistemdir. Bu sistem ilk defa kullanılmaya başlandığı zaman, bu sistemin korsanlığa karşı en

güvenli sistem olduğu iddia edilmekteydi. VideoCrypt sistemi, ayrılabilir güvenli mikrokontrolör prensibini baz almaktadır. Kod çözücünün kendisi sadece akılsız bir terminaldir. Ayrılabilir güvenli mikrokontrolör ise bir akıllı karttır. Teorik olarak bu akıllı kart kritik veriyi, kod çözücü ise önemli olmayan bilgileri içermektedir.

Kod çözücü sadece bir 6806 maskelenmiş ROM ve bir 8052 maskelenmiş ROM içermektedir. Bu her iki mikroçipin içindeki bilgiler korsanlar tarafından tamamen okunmuştur. Çünkü 8052 mikroçipi gerçekten korumasızdı. 8052 idareyi sağlayan mikroçiptir. 6805 mikroçipi ise havadan kod çözücüye gönderilmeyen veri işleme rutinlerini içermektedir.

Bu sistemde kullanılmış olan algoritmaların yaratıcısı, önemli bir matematikçi olan Profesör Adi Shamir'dir [1]. News Datacom'un teknik destek materyallerinde akıllı kartların her birkaç saniyede bir kartın doğruluğunu nasıl kontrol ettiğine dair anlatımlar vardı. Bu kartın doğruluğunu ispatlama prosedürü yenilmez olduğu için bu sistemde korsan bir akıllı kart kullanılmasının hiç bir yolu olmadığı iddia edilmekteydi.

Fiat-Shamir Sıfır Bilgi Testi, kartın doğruluğunu ispatlama prosedürüdür ve uygun bir biçimde kullanıldığı zaman hack edilmesi hemen hemen imkansızdır.

1990 yılında News Datacom, VideoCrypt sistemine patent almak için başvuruda bulunulmuştur [1]. Bu başvuru, Hong Kong'taki News Data Security Products Ltd. tarafından tasnif edildi. Tasarımcılar, İsrailli Michael Cohen ve Jonathan Hashkes'ti. VideoCrypt sistemi tasarımının özeti, yayın iletimine erişimi kontrol etmek için geliştirilmiş aparatlar ve teknikler sağlanmasıydı. Ayrıca, tercihen bir Fiat-Shamir genel anahtar ispatı olan bir genel anahtar ispatı prosedürü de içermektedir. Bu, akıllı kartın doğruluğunu kod çözücüye ispatlaması için kullanılmıştır.

Bu patent başvurusu, sistem mimarisi hakkında çok ayrıntılı bilgi vermiştir. Sistem gerçekleştirilirken çok küçük değişiklikler yapılmıştır. Bu patent, son birkaç yıl içersinde çeşitli kaynaklardan elde edilen bilgilerin büyük bir kısmının doğru olduğunu kanıtlamıştır. Ayrıca, sistemde kullanılmış olan programların bazılarının nesne kodunda örnekleri de mevcuttur.

Patent başvurusundaki bilgiler eski olmasına rağmen VideoCrypt sistemindeki erişim kontrol yapısı hakkında bir fikir vermektedir. Bu, EuroCrypt gibi modern bir sistemden çok daha düşük bütçeli bir sistemdi. Günümüzde daha fazla önem verilen husus, herşeyi içeren bir sistemden ziyade düşük maliyetle gerçekleştirilebilecek bir çözüm üretmektir.

Kod çözücü, sadece bir terminaldir ve herhangi bir anahtar içermemektedir. Ayrıca, her bir kullanıcıya kişisel mesajlar göndermek için bir posta kutusu özelliği de mevcuttur. Bu bakımdan, oldukça güzel bir mesaj gönderme sistemine sahip olan eski BSB EuroCypher sistemine benzemektedir.

6.1.1 VideoCrypt abone yönetim sistemi

VideoCrypt abone yönetim sistemi hakkında elde edilmiş olan bilgilerin büyük bir kısmı patent dökümanlarından sağlanmıştır. Abone yönetim sistemi yapısının en önemli kısımları uygulamada değiştirilmemiştir. Adresleme, patent bilgilerinde belirtildiği gibi 32 baytlık 74h paketleri aracılığıyla yapılmaktaydı.

News Datacom'un teknik dökümanlarındaki resimlere göre birçok terminal, müşteri hizmetleri bilgisayarına bağlıdır. Bu durum, merkezi işlem birimi temelli büyük bir ağın olduğunu göstermektedir. Müşteri hizmetleri için kullanılmış olan bilgisayarların markası bilimemektedir. Fakat bu yapının büyük bir bölümünün markasının IBM olduğu belirtilmiştir. Merkezi işlem birimi de büyük bir ihtimalle IBM'di.

Görünüşe göre abone yönetim sistemi İskoçya, Livingstone'da kurulmuştu [1]. Bunlar, abone numaraları ve abone olunan kanal bilgileri gibi müşteri detaylarını içeren bir grup manyetik şeritli kartuşu hazırlayarak, daha sonra bunları İngiltere Maidenhead'deki News Datacom tesislerine yollamaktaydı. Daha sonra Maidenhead tesislerinde abone akıllı kartları hazırlanarak abonelere gönderilmekteydi.

Patente göre, abone yönetim sisteminin yapısı özel bilgisayarları baz almaktaydı. Bu elemanların yapısını, farklı bilgisayarlardan ziyade bilgisayar programları olarak sınıflandırmak daha doğru olur. Bunlar tabiki bir ağa bağlıydı. Herbir kanal, kendi farklı ana kartını gerektirmekteydi. Aksi taktirde anahtar, 8052 gerçekleyicisinden (verifier) elde edilebilmektedir.

8052 gerçekleyicisinden anahtarın üretimi, serbest erişim modu için anahtar üretmenin en mantıklı metodudur. 8052'lerin herbirinde 256 baytlık büyük bir tablo mevcuttur. Bu, Fiat-Shamir Sıfır Bilgi Testi'nde kullanılan genel modüller için veri olarak kullanılabilmektedir. Ayrıca bu, kod çözme anahtarı üretimi için kod tablosu olarak da kullanılabilmektedir.

6.1.1.1 Güvenlik bilgisayarı

Patente göre bu bilgisayar, birçok seri porta sahip olan bir IBM AT'dir. Buna benzer bir

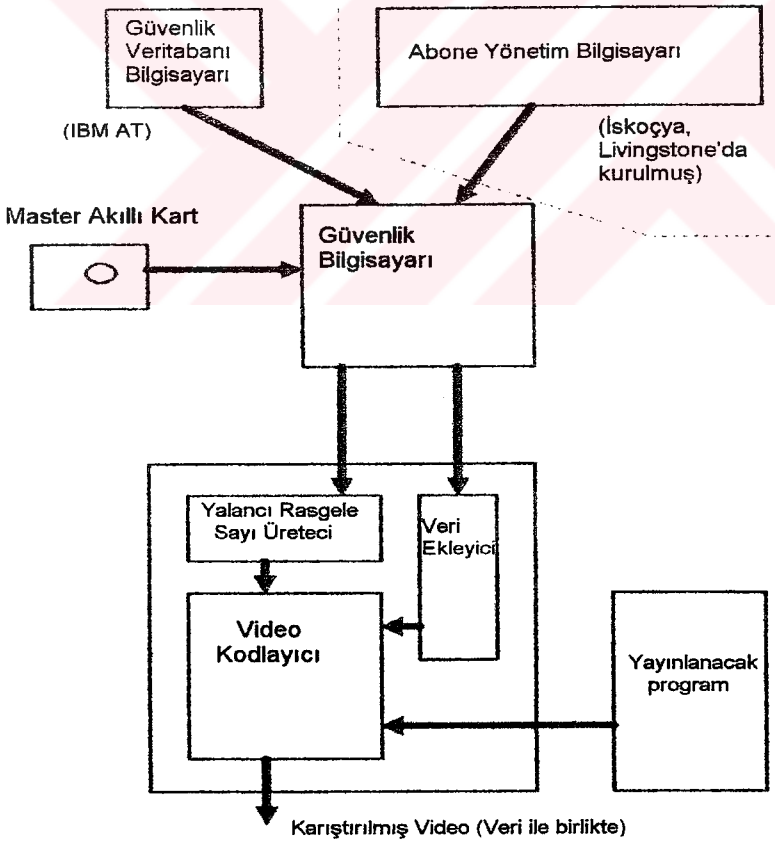
konfigürasyon, birçok seri porta sahip olan bir 486 veya üstüdür.

Güvenlik bilgisayarının görevi, ağdaki diğer bilgisayarlar için bir hub gibi davranmaktır. Bu bilgisayarın, Güvenlik Veritabanı Bilgisayarından, Abone Yönetim Sisteminden ve ana (master) akıllı karttan gelen bilgileri birleştirmesi gereklidir. Güvenlik Bilgisayarından gelen bilgi VideoCrypt yayın kodlayıcısına geçmektedir.

Patentte, bir kanal için gerçekleştirilmiş olan bir uygulama verilmiştir. Aynı anda çalışan birkaç kanal olması durumunda herbir kanal için farklı bir Güvenlik Bilgisayarı gerekmektedir.

6.1.1.2 Abone yönetim sistemi

Bu bilgisayar hizmetleri, müşteri hizmetleri bilgisayarına bağlanmıştır ve aktif hale getirilmesi ve kapatılması gereken akıllı kartların listesini üretmektedir. Patente göre abone yönetim bilgisayar sistemi, bir merkezi işlem birimini baz alabilmektedir. Sistemin geri kalanı IBM olduğu için buradaki en mantıklı seçim bir IBM merkezi işlem birimidir.



Şekil 6.1 VideoCrypt abone yönetim sisteminin blok diyagramı [1]

Abone yönetim sistemi İskoçya, Livingstone'da bulunmaktaydı. Fakat merkez yayın stüdyosu Londra civarındaydı. Bu iki nokta arasında, muhtemelen ISDN olan özel bir hat sistemi bulunmaktaydı.

Master akıllı kart, karıştırıcı için çekirdekleri üretmek için kullanılmaktadır. Ayrıca, 8052 gerçekleyici mikroçipi de kullanılabilmektedir. Bu, ödemeli televizyon kanallarının kodunu kart olmaksızın çözen sahte düzelticilerin bildirilmesi için önemlidir.

6.1.1.3 Güvenlik veritabanı bilgisayarı

Güvenlik Veritabanı Bilgisayarı, yayınlanan programlar ve görüntü başına ödeme hakkındaki işletme bilgilerini Güvenlik Bilgisayarına vermektedir. Bu işletme bilgisi kimlik bilgisi, izlenme payı ve süreklilik, yayınlanacak olan programların gruplanması ile ilgilidir.

6.1.2 VideoCrypt video karıştırıcı tekniği

VideoCrypt sisteminde kullanılmış olan karıştırıcı tekniği, satırı kesme ve yer değiştirmedir. Video dijitalleştirilir ve daha sonra olası 256 noktanın birinde kesilmektedir. Daha sonra, bu nokta etrafında dijitalleştirilmiş olan video parçalarının yerleri değiştirilir ve dijital video analog hale çevrilmektedir.

Kesme noktasının 256 noktadan biri olması, bunun 8 bitlik bir sözcükle tanımlanabilir olduğu anlamına gelmektedir. Bu bayt (8 bit), bir Yalancı Rasgele Sayı Üreteci tarafından sağlanmaktadır. Bu Yalancı Rasgele Sayı Üreteci, 60 kademe uzunluğundadır ve yaklaşık olarak her 2.5 saniye sonunda resetlenmektedir.

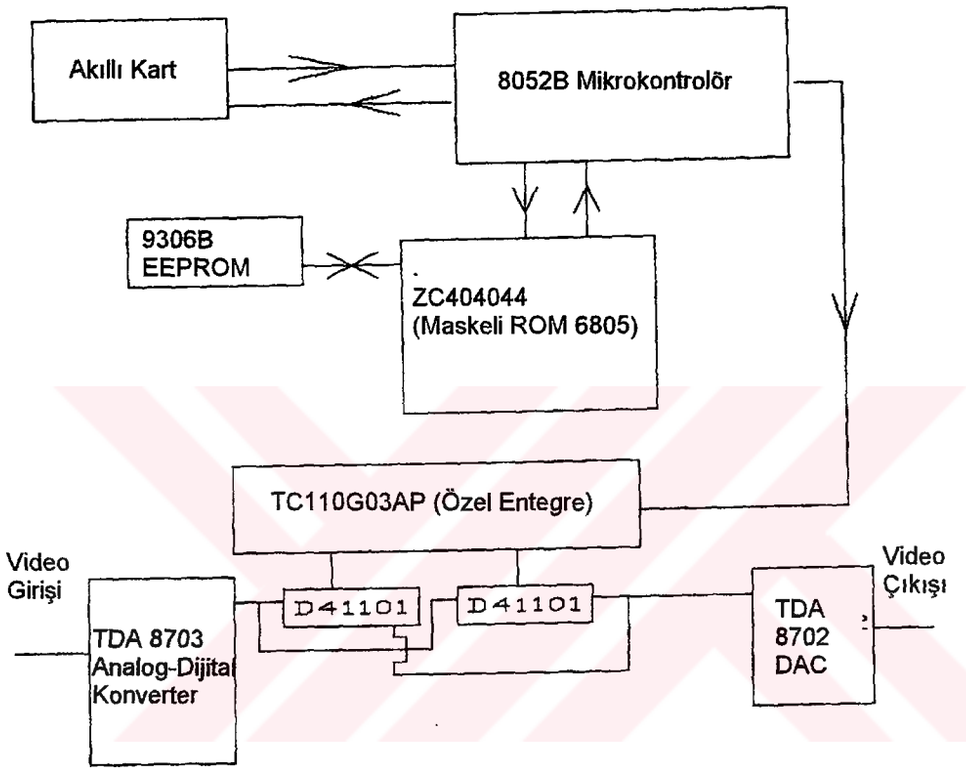
VideoCrypt sisteminde, düşey karartma aralığının birkaç satırında erişim kontrol verisi iletilmektedir. Bu veri hızı teleteksttekinden daha yavaştır. Verinin paketlerinin herbiri bir kontrol işlemine sahiptir. Bu kontrol işlemi, paketlerdeki aktif verinin bir ürünüdür.

Herbir görüntüde, sadece 585 satır karıştırılmıştır. Bu durum, düşey karartma aralığı sinyallerinin videonun kodu çözülmeksizin kontrol edilebilmesine imkan tanır. Bunun sebebi SMATV ve kablolu sistemlerde sinyal kalitesinin, sinyalin kodunun çözülmesine gerek kalmaksızın kontrol edilebiliyor olmasıdır. Bu, karıştırıcı sistemlerin büyük bir kısmında standart bir özelliktir.

6.1.3 VideoCrypt düzelticisinin yapısı

VideoCrypt bağımsız (stand alone) kod çözücü, hibrit bir tasarımdır. Bu kod çözücü, ayrık

(diskrit) bileşenler ve yüzeye monte edilebilen bileşenlerin her ikisinide kullanmaktadır. Bu, devre kartının boyutlarını küçültmek için gereklidir. İlk kod çözücü tasarımında kullanılmış olan devre kartı tipi, senetik reçine yapıştırılmış kağıttır. Bu, devre kartı malzemelerinin en güveniliri değildir. Fakat, en ucuzlarından biridir. Fakat bu durum, televizyon imalat endüstrisinin televizyon alıcılarında kullandıkları devre kartlarının bu tipte olduğunu göstermez.



Şekil 6.2 VideoCrypt düzeltici yapısının blok diyagramı [1]

VideoCrypt'in IRD versiyonunda güç kaynağı, başlıca alıcı olan PSU'nun bir parçasıdır. Kod çözücüde, +21V, +12.5V, +15V ve +5V olmak üzere dört voltaj hattı mevcuttur. Devre yapısının ana kısmı +5V hattından beslenmektedir.

Piyasada on adet değişik VideoCrypt IRD tasarımı olduğu tahmin edilmektedir. Herbir tasarımdaki çalışma şekli büyük ölçüde aynı olmasına rağmen kendine özgü alıcı tasarımları kullanılarak çalışmaları sağlanmıştır. VideoCrypt kod çözücüsünün devre diyagramları, fotokopisi çekilemeyen kağıt üzerinde olmak üzere yetkili servislere dağıtılmıştır.

6.1.3.1 İdareyi sağlayan mikrokontrolör

Düzelticideki en önemli işlemci Intel 8052 mikrokontrolörüdür. Bu mikrokontrolör, mikroçip üzerinde bir ROM'a ve bir RAM'e sahiptir. Bu mikrokontrolörün, temel ROM versiyonu ve maskeli programlanabilir versiyonu olmak üzere iki tipi mevcuttur. Düzeltici tasarımında kullanılmış olan maskeli programlanabilir versiyonudur. Bu, düzelticiyi çalıştıran 8 kb'lık bir program olduğu anlamına gelmektedir. 8052, bu kontrol programını vermesi için zorlanabilmektedir. Fakat, Sky kod çözücülerini inceleyen birçok tecrübeli bilgisayar korsanı 8052'nin kontrol programını vermesi için zorlanmasının hiçte kolay olmayacağını düşünmekteydi.

Bu mikroçipteki ROM'un neden korumasız olduğunu gösteren birkaç teori mevcuttur. Bunlardan en belirgin olanı, mikroçipin hata yaptığı hız ile ilgilidir. Bu mikroçip, kart arabirimini yönettiği için bilgisayar korsanlarının üzerinde çalışması gereken bir noktadır. Bunun sonucunda, bu mikroçip en yaygın olarak hack edilenlerden biridir.

Hack edilmesi mümkün olmayan bir sistem tasarımında ROM'un korunmuş olması şarttır. Bu yüzden VideoCrypt sistemi, hack edilemez bir sistem olmaktan çok uzaktır. VideoCrypt-II kod çözücülerinde ROM korunmuş olmasına rağmen bu pek işe yaramamıştı. Çünkü, ROM'un içindeki bilgi çok kolay çıkarılmış ve incelenmişti.

8052 içindeki programın okunabilir ve incelenebilir olduğu gerçeği, güvenli işkemci arabiriminin bulunduğu kartın tamamı izlenebilir olduğu ve gerekli olan yerlerde bu verinin modifiye edilebilir olduğu anlamına gelmektedir. Bu gerçek, VideoCrypt sistemindeki en yıkıcı hack işlemlerinden biri olan KENtucky Fried Chip hack'inin gerçekleşmesine yol açmıştır.

VideoCrypt patent başvurusundaki bilgilerin büyük bir kısmı VideoCrypt-I sisteminde de tekrarlanmıştır. Bu sistemde de, 8052 ve 256 baytlık veri tablosu mevcuttu. Uygulamalar arasında çok küçük farklılıklar olduğu için bu sistemler görünüşe göre büyük ölçüde aynıydı.

Bu sistemdeki diğer yaklaşımlar da belirgin hale geldi. Kod çözücü, akıllı kartların ve bellek kartlarının her ikisini de kullanabilmekteydi. Kod çözücü, bellek kartlarını kullandığı zaman çekirdeği üretmek için dahili bir algoritma kullanmaktaydı. Yani, gerçek kod çözücüde bir kod çözme algoritmasının mevcut olması gerekliydi.

8052'deki bir özellik, günümüzdeki Sky kanallarında kullanılmamaktadır. Bu, VideoCrypt sisteminin güvenliğinin önemli bir parçası Fiat-Shamir Sıfır Bilgi Testi'dir. Patent

başvurusunda bu testin, akıllı kartların korsan bir şekilde klonlanmasını durduracağı iddia edilmekteydi. Gerçekten de eğer Fiat-Shamir Sıfır Bilgi Testi kullanılmış olsaydı, o zaman 07 Sky kartlarındaki korsanlık gerçekleşemeyecekti. Korsan kartların hepsi, videoyu düzeltmek için algoritmayı ve kod tablosunu içermekteydi.

Adult Channel halen VideoCrypt sisteminin çok eski bir versiyonunu kullanmaktadır ve peryodik olarak Fiat-Shamir Sıfır Bilgi Testini uygulamaktadır. Fakat korsan kartlar bu testi başarıyla geçmektedir. Bu durum, bu uygulamada birşeylerin yanlış olduğunu işaret etmektedir.

Akıllı kart resetlendikten kısa bir süre sonra kimlik numarasını kod çözücüye gönderir. Korsan akıllı kartların hepsi sıfırlardan oluşan bir diziyi kod çözücüye göndermektedir. Bu kartların kimlik numaraları 00 00 00 00 00 00 şeklindedir. Kod çözücü, bu kimlik numarasını reddetmemektedir ve muhtemelen hiçbir VideoCrypt kod çözücüsü bu kimlik numarasını reddetmeyecektir. En belirgin olan bu hack etme işlemi Sky tarafından görmezden gelinmiştir. Kod çözücü, akıllı kartın kimlik numarasının doğru olup olmadığını kontrol etmemekteydi. Bu yüzden bilgisayar korsanları sahte kimlik numaraları ile kod çözücüyü çalıştırmayı denediler. En azından kod çözücülerin bu sahte kimlik numaralarını reddediyor olması gerekirdi.

Adult Channel'da akıllı kart tarafından iletilmiş olan Fiat-Shamir paketlerinin herbiri 64 baytlık sıfırlardan oluşmaktadır. Bu işlemde kullanılmış olan sayılardan bir tanesi sıfır olduğu için kod çözücü tarafından bu cevap gerçekten doğru olarak kabul edilmekte ve sahte olduğu açıkça görünen böyle bir cevaba izin verilmekteydi.

Fiat-Shamir Sıfır Bilgi Testi, taklit edilmesi aslında çok zor olan bir algoritmaydı. Gerçekten uygun biçimde uygulanmış olsaydı, VideoCrypt sistemini hack edilmesi zor bir sistem yapardı. Kod çözücünün, problemlerin bulunduğu test noktalarını yürütmek için bazı rutinlere sahip olması gereklidir.

8052 mikrokontrolörü korumasızdır. Bu yüzden, 8052'nin içindeki program çıkarılmıştır ve bu programı gerçek zamanlı çalıştırarak denemeler yapmak için devre emülatörleri kullanılmıştır.

Fiat-Shamir Sıfır Bilgi Testi ile ilgili olan rutinler çok çabuk kurulabilmekteydi. Bunun sonuçları, programda bir bayrağı ayarlamaktadır. Eğer bilgisayar korsanları, benzer bir gecikme sağlanmış bir dizi döngü ile Fiat-Shamir Sıfır Bilgi Testini değiştirerek 8052 programını yeniden yazarsa, Fiat-Shamir Sıfır Bilgi Testinin amacını gerçekleştirmesi

engellenmiş olmaktadır. Bilgisayar korsanları için 8052 programının yeniden yazılması yeni bir durum değildi. KENtucky Fried Chip hack işleminin ve Ho Lee Fook hack işleminin ilk versiyonları bunu kanıtlamamıştır.

VideoCrypt-I kod çözücüsü tasarımındaki sorun çıkaran hatalardan bazıları VideoCrypt-II kod çözücüsü tasarımında düzeltilmiştir. Sistemin güvenliğinin geliştirildiği iddia edilmekteydi. Fakat bu kod çözücüdeki 8052 ve 6805 mikroçiplerinin içindeki bilgi de okunmuş ve programları analiz edilmişti.

Çizelge 6.1 Fiat-Shamir sıfır bilgi testinin çalışma şekli [1]

Komut	Akıllı Kart Cevabı
RESET	3F FA 11 25 05 00 01 B0 02 3B 36 4D 59 02 81 80
DCDR 72	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
CARD 70	00 00 00 00 00 00
CARD 7A	D8 53 45 41 53 4F 4E 37 20 56 31 43 33 20 20 20 30 30 3A 34 38 20 20 20 20
CARD 7C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DCDR 74	E8 42 3A 20 4B 1E 01 FB 7E 86 78 AA AB AD AE B2 B5 B9 BB BC 00 00 00 00 00 00 00 DD FF 9E 0C CE
CARD 78	D3 5B 02 60 B9 65 6B 0D
CARD 7A	80 53 45 41 53 4F 4E 37 20 56 31 43 33 41 44 55 4C 54 43 48 41 4E 4E 45 4C
CARD 7C	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
CARD 7E	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
DCDR 80	01
CARD 82	00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
CARD 70	00 00 00 00 00 00
DCDR 74	E0 42 3A 20 55 74 01 FB 7E 86 78 E2 E3 E4 E5 E6 E7 E9 EA 00 00 00 00 00 00 E9 DD 33 D2 58

Çizelge 6.1'de görülen yakalanmış veriler, akıllı karttın doğruluğunu kod çözücüye nasıl ispat ettiğini göstermektedir. Burada kullanılmış olan kart, korsan bir karttır. Görüldüğü gibi, Fiat-Shamir Sıfır Bilgi Testi korsan kart tarafından başarısızlığa uğratıldığı halde kod çözücü kapatılmamıştır ve bu kod çözücü, karıştırılmış görüntüyü düzeltmeye devam etmiştir. Korsan kart tarafından kod çözücüye gönderilmiş olan kimlik numarası cevabı 00 00 00 00 00 00 şeklindedir. Kod çözücünün en azından, sahte olduğu açıkça belli olan bu kimlik numarasını tanıması gerekliydi. Fakat tanımadığı için işleme devam etmekteydi.

6.1.3.2 Güvenli işlemci

Sky düzelticisinin gerçek işlem yapma merkezi ZC404044 vaya sonraki versiyonlarda kullanılmış olan ZC404047 mikroişlemcisidir [1]. İlk çıkan düzelticiler, 8 pinli bir 9306 EEPROM'una sahiptir. Sonraki versiyonlarda ise EEPROM verisi ZC404047 mikrokontrolörünün içine yerleştirilmiştir. Kontrol programı, maskelenmiş ROM'da tutulmaktadır ve bunun içindeki bilgilerin okunması oldukça zor olmasına rağmen imkansız değildir. Bu mikroçipin içindeki bilgilerin okunması, hack işleminin en önemli kısmıdır.

Buradaki ilk problem mikroçipin kimliğinin saptanmasıdır. Mikroçipin üzerindeki metin, ZC404044'ün bir Motorola mikrokontrolörü olduğunu ispatlamaktadır. Genellikle müşteriye özel versiyonlarda ZC öneki kullanılmaktaydı. Daha sonra, bu ZC404047 tasarımı daha genel olan bir Thomson numarası ile değiştirilmiştir ve böylece bu mikroçipin bulunması kolaylaştırılmıştır. Bu yeni mikroçip, bir 6805 mikrokontrolörünün maskelenmiş ROM versiyonuydu.

6805 mikrokontrolörünün başlıca görevi, havadan gelen veri için demodülatör olarak davranmaktır. Bu bilgi, özel mikroçip tipi belirtilmemesine rağmen patent başvurusunda verilmiştir. Ayrıca bu mikroçip, konu ile ilgili olan veri paketlerini 8052 idareyi sağlama mikrokontrolörüne iletmektedir.

Patent başvurusu, kullanılmış olan gerçek trafik ve protokol bakımından çok açıktır. Burada, prosedürlerle birleştirilmiş olan dalga biçimleri bile verilmiştir. 8052 mikrokontrolörüne iletilmiş olan en önemli veri paketi 32 baytlık 74h paketidir.

Ekranda gösterilen mesajların çoğu 6805 tarafından kontrol edilmektedir. Bu, gerçekten kod çözücünün en önemli işlemcisidir. Ayrıca bu işlemci, herbir alanın başlangıcındaki kendine özgü lojikteki Yalancı Rasgele Sayı Üreteci için yeni bir çekirdek (seed) üretmektedir. Bu çekirdekleri oluşturmak için bu 8 baytlık kod çözme anahtarı, görüntü sayacı (frame counter) ile birleştirilmiştir.

6.1.3.3 Uygulamaya özel lojik entegre devre

Burada kullanılmış olan uygulamaya özel lojik entegre devre, TC110G03AP'dir. Bu, video düzeltici devre yapısının kontrolünü gerçekleştirmektedir. Ayrıca bu, Yalancı Rasgele Sayı Üreteci için en uygun bölgedir. VideoCrypt kod çözücülerinin yeni versiyonlarının bazılarında bu parça TCE PTV-2 olarak etiketlenmiştir. Buradaki TCE, Thomson Consumer Electronics'e karşılık gelmektedir. Ayrıca bu entegre devre, kod çözücünün bütün kısımları

için clock üretimini de yönetmektedir. Bu entegre devrenin clock sinyali, 28 MHz'lik bir kristalden elde edilmektedir.

VideoCrypt teknik dökümanlarında verilmiş olan bilgilere göre Yalancı Rasgele Sayı Üreteci, 60 kademe uzunluğundadır. 8 baytlık karma fonksiyon çıkışı, yeniden çekirdek üretme değerini ve kullanılmamış olan dört durum bayrağını taşıdığı için bu çok uygun bir uzunluktur.

Yalancı Rasgele Sayı Üretecinin karakteristiği tam olarak bilinmemektedir. Ayrıca bu mikroçip, çoklayıcı kontrol devre yapısını da içermektedir. Bu devre yapısı, video depolama satırları ve anahtarlama için kontrol sinyalleri üretmektedir.

6.1.4 VideoCrypt video düzeltici tekniği

VideoCrypt kod çözücüsünün video bölümü oldukça basittir. Karıştırılmış olan video, bir TDA8703 analog-dijital konverteri tarafından dijitalleştirilmektedir. Bu konverter videoyu, 8 bitlik sözcükler dizisine dönüştürmektedir. Daha sonra bu dijitalleştirilmiş video, iki FIFO bellek grubunu beslemektedir. FIFO, ilk giren ilk çıkar (first in first out) tabirine karşılık gelir. Bu entegre devrelerin herbiri, 910 adet 8 bitlik sözcük depolayabilmektedir.

Herbir FIFO, satırın bir bölümünü tuttuğu için videoyu yeniden düzenlemek sadece bu iki FIFO arasında veri clock'landığı zaman anahtarlama yapmaktan ibarettir. Doğru sıradaki bölümler ile düzeltilmiş olan dijitalleştirilmiş video bir TDA8702 dijital-analog konverterini beslemektedir.

Çoklama ve kapılama, bu entegre devre tarafından kontrol edilmektedir. Daha sonra bu analog video, çıkış katını beslemektedir. Çıkış katı, bir diskrit transistörlü tasarımdır. Video sinyali kenetlenmektedir ve ekranda görülecek olan grafikler eklenmektedir. Ortaya çıkan bu sinyal, SCART konnektörüne gönderilmeden veya alıcıya geri gönderilmeden önce filtrelenmektedir.

6.1.5 VideoCrypt-I kart protokolü

VideoCrypt sisteminde, sınırlı sayıda paket tipi mevcuttur. Birçok gözlem ve denemeden sonra herbir paketin görevi neredeyse tamamen öğrenilmiştir. Kart adresleme bölgesi gibi bazı bölgelerde, değişik kart serileri için farklılıklar vardır. 09 serisi Sky akıllı kartı, 74h paketinde basit bir aylık kod bazlı kodlama kullanmaktadır.

EuroCrypt-M gibi bir sistemle karşılaştırıldığı zaman VideoCrypt sisteminin gerçekten çok

zayıf bir sistem olduğu görülür. Burada sadece on adet paket tipi kullanıldığı bilinmektedir. Ayrıca, VideoCrypt-II protokolünün bunlardan başka herhangi bir ilave paket tipine sahip olup olmadığı bilinmemektedir. Bununla birlikte, VideoCrypt sisteminde bu paketlerin kullanımı birçok bakımdan daha mükemmeldir.

1) 70h Komutu

Yönü : Akıllı karttan kod çözücüye

Uzunluğu : 6 Bayt

İçeriği : Akıllı kartın kimlik saptama numarası

Herbir akıllı kart, kendisine ait bir seri numarasına sahiptir. Bu seri numarası 6 bayt uzunluğundadır ve kartın dağıtım numarası baytı, kart kimlik saptama numarası ve kontrol işlemi olmak üzere üç bölüme ayrılır.

Kartın dağıtım numarası, tek bir bayt ile temsil edilmektedir. Yüksek nybble her zaman 2 olmaktadır. Bu durum, kart tipinin basit bir bellek kartından ziyade bir akıllı kart olduğunu göstermektedir. Düşük nybble ise dağıtım numarasını vermektedir. Güncel dağıtım numarası 10 (0A) ve en son dağıtım numarası ise 09'dur. Sonraki dağıtım numarası 0B olabilir.

İkinci bölüm, kartın kimlik saptama bölümüdür. Bu, kartın kimlik numarasını içeren 4 baytlık bir sayıdır. Üçüncü bölüm ise kart kimlik numarası için kontrol işleminin yapıldığı bölgedir.

2) 72h Komutu

Yönü : Kod çözücüden akıllı karta

Uzunluğu : 16 Bayt

İçeriği : Önceki kart kimlik saptama numarası, görüntü başına ödeme ve sıralama bilgisi

Bir akıllı kart kod çözücüye yerleştirildiği zaman kod çözücü bu karta, kart kimlik saptama numarası ve diğer bilgilerin 4 baytını içeren bir mesaj göndermektedir. Diğer bilgiler muhtemelen, kartın yetki verme düzeyi, kalan görüntü başına ödeme (PPV) kredisi ve kartın zincirlenmiş olup olmadığı hakkında bilgiler içermektedir.

Bu zincirleme işlemi tasarlanmış olduğu için herbir kod çözücü bir kart seri numarası ile damgalanmaktadır ve eski kartlarda kalan kredi bilgisinin yeni abone kartlarına aktarılmasına izin vermektedir. Bu sistem, EPROM kartları akıllı kartlardan daha üstün olduğu sıralarda tasarlanmıştır. Bu zincirleme işlemi Avrupa'daki sistemlerde kullanılmamıştır.

3) 74h Komutu

Yönü : Kod çözücüden akıllı karta

Uzunluğu : 32 Bayt

İçeriği : Mesaj bloğu (adresleme ve anahtar verisi)

Bu, VideoCrypt sisteminde en çok kullanılan komuttur. Bu mesaj paketi, akıllı kartı aktif hale getirme veya kapatma kodlarının tamamını taşımaktadır. Ayrıca bu, kod çözme anahtarını üreten karma fonksiyon için veri olarak kullanılmaktadır. 09 serisi karttan 10 (0A) serisi karta geçildiği zaman 74h'ın paket yapısı bu yeni karta tamamen yerleştirilmemiştir. Aşağıda verilmiş olan bilgiler 09 serisi akıllı kart yapısını anlatmaktadır.

Bu paketteki veri, 27-4-1 yapısına sahiptir. İlk 27 bayt kod çözücü bayraklarını, kart adresleme komutlarını, kanal kimliği saptayıcıyı ve bu paket tarafından gerçekleştirilmiş olan kart adreslerini içermektedir. Bu paket karma fonksiyon ile işleme sokulduğu zaman 28, 29, 30 ve 31 bölümlerindeki sonuç kısımları, bu kontrol işlemi baytlarındaki baytlar ile eşitlenmelidir. Bu akıllı kart, geçerli bir kontrol işlemine sahip olmayan paketleri reddedecektir. Bu kontrol işleminin görevi, karma fonksiyona düzenlenecek bir yalın metin saldırısını önlemek veya bir akıllı karta korsanlar tarafından yetki verilmesini önlemektir. 09 karma algoritması tehlike altında olduğu zaman erişim kontrolü yönetim sisteminin tamamı çökmüştü ve bu yüzden, akıllı kartları aktif hale getirmek ve güncellemek için kontrol mesajlarını headend'ten emüle etmek mümkündü.

Son bayt, bir paket kontrol işlemidir. Bu baytın değeri, paketteki baytların toplamını 256'nın bir katı haline getirmek için gerekmektedir.

Bu paketteki Bayt 0, kod çözücü bayraklarını taşımaktadır. Bu bayt kod çözücüye, paketlerin nasıl yönetileceğini bildirmektedir. Yüksek nybble, kullanılmakta olan karıştırıcı tipini saptamaktadır. Bir Cxh değeri, kanalın karıştırılmamış olduğunu göstermektedir. Bir Exh veya Fxh değeri, kanalın sıkı (hard) karıştırılmış olduğunu göstermektedir. Dxh değeri ise serbest bir karıştırıcı erişim modunu göstermektedir. Düşük nybble'ın gösterdiği x8h değeri, bu paketin yeni bir kod çözme anahtarı üretmek için kullanıldığını belirtmektedir. x0h değeri ise, paketin bir bilgi paketi olduğunu ve yeni bir anahtar üretmek için kullanılmadığını göstermektedir.

4) 76h Komutu

Yönü : Kod çözücüden akıllı karta

Uzunluğu : 1 Bayt

İçeriği : Kod çözücüdeki yetki verme düğmesine basıldı

Bu paket, kod çözücü üzerindeki yetki verme düğmesine basıldığı zaman akıllı karta bu bilgiyi vermektedir. Eğer program, bir görüntü başına ödeme programı ise akıllı kart abonenin kredisinden doğru miktarda krediyi çıkartacaktır.

Bu komut, Sky 07 ve 09 serisi kartları hack edilmiş olarak kaldığı süre boyunca bilgisayar korsanları tarafından kullanılmıştır. Yetki verme düğmesine basıldığı zaman korsan akıllı kart, kartta depolanmış olan bilinen bütün karşı tedbirler nedeniyle çevrim yapacaktır.

Bu komut, VideoCrypt sisteminin güvenli olduğu düşünüldüğü zaman sona erdikten sonra kullanılmamıştır. Akıllı kartın güvenliği garanti edilemediği için kart üzerindeki bir kredi deposunun bir görüntü başına ödeme (PPV) ile darbelenmesi artık kullanılamamaktadır. Sky Channel'ın ilk görüntü başına ödeme uygulaması ön kayıtlı bir olaydı. Abonenin, abone yönetim merkezini telefonla arayarak akıllı kartına havadan gönderilen sinyaller ile yetki verdirmesi gerekmekteydi.

5) 78h Komutu

Yönü : Akıllı karttan kod çözücüye

Uzunluğu : 8 Bayt

İçeriği : Kod çözme anahtarı

Bu paket, akıllı karttaki karma fonksiyon tarafından üretilmiş olan 8 baytlık kod çözme anahtarıdır. Bu anahtar, uygulamaya özel lojik entegre devredeki Yalancı Rasgele Sayı Üretecine geçmektedir. Bu sonucun sadece 60 biti Yalancı Rasgele Sayı Üretecine çekirdek oluşturmak için kullanılmaktadır.

6) 7Ah Komutu

Yönü : Akıllı karttan kod çözücüye

Uzunluğu : 25 Bayt

İçeriği : Ekranda görülen mesaj verisi

Bu paketteki veri, ekranda gösterilecek olan metindir. Bu metin ekranda, 12 karakterlik iki

metin olarak gösterilmektedir. İlk bayttaki bitlerin durumuna bağlı olarak bu mesaj gösterilebir veya gizlenir. Sky kanallarının bazılarında bu mesaj "THIS PROGRAMME IS BLOCKED" şeklindedir.

7) 7Ch Komutu

Yönü : Akıllı karttan kod çözücüye

Uzunluğu : 16 Bayt

İçeriği : Akıllı kartın kimlik saptaması, görüntü başına ödeme ve sıralama bilgisi

Bu bilgi paketi, kartın kimlik saptaması, görüntü başına ödeme ve sıralama bilgisinden oluşmaktadır. Bu mesaj paketinin her zaman Fiat-Shamir Sıfır Bilgi Testi dizisinden önce gelmesi, bu bilgi paketinin Sıfır Bilgi Testinde kullanılmakta olduğunu göstermektedir.

8) 7Eh Komutu

Yönü : Akıllı karttan kod çözücüye

Uzunluğu : 64 Bayt

İçeriği : Fiat-Shamir Sıfır Bilgi Testinin X değeri

Bu veri paketi, akıllı karttan gelen X cevabını içermektedir. Bu cevap, $X = R^2$ Mod N işleminin sonucudur. Buradaki R, rasgele bir sayıdır. Bu R sayısı, kod tablosundan alınabilmektedir.

9) 80h Komutu

Yönü : Kod çözücüden akıllı karta

Uzunluğu : 1 Bayt

İçeriği : Fiat-Shamir Sıfır Bilgi Testi için Q bayrağı

VideoCrypt sisteminde kullanılmış olan Fiat-Shamir Sıfır Bilgi Testi protokolünde, 00h ve 01h olmak üzere iki muhtemel değer mevcuttur. Bu bayt akıllı karta, Fiat-Shamir Sıfır Bilgi Testi için cevabı nasıl hesaplıyacağını bildirmektedir.

10) 82h Komutu

Yönü : Akıllı karttan kod çözücüye

Uzunluğu : 64 Bayt

İçeriği : Fiat-Shamir Sıfır Bilgi Testi için akıllı kart cevabı

Bu cevabın yapısı, Q Baytının 00h veya 01h olup olmamasına göre değişmektedir. Bu bayrak akıllı karta, Y cevabını üretmesini emretmektedir. Eğer Q Baytı 00h ise o zaman bu cevap Y = R olmaktadır. Eğer Q Baytı 01h ise o zaman bu cevap Y = (R . S) Mod N olmaktadır. Buradaki R, akıllı karttaki bir tablodan gelen bir sayıdır ve S ise kartın seri numarasıdır.

Eğer (6.1) ve (6.2) eşitliklerindeki sonuçlar elde edilmişse, akıllı karta kod çözücü tarafından yetki verilmektedir.

$Y^2 = X \text{ Mod } N$ [eğer Q = 00h ise] (6.1)

$Y^2 = (X . V) \text{ Mod } N$ [eğer Q = 01h ise] (6.2)

Kod çözücü, yetki verme işleminden hemen önce V sayısını almaktadır. Bu V sayısı, kart kimlik numarasıdır ve S ise $S = \sqrt{V} \text{ Mod } N$ işleminden elde edilmektedir.

11) Diğer Komutlar

Yukarıda listelenmemiş olan en önemli komut 86h komutudur. Bu komut, kart kişiselleştirme komutu gibi görünmektedir. Bu komut, Sky 09 ve 10 serisi kartlarda mevcuttur. Ayrıca bu komut, 17.03.1996 görüntü başına ödeme olayını aktif hale getirmek için bilgisayar korsanları tarafından kullanılmıştır.

6.1.6 VideoCrypt sisteminde Fiat-Shamir sıfır bilgi testi

Daha öncedende bahsedildiği gibi Fiat-Shamir Sıfır Bilgi Testini veri akışlarının bir bölümü olarak kullanmakta olan Avrupa'daki tek kanal Adult Channel'dır. Bu prosedür Çizelge 6.2'de gösterilmiştir.

Çizelge 6.2 Akıllı kartın Fiat- Shamir Sıfır Bilgi Testi'ne cevabı [1]

Komut	Akıllı Kart Cevabı
70h	Akıllı kart kod çözücüye kart kimlik numarasını (V) gönderir
7Ch	Akıllı kart kod çözücüye kimlik saptamayı ve N sayısını gönderir
7Eh	Akıllı kart kod çözücüye 64 baytlık X paketini gönderir
80h	Kod çözücü akıllı karta Q baytını gönderir
82h	Akıllı kart kod çözücüye Y cevabını gönderiri
70h	Akıllı kart kod çözücüye kart kimlik numarasını (V) gönderir

Çizelge 6.2'de görülen sıra daha önceki bölümde Fiat-Shamir Sıfır Bilgi Testi için verilmiş

olan modeli izlemektedir. Bununla birlikte genel modül N, kart tarafından kod çözücüye 7Ch paketinin bir parçası olarak gönderilebilmektedir. Daha sonra Q baytı, Y cevap tipini emretmekte ve akıllı kart 82h paketindeki bu cevabı göndermektedir. Buradaki problem 7Ch paketinin kesin yapısının bilinmemesidir. Bu paket, genel modül N'i kart kimlik numarasının bir parçası olarak da içerebilmektedir.

Fiat-Shamir Sıfır Bilgi Testi'nin Adult Channel'da düzgün bir şekilde çalışmamıştır. Eğer çalışmış olsaydı, kod çözücü korsan akıllı kartı reddederdi. Bunun yerine, korsan kart çalışmaya devam etmişti. Fiat-Shamir Sıfır Bilgi Testi paket dizisi, 07 serisi akıllı kartta görülmemektedir. Bu paket, 09 serisi kartta korsan kartların çalışmasını engellemeyi denemek için kullanılmıştır. Fakat, korsanlar bu durumun üstesinden gelmiştir.

Fiat-Shamir Sıfır Bilgi Testi, VideoCrypt-II sisteminde daha etkili bir biçimde kullanılmıştır. Burada, akıllı kartın bir Fiat-Shamir Sıfır Bilgi Testi sonucu hesaplaması gerekmekte ve hesaplanmış olan bu sonuca zıt yönde çekirdek değerini EXOR'laması gerekmekteydi. Yani, akıllı kartın kendisine yetki vermesi gerekmekteydi ve 07 VideoCrypt hack işleminde kullanılmış olduğu gibi sadece bir algoritma ve anahtar hack işlemi çalışmayacaktı. VideoCrypt-II kartındaki algoritma, 07 kartına kullanılmış olan algoritma ile aynıydı. Fakat, anahtarlar ve baud hızları farklıydı.

Fiat-Shamir Sıfır Bilgi Testi, gizli bilgiye veya veriye güvenmektedir. Bu, projenin doğru bir biçimde çalışması için çok önemlidir. Fakat bu algoritmanın gerçekleştirilmesindeki problem gizli verinin kesinlikle gizli kalmasının gerekmesiydi. Eğer bu veri öğrenilirse, o zaman kartın doğruluğunu kod çözücüye ispatlaması prosedürü tehlikeye girmektedir.

Bahsedilmiş olan bu tehlike, 07 Sky kartının güvenliğinin çökmesi ile sonuçlanmıştır. Eğer bu algoritma doğru biçimde çalışmış olsaydı ve kod çözücüdeki 8052 mikrokontrolörü hatalı olmasaydı, 07 kartındaki Fiat-Shamir Sıfır Bilgi Testi bu kadar başarısız olmayacaktı.

6.1.7 Dorchester kodu

Sky Channel'ın 07 serisi kartının güvenliği artık söz konusu değildi. Herkes 07 koduna sahipti ve Sky'ın bu duruma karşı yapabileceği çok az şey vardı. İngiltere'de beşyüz bir korsan 07 kartı olduğu tahmin ediliyordu ve Sky'ın bu kadar kişiye, servislerini hack ettikleri için dava açması ekonomik bakımdan mümkün değildi.

Sky, korsan 07 kartlarına karşı bazı elektronik karşı tedbirler uygulamıştır. Fakat korsanlar tarafından 07 kartının kodunun tamamen okunmuş olduğu bir gerçekti. Korsanların büyük bir

çoğunluğu karşı tedbirlerde bazı anahtar tablolarının değiştirileceğini tahmin edebiliyordu. Fakat kodun ve algoritmanın, daha fazla işlemci bağımlı yapılabilmesi de mümkündü.

Sky, bu problemden kurtulamayacağını anladığı için yeni akıllı kartı olan 09 serisine geçmiştir. 18.05.1994 tarihinden sonra korsan akıllı kartlar artık çalışmadı. SEASON7 programı da çalışmıyordu.

20.06.1994 tarihinde Londra'daki Dorchester otelinde yapılmış olan bir açık arttırmada 09 Sky kartının kodu satışa sunulmuştu. Bu kod için istenmiş olan çok fazla olduğu için ancak bu kodun bir kısmı satın alınabilmişti. Artık korsan kartlar yeniden çalıştırılabilecekti. Bu durum, Sky için tam bir felaket oldu. Çünkü eski 07 korsan kartlar 09 kartına dönüştürülebiliyordu.

Bu yeni 09 kodu, bir PIC16C84 mikrokontrolörünün belleğine sığacak kadar küçüktü. Bu yeni kod, 07 algoritmasında yapılmış olan büyük bir değişiklikti. Fakat bir PIC16C84'e emüle edilemeyecek kadar farklı değildi. Bu yeni algoritmadaki değişikliği sağlayan şey çarpma işleminin kullanılmış olmasıydı.

Dorchester kodu sadece bir hafta geçerli kaldı. Çünkü Sky, sadece 09 algoritmasının bir geçiş versiyonunu kullanmıştı. Yani, PIC16C84'te 09 algoritmasının basit bir uygulaması çalıştırılmıştı. Daha sonra Sky, bu Dorchester koduna bir elektronik karşı tedbir uygulayarak korsan piyasayı çökertti.

Dorchester kodu, 07 algoritmasının geliştirilmiş bir şekliydi. Kodun yeniden yazılmasıyla herhangi bir veri paketi için doğru imzanın üretilmesi mümkündü. Sky'ın VideoCrypt sistemi havadan gönderilen sinyalle yetki verilme prosedüründe çalıştığı için, muhtemelen Sky'ın müdahalesi olmaksızın korsan kartların açılması mümkün olacaktı.

Havadan gönderilen veri kayıtlarının birkaç analizinden sonra, numuneler anlaşılır hale geldi. Bir kart kod çözücüye yerleştirildiği zaman kart kimlik numarası servis merkesine gönderilmekteydi. Sky'a telefon edip birkaç kartı havadan aktif hale getirmelerini sağlayarak yetki verme planının işleyiş şeklinin bir kopyasının yapılması mümkündür. Daha sonra, Markus Kuhn tarafından Phoenix programı yaratılmıştır. Bu program, bilgisayarın bir VideoCrypt kod çözücüsünü emüle etmesini sağlayan ve paketleri bir arabirim üzerinden bir karta gönderlmesine izin veren DECOEM.C programını baz almaktaydı. Phoenix programı, VideoCrypt sisteminin çalışma şeklini gösteren başarılı bir uygulamadır.

6.1.8 74h paketi

07 ve 09 serisi kartlardaki paketler, 27-4-1 yapısındaydı. İlk 27 bayt veri baytları, diğer 4 bayt karma imza/kontrol işlemi baytları ve son 1 bayt ise bir Modülo 256 paket kontrol toplamıdır.

09 uygulamasında, kart seri numaraları küçük bir kodlama rutiniyle kodlanmıştır. Bu ilave güvenlik seviyesi, algoritma kırıldığı zaman biraz işe yaramaktaydı. Bu algoritma, 4 baytlık bir tablo üretmektedir. Komutu elde etmek için bu tablonun Bayt 0'ı, 74h paketinin Bayt 3'ü ile EXOR'lanmıştır. Bu tablonun Bayt 2'si ise nanokomutlar ile EXOR'lanmaktadır.

VideoCrypt-II sistemi, giriş baytlarının konumları farklı olmasına rağmen önceki versiyonu ile büyük ölçüde benzer bir algoritma kullanmaktadır. VideoCrypt-II Phoenix programı bu sistemde kullanılabilmesine rağmen ticari amaçlı korsanların bu programı satışa çıkarması mümkün görünmüyordu. Çünkü bu program, VideoCrypt-II kod tablosunun serbest bırakılmasını kapsamaktaydı.

Nanokomut kod çözme algoritmasının bir bölümü aşağıda verilmiştir:

```
xx = 74msg[1] ^ 74msg[2] ;

xx = (xx>>4) | (xx<<4) ;

b =  74msg[2] ;

for (i = 0; i<4; i++)
        {
        b = (b<<1) | (b>>7) ;
        com_arr[i] = xx + b ;
        b = com_arr[i] ;
        }
```

6.1.9 09 serisi korsan kartlar

BSkyB kanalı, 1994 yılında üç ay içinde 750,000 adetten fazla orijinal akıllı kartını Genesis aktif hale getirici-bloke edici korsanlığında kaybetmiştir. Kaybedilmiş olan bu akıllı kartları kapatmak için birçok elektronik karşı tedbir gerçekleştirilmiştir. Fakat bilgisayar korsanları, bu kapatma kodlarını bloke edici devre yapıları ile engellemiş ve kartların kapatılmamasını sağlamışlardır. Bununla birlikte, korsan 09 serisi bir akıllı kart da piyasada mevcuttu. Bu

durum, Sky'ın 09 serisi akıllı kartının güvenliğinin çökertildiğni göstermekteydi.

Bu sıralarda, korsan 09 kartının çeşitli uygulamaları piyasada satılmaktaydı. Fakat bunlar genellikle bir haftadan fazla çalışmadılar. Çünkü Sky'ın düzenli olarak gerçekleştirmiş olduğu karşı tedbirler bu korsan kartları kapatmaktaydı. Bununla birlikte, korsanların bu karşı tedbirlerden elde ettikleri bilgiler çok değerliydi. Bunun sonucunda, çok çabuk iyileştirilebilen korsan 09 kartı ortaya çıkmıştır.

Bu korsan 09 kartının ilk versiyonlarında, iki adet PIC16C84 ve bir adet 24C65 mikroçipi kullanılmıştır. Sky tarafından karşı tedbirler gerçekleştirildiği zaman bu kartların yeniden programlanması gerekiyordu. Fakat gerçekleştirilmiş olan bu karşı tedbirler sayesinde korsanların bu konudaki bilgisi artmaktaydı.

News Datacom, 09 kartının adres bölgesinin tamamını karma fonksiyon için giriş verisi olarak kullanılabilecek şekilde yapmıştır. Bundan dolayı, herhangi bir korsan kartın çalışabilmesi için orijinal Sky kartının belleğinin bir kopyasına sahip olması gerekliydi.

Ayrıca bu yeni kartta kullanılmış olan diğer yaklaşımlar da çok yenilikçiydi. Yeni abone yükü altında ezilen abone yönetim sistemine güç vermiş olan nanokomutlar kullanılmıştır. Ayrıca bu nanokomutlar, abonelerdeki akıllı kartların havadan gönderilen sinyallerle yeniden programlanabilmesini sağlamaktaydı. Ayrıca, yeni kanalları ve görüntü başına ödemeli olayları da sisteme dahil etmek mümkündü.

Daha sonra, 09 kartının emüle edilmesi daha kolay hale geldi. 09 kartının en güçlü yaklaşımlarının büyük bir kısmı News Datacom tarafından kullanılmamıştı. Genesin/Phoenix hack işlemleri, orijinal Quickstart akıllı kartlarında uygulanmıştı. Bu nedenle Sky Channel, Quickstart projesini 1995 yılı başında durdurmak zorunda kalmıştır.

09 Sky kartı bir adet Motorola MC68HC05SC21 mikrokontrolörü kullanmaktaydı. Bu mikrokontrolör, MC68HC05C4 mikrokontrolörünü baz almaktadır. Bu kartın içindeki bilgilerin nasıl okunacağına dair pekçok teori mevcuttur. Bu teorilerden bazıları, kartın test modunun aktif hale getirilmesini ve içeriğinin boşaltılmasını içermekteydi. Diğer teoriler ise nanokomutları kapsamaktaydı.

Bir kartın içindeki kodun boşaltılmasındaki problem, bunu bir emülasyonda gerçekleştirilmesi değildi. Bu aslında, herbir rutindeki fonksiyonu anlamaktan ibaretti. Etkisi görülünceye kadar bir rutinin fonksiyonunun anlaşılması gerçekten çok zordur. Fakat bu etki görüldükten sonra emüle etme işlemi devre dışı bırakılacağından çok geç olacaktır.

6.1.10 Nanokomutlar

Sky'ın 09 serisi akıllı kartı 07 serisi kartından biraz daha karmaşıktır. Gelişmiş mimarisinin yanısıra kullanılmış olan kod daha mükemmeldir. 09 serisi karttaki karma fonksiyon, herbir iterasyondaki 8 baytlık cevabın bütün baytlarınımodifiye ettiği için 07 serisi karttakinden çok daha fazla karmaşıktır. 07 serisi kartlarda, herbir iterasyonda sadece 2 bayt modifiye edilmiştir.

Ayrıca 09 serisi kart, Sky'ın bu kartı havadan göndereceği sinyallerle yeniden programlayabilmesini sağlayan rutinler içermekteydi. Daha sonra rutinler, D2-MAC ve VideoCrypt-II sistemlerinde kullanılmış olan 09 serisi kartları yeniden programlamış olan korsanlar tarafından da kullanılmıştır.

Bunu gerçekleştirmenin metodu, havadan gönderilen verinin içine özel bir 74h paketi ilave etmekten ibaretti. Bu paket, sıradan bir 74h paketinden biraz farklıydı. Açılması veya kapatılması gereken kart kimlik numaralarının bir yığınını (batch) içermesinin yanısıra kartın okuyacağı ve işlem yapacağı bir grup komuta sahiptir.

Kart kimlik numaraları ve nanokomutlar, küçük bir algoritma ile kodlanmıştır. Bu algoritma çekirdek olarak Card Age baytını (Bayt 02) ve nanokomut kod çözme anahtarı baytını (Bayt 02) kullanmıştır. Bu algoritmanın çıkışı, paket komutu baytı (Bayt 03), kart kimliği baytları (07-10 arası baytlar) ve nanokomut baytları (12-26 arası baytlar) ile EXOR'lanmıştır. Sıradan bir kart açma/kapatma paketinde bu nanokomut baytları, bu paket tarafından adreslenecek olan kart kimliklerinin en sağdaki baytı (beşinci bayt) olmaktadır.

Card Age baytı, genellikle her ay değiştirilmektedir. Verilmiş olan bir Card Age baytı ve herbir olası nanokomut kod çözme anahtarı baytının çıkışlarının bir tablosunun üretilmesi mümkündür. Bu tablolar, düzenli olarak internet üzerinde Usenet haber grubunda (alt.satellite.tv.europe) yayımlanmaktaydı. Algoritma bilindiği zaman bu çok fazla gerekli olmadığı için pekçok kişi bu tabloları, bilgisayarları için yapmış oldukları bloke edici programlarda kullanmıştır.

Bir nanokomut paket değerini gösteren paket komut değeri, genellikle 80h'tır. Yani 12 ile 26 arasındaki kart yorumlayıcı baytları, komut olarak davranmaktadır.

Sky bu komutları kullanarak, kartlar bloke edicilerin içindeyken bu kartlara yazabilmekteydi. Phoenix programının ömrü boyunca, kart kimliğinin en sağdaki baytlarının sırasının düzensiz olduğu görülmüştür. 07 serisi kartta bu değerler ardışıktı. Bunun değeri o zaman korsanların

gözünden kaçmıştı. Fakat Phoenix arabirimli 09 kartları bloke edicilerin içindeyken Sky tarafından kapatılmaya başlandığı zaman bunun farkına varılmıştı.

Havadan gönderilen sinyalle adresleme planında nanokomutların kullanımı çok etkili ve tehlikeli bir tercihtir. Bunun etkili olmasının nedeni, oldukça sınırlı bir adresleme sistemini yeniden hayata geçirmesidir. Tehlikeli olmasının nedeni ise potansiyel bilgisayar korsanlarına, üzerinde çalışmaları için tamamen yeni yaklaşım verilmesidir. Bu, korsanların kartın adres bölgesinindeki bilgileri boşaltasını sağladığı için 09 kartının tehlikeli olduğunu ispatlamıştır.

Bazı nanokomutlar giriş olarak sadece karma fonksiyonu 00h ile iki kere gerçekleştirmektedir. Bunlar, ilerde kullanılmak üzere programlanmadan bırakılmış olan nanokomutlardır. Yalnızca kriptografik olduğu görülen (karma fonksiyonu yineleyen) nanokomutlar ve bellekten veri yükleyebilen veya okuyabilen nanokomutlar arasında belirgin bir fark vardır (Çizelge 6.3).

Nanokomut kavramının temel bir elemanı pointer değeridir. Bu pointer değeri, herbir nanokomut uygulandıktan sonra bu nanokomuttaki baytların sayısı ile arttırılmaktadır. Bazı nanokomutlarda bu pointer değeri, karma fonksiyonuna giriş değeri olarak kullanılmaktadır. Bu, prosedürleri daha fazla karışık hale getirmektedir ve nanokomutların önceden anlaşılmasını daha fazla zorlaştırmaktadır.

Çizelge 6.3 Yalnızca kriptografik olan nanokomutlar [1]

Komut	Görevi	Girişler
0Ch (2 Bayt)	Karma fonksiyonu iki kere yinele	00h Herbir turda
14h (5 Bayt)	Karma fonksiyonu iki kere yinele	00h Herbir turda
1Dh (2 Bayt)	Karma fonksiyonu iki kere yinele	00h Herbir turda
24h (3 Bayt)	Karma fonksiyonu iki kere yinele	00h Herbir turda
34h (4 Bayt)	Karma fonksiyonu iki kere yinele	00h Herbir turda
FFh (1 Bayt)	Karma fonksiyonu iki kere yinele	00h Herbir turda
3Ch (1 Bayt)	Karma fonksiyonu iki kere yinele	3Ch Herbir turda
41h (1 Bayt)	Karma fonksiyonu iki kere yinele	41h ve 00h
49h (1 Bayt)	Karma fonksiyonu iki kere yinele	60h ve 49h
19h (1Bayt)	Karma fonksiyonu iki kere yinele	Pointer ve 19h
03h (1 Bayt)	Karma fonksiyonu 64 kere yinele, sonra dur	Pointer

1) Kontrol nanokomutları

46h (1 Bayt) Nanokomut işlemi durdur ve çık

2) Okuma/yazma nanokomutları

09h (3 Bayt) Format: 09h xx yy

Bu, 30h nanokomutu için bir adres yükleyicidir. Burada xx, adresin en soldaki bit ve yy ise adresin en sağdaki bitidır. Daha sonra karma fonksiyonu, 63h ve 00h giriş değerleri ile iki kere yinelenmektedir.

0Fh (2 Bayt) Format: 0Fh aa

BFh (Adresin en soldaki bitini tutar) ve C0h (Adresin en sağdaki bitini tutar) 'ta depolanmış olan değerler ile tanımlanmış olan adrese aa verisini yazmaktadır.

11h (3 Bayt) Format: 11h aa xx yy

aa verisini xx yy adresine yazmaktadır. Buradaki xx, en soldaki bit ve yy ise en sağdaki bittir.

30h (2 Bayt) Format: 30h cc

Bu bir okuma komutudur. cc değeri, okunacak olan baytların sayısıdır. Başlangıç adresi, 09h veya 11h nanokomutu tarafından yüklenmekte olan adresler tarafından belirlenmektedir. Okunabilecek baytların maksimum sayısı 127'dir. Eğer cc sıfır ise, sadece tek bir bayt okunur. Karma fonksiyon, okunan herbir bayt ile yinelenmektedir.

39h (2Bayt) Format: 39h aa

aa verisini 0092h adresine yazar ve daha sonra, karma fonksiyonu 00h girişi ile yineler.

11h (4 Bayt) Format: 11h aa xx yy

RAM'de xx yy ile belirlenmiş olan adrese aa verisini yazar. Sky 09 serisi kart, RAM'in 0080h'tan 00FFh'a kadar 128 baytına sahiptir. Eğer xx'teki değer sıfır değilse (Bu bir ROM adresini gösterir), yazma işlemi gerçekleştirilmez.

28h (5 Bayt) Format: 28h aa bb cc dd

aa bb cc dd nanokomut dizisini 008Dh'tan 0090h'a kadar olan RAM adreslerine yazar. Daha sonra, dd ve pointer giriş değerleri ile karma fonksiyonu iki kere yineler.

Çizelge 6.4 09 Sky kartının ve DSS 01 kartının bellek haritası [1]

MC68HC05SC21	
0000-000F	Yazmaçlar (Registers)
0080-00FF	RAM (128 Bayt)
0520-10FF	EEPROM
1100-1FF7	ROM Sayfa 0
1100-19FF	ROM Sayfa 1
1FF8-1FFF	ROM Kullanıcı Vektörleri
RAM:	128 Bayt
ROM:	6144 Bayt
EEPROM:	3008 Bayt

Nanokomutların çalışma şeklini ve belleğin çeşitli bölgelerinin (Çizelge 6.4) nasıl seçildiğini anlamanın en iyi yolu, 09 Sky kartlarının içindeki bilgileri okumak için kullanılmakta olan Vampire programlarından birinin kaynak kodunun incelenmesidir. Bunun için kullanılabilecek olan en iyi programlardan biri GETROM isimli programdır. Bu program, ilgili internet sitelerinde ve BBS'lerde mevcuttur.

6.1.11 VideoCrypt karıştırıcı sisteminin hack edilmesi

Aşağıdaki paragraflarda, VideoCrypt karıştırıcı sistemlerinde gerçekleştirilmiş olan çeşitli hack işlemleri kısaca anlatılmıştır. Bu bölümün alt başlıkları olarak bu hack işlemleri daha detaylı olarak tek tek incelenmiştir [1].

VideoCrypt sistemi artık, seksenli yıllarda olduğu kadar güvenli bir sistem değildi. Bunun sebebi, korsanlık teknolojisinin çok ilerlemiş olmasıdır. 06 serisi ve 07 serisi akıllı kartlar, ters mühendislikten geçirilmiştir. 06 serisi akıllı kartın hack edilmesi, korsan bir akıllı kartın geliştirilmesini sağlayacak ucuz bir mikrokontrolör bulunmadığı için ekonomik açıdan uygulanabilir bir hack etme işlemi değildi. 07 Ho Lee Fook hack işleminin ilk versiyonu bu düşünce tarzının doğruluğunu kanıtlamıştır. Bu hack, orijinal kod çözücüdeki 8052 mikrokontrolörünün bir 8752 mikrokontrolörü ile değiştirilmesini baz almaktaydı. Bu hack işleminin piyasaya çıkmasından birkaç ay sonra PIC16C84 mikrokontrolörünü baz alan ilk korsan kartlar ortaya çıkmıştır. Bundan sonra, 07 Sky kartının akıbeti Sky ve News Datacom kanalları dışında herkes tarafından bilinmekteydi [1].

09 serisi ve 10 serisi kartlar, sistemi destekleyen oldukça güzel olan bazı çalışmalara sahipti. Bu akıllı kart serileri, kartın hack edilmeden kalmasını sağlayacak ve VideoCrypt sistemini gerçekten çok güvenli bir sistem yapacak bazı güzel unsurlara sahipti. Fakat yinede bu 09 ve

10 serisi kartlara bilgisayar korsanları tarafından ters mühendislik çalışması uygulanmış ve bu kartlar kopyalanmıştır.

İlk ticari amaçlı hack işlemi 1990 yılında gerçekleşmiştir. Bu hack işleminin ismi, bu hack işlemini ilk defa piyasaya süren Morley Research firmasının ismini almıştır. Fakat bu tür faaliyetler İngiltere sınırları içinde yasadışı olduğu için Morley Research firması, bu hack işlemini piyasaya sürmekten vazgeçmiştir.

İkinci hack işlemi, bunun gerçekleştirilebilir olduğuna inanılmadığı için bilgisayar korsanları arasında en az bilinenidir. Piyasada çok sayıda, akıllı kart belleğinin programlanmasını engelleyen ucuz gerilim sınırlayıcılar mevcuttu. Bu hack işleminin ismi Infinite Lives hack'ti. Ayrıca, Zener Diode hack olarak ta adlandırılabilmektedir. Bu, EPROM yazma voltajını sınırlayarak Sky Channel'ın havadan gönderdiği sinyaller ile korsan bir EPROM kartını kapatmasını engellemiştir.

Üçüncü hack işlemi, KENtucky Fried Chip hack olarak bilinmektedir. Bu, önceki hack işlemlerinden tamamen farklıydı. VideoCrypt kod çözücüsündeki gerçek yazılımın, sisteme karşı kullanıldığı ilk hack işlemidir.

Dördüncü hack işlemi olan McCormac hack işlemine, gerçekleştirilme yapısından dolayı VideoCrypt sisteminin buna karşı hiçbir savunması yoktu. Bu hack işlemi, VideoCrypt sistemindeki ve de diğer akıllı kart bazlı sistemlerdeki temel ilkelerden birindeki kusura dayanmaktaydı. Bu hack işlemini engellemek için bazı metodlar mevcuttu. Fakat bu metodların büyük bir kısmı, eski sistemlerde düzgün bir şekilde çalışmamaktaydı.

Beşinci hack işlemi, 07 Ho Lee Fook hack olarak adlandırılmıştır. Bu, 1993 yılına kadar VideoCrypt sisteminde gerçekleştirilmiş olan en etkili hack işlemidir. Bu, News Datacom tarafından kartın doğruluğunu kod çözücüye ispatlaması için kullanılmış olan rutinlerin geçersiz olduğunu veya en azından hiç kullanılmadıklarını ispatlamıştır. Bu hack, gerçek bir korsan akıllı karttı. Bazı kimseler bunun kopya (klon) bir kart olduğunu önesürmüş olsada bu iddia doğru değildi. Çünkü bu hack, sahte veya klon master kimliği kullanmaya güvenmemektedir.

Altıncı hack işlemi OMIGOD hack olarak bilinmektedir. Ayrıca bu hack, SEASON7 olarakta bilinmektedir. Bu hack, ticari amaçlı olmadığı için önceki bütün hack işlemlerinden farklıdır. Bu hack, bir bilgisayar programıdır ve bu program, sanal bir akıllı kart gibi davranarak kod çözücüyü sürmektedir. Bu program ücretsizdir ve bu konu ile ilgili internet sitelerinden temin edilebilmektedir.

Yedinci hack işlemi, Delayed Data Transfer (DDT) hack olarak bilinmektedir. Temelde bu hack, OMIGOD hack işleminin bir uzantısıdır. Buradaki farklı yaklaşım, geciktirilmiş veri transferinin sağlanmış olmasıdır. Karıştırılmış olan bir televizyon programını video kayıt cihazında kaydetmek ve internet üzerinden gerekli olan anahtar akışını bilgisayara indirmek mümkündür. Daha sonra OMIGOD arabirimi aracılığıyla bu anahtar akışı, kaydedilmiş olan televizyon programını düzeltmek için kullanılmaktadır.

Video karıştırıcı sisteminde başka bir hack işlemi de ortaya çıkmıştı. Buna göre, karıştırılmış olan videonun yeteri kadar bilgisayar gücü kullanılarak gerçek zamanlı olarak düzeltilmesi mümkündü. Bu hack, SEASON7 hack'inin de yaratıcısı olan Markus Kuhn tarafından ortaya çıkarılmıştır. Bu hack işleminin uygulanmasındaki başlıca problem, karıştırılmış videoyu düzeltmek için herkesin pahalı bir donanıma sahip olmasının gerekli olmasıydı. Fakat bu, en mükemmel hack işlemiydi. Bu hack işlemi için yazılım, ilgili internet sitelerinden ücretsiz olarak temin edilebilmektedir.

07 serisi karttan 09 serisi karta geçildiği zaman bilgisayar korsanlarının büyük bir kısmı yenilgiye uğratılmıştı. Fakat bu durum fazla uzun sürmedi. Yeni 09 kodunun bir kısmı, Londra'da Dorchester otelinde gerçekleştirilen bir açık arttırmada satışa çıkarılmıştır. Bu kod, sadece bir hafta çalışmış olmasına rağmen VideoCrypt sistemindeki bu zamana kadar gelmiş geçmiş en mahvedici saldırı olan Phoenix hack ve Genesis bloke edicilerinin korsanlar tarafından yaratılmasını sağlamıştır.

Phoenix hack işlemi, VideoCrypt sisteminde kullanılmış olan abone yönetim sisteminin nasıl çalıştığını deneyerek anlamaya dayalı zekice bir denemeydi. Temel olarak bu hack işlemi, bir kod çözücüyü emüle etmek için yazılmış olan bir programdan ibaretti. DECOEM.C isimli bu kod çözücü emülatörü programı, kartın yetki verme düzeyini değiştirecek olan 74h paketlerini karta göndermektedir. Bu, Dorchester kodunu baz almaktadır ve karma fonksiyon ve temel yetki verme komutları bilindiği zaman, geçerli kontrol mesajlarının karta gönderilebileceğini ispatlamıştır. Bu tamamen zekice bir denemeydi. Fakat ticari amaçlı kişiler bu Phoenix kodunu çalarak bu kodu başka bilgisayar korsanlarına satmışlardır ve bunun sonucunda, Genesis bloke edicileri ortaya çıkmıştır.

Genesis bloke edicisi, Phoenix aktivasyon rutinlerinin içine bloke etme rutinlerini dahil etmiştir. Fakat bu durum, Phoenix rutinleri ile aktif hale getirilmiş olan kartlar bu bloke edicilerde kullanılmış olsalar bile Sky ve News Datacom tarafından kapatılmıştır. Bunun sebebi, 09 kartının nanokomutlar olarak adlandırılmış olan alt komutlara sahip olmasıydı. Bu

nanokomutlar, bloke edicilerdeki kart seri numaralarını araştırmaktaydı. Genellikle bu nanokomutlar, aktif hale getirilmiş olan korsan kartları kapatmaktaydı. Sky tarafından bu yolla, bir ay içerisinde bir milyonun üzerinde korsan kart kapatılmıştır. Fakat bu sırada, yeni bir hack işlemi piyasaya sürülmek için hazırdı.

09 serisi kartı hack işleminin çalışan bu versiyonu, orijinal akıllı kartın bellek alanının bir kopyasını gerektirmekteydi. Bunun sebebi, News Datacom'un algoritmayı, adres alanındaki herhangi bir baytın karma fonksiyon için bir giriş değeri olarak kullanılabilecek şekilde tasarlamış olmasıydı. Fakat bu yaklaşımdaki temel ilkelerden birindeki hataya fazla önem vermemişlerdi. Bu hata, kullanılmış olan algoritma ve baytları seçme metodu bilindiği zaman kartın içeriğinin elektronik olarak boşaltılabilmesinin mümkün olmasıdır.

Kartın içeriğinin elektronik olarak boşaltılması şeklinde gerçekleşen bu hack işlemi, News Datacom'un en çok canını sıkanlardan biriydi. Çünkü, adres alanının bir karma fonksiyona giriş değeri olarak kullanılabileceği ve karma fonksiyonu ile bayt seçme metodu bilindiği zaman bu yaklaşımın zayıf kaldığı, birçok makalede daha önceden belirtilmişti. Bu hack işlemine Vampire Hack ismi verilmiştir.

Sky 09 serisi kartın bellek alanının tamamı herkes tarafından bilindiği zaman, Sky Channel için herşey bitmişti. 1994 yılının Aralık ayında 09 kartının güvenliği tamamen çökertilmiştir. Bundan sonra Sky Channel, korsan kartlar üzerinde etkisi birkaç saatten fazla sürecek bir elektronik karşı tedbir gerçekleştiremedi.

Sky 10 serisi kart 31.10.1995 tarihinde kullanılmaya başlandı. Bu yeni kart üzerinde gerçekleştirilmiş olan en büyük hack işlemi, Sky'ın görüntü başına ödeme (PPV) servisinde olmuştur. Bu hack işlemi, Sam Chisum hack olarak bilinmektedir. Bu hack, görüntü başına ödemeli program başlamadan 24 saat önce, internet sitelerine ve BBS'lere gönderilmiş olan bir metin dizisi şeklinde dağıtılmıştır. Bu metin dizisini bir Phoenix arabirimi ile karta göndererek, kartı bu görüntü başına ödemeli program için yetki verilmiş hale getirmek mümkündü.

6.1.11.1 Morley Research hack işlemi

Morley Research hack işlemi, 1990 yılında gerçekleştirilmiştir. Bu hack, Sky Channel'ın havadan gönderdiği sinyaller ile korsan akıllı kartları kapatmasına engel olmuştur. Kullanılmış olan temel metot, yazma rutinlerinin engellenmesi ve bunların üzerindeki adresin değiştirilmesidir. Bu işlem, kart ve kart okuyucusu arasına bağlanmış olan bir devre ile

gerçekleştirilmiştir. Çizelge 6.5'te verilmiş olan kod ve Şekil 6.3'te gösterilmiş olan diyagram orijinal hack işleminden alınmıştır.

Bu yazılım, kod çözücü için başka bir kart kimlik numarası üretmektedir. Bu dikkate değer hack işlemi, birkaç yıl önce başarılı olmaktaydı. Fakat daha sonra Sky, bu hack işleminin işe yaramasını engelleyecek birkaç tedbir aldı ve çalışmasını engelledi.

Bu hack işleminin amacı, kod çözücüye yerleştirilmiş olan kartın farklı bir kimlik numarasına sahip olduğunu düşünmesi için kod çözücüyü kandırmayı denemekti. Bu hack işlemi artık, Avrupa'da kullanılmakta olan VideoCrypt-I sisteminde çalışmamaktadır. 8748 mikrokontrolörüne yüklenmesi gereken program Çizelge 6.5'te verilmiştir.

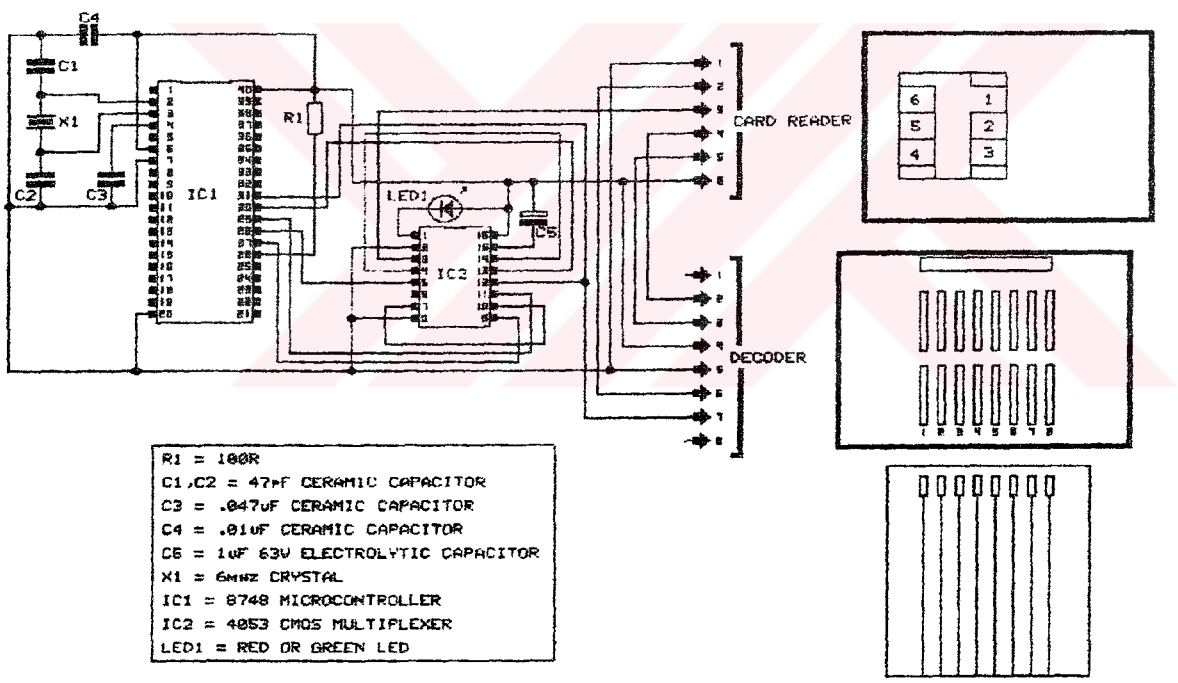
Çizelge 6.5 8748 mikrokontrolörüne yüklenmesi gereken kod [1]

0000	0409000409000004	0080	83AF095310968299
0008	09231339273A0410	0088	103489BE08BC00FF
0010	1458D3AC96108A02	0090	F7AFE6951C27F7F7
0018	F8D36F96101458D3	0098	4310393492EE8FFC
0020	81C648FFD383C64A	00A0	5301D301F7431039
0028	FFD385C64CFFD387	00A8	3492231339349234
0030	C64EFFD389C650FF	00B0	9283AF0953109683
0038	D38BC652FFD38DC6	00B8	2315393489BE08BC
0040	54FFD38FC6560410	00C0	00FFF7AFE6C71C27
0048	04E804F1241B2438	00C8	F7F7F7F743153934
0050	243C24452449246B	00D0	92EEC1FC5301D301
0058	094767F658BE06EE	00D8	F7F7F74315393492
0060	5FBE081478094767	00E0	2313393492349283
0068	FFF7AFEE63147814	00E8	8A02231239890104
0070	78F9A8FAA9FFAA83	00F0	108A04BB0A1458D3
0078	BD0DED7A8A019A00	00F8	8396F523FE148123
0100	FB14812304148123	0170	8F966D23B0148123
0108	071481230B148123	0178	1514812306148123
0110	FB148123FF1481EB	0180	1614812359148104
0118	1304108A08BB1814	0188	109A00BD07ED8D8A
0120	58D3E6961F238514	0190	80839A00BD09ED96
0128	81237F1481000000	0198	8A8000839A01****
0130	23FF1481EB300410		
0138	8A1004108A202312		
0140	398A0104108A4004		
0148	108A80BB0A1458D3		
0150	FC964D23D514B223		
0158	4F14B223E014B223		
0160	FB14B223FF14B2EB		
0168	6304108A801458D3		

Yeni bir kart kimlik numarası yaratmak için &174, &178, &17C, &180, &184 baytlarının &00'dan &FF'e kadar olan rasgele değerlerle değiştirilmesi gerekmektedir. Bu, kod çözücünün kullanmış olduğu korsan akıllı karta uyan bir deaktivasyon kodunun kod çözücü tarafından alınma şansını azaltmaktadır. Çünkü kod çözücü, orijinal akıllı kartın yerleştirildiğini düşünmektedir.

Morley Research hack işleminin, bir kart okuyucu kullanılmaksızın gerçekleştirilmesi planlanmıştı. Çünkü 1990 yılında bu kart okuyucular, günümüzde olduğu kadar kolay bir şekilde temin edilemiyordu. Bu tarihte gerçekleştirilmiş olan çözüm, kartı doğru konumda tutmak için bir konnektör düzeni ve bir kenet (clamp) kullanılarak geçici bir kart okuyucusu yaratmaktı. Bu ünite, kart ve kod çözücü arasına yerleştirilmektedir. Bu bakımdan, 09 Sky kartları ile kullanılmış olan Genesis bloke edicilerine benzemektedir.

Şekil 6.3'te gösterilmiş olan devre yapısı, alışık olunmayan bazı konfigürasyonlara sahipti. Çoklayıcıya bağlanmış olan LED, kart açıldıktan sonra çoklayıcıya akım boşaltmaktadır.



Şekil 6.3 Morley Research hack işleminin devre diyagramı [1]

Bu hack işleminde, karttan kod çözücüye giden veriye ilk defa ekonomik açıdan uygulanabilir bir biçimde saldırıldığı için dikkate değer bir hack etme işlemiydi. Fakat, Sky ve News Datacom bu hack işleminin çalışmasını engellemiştir.

6.1.11.2 Infinite Lives hack işlemi

VideoCrypt sisteminde kullanılan kod çözücünün, hiçbir önemli bilgiyi içermeyen akılsız bir teminal olduğu düşünülmektedir. Fakat 06 serisinden önceki kartlarda çok önemli bir kusur vardı. Bu kusur, kullanmış oldukları EPROM tipleriydi. Bu EPROM'lar, kartın üzerine yazmak için 17 V'tan daha büyük bir voltaj gerektirmekteydi.

Kod çözücülerin modifiye edilmesi mümkündü. Böylece, kartlar Sky tarafından geçersiz kılınamayabilirdi. Bu yüzden, bir korsan Sky akıllı kartının süresiz olarak kullanılması veya en azından bir sonraki ROM değiştirilmesine kadar kullanılması mümkündür.

Bu hack işlemi, Infinite Lives hack olarak adlandırılmıştır. Bunun çalışma şeklinin ayrıntıları, konuyla ilgili internet sitelerinde ve BBS'lerde mevcuttu. Bu çalışma birkaç kablonun kesilmesi, başka birkaç kablonun lehimlenmesi ve bir zener diyot yerleştirilmesinden ibarettir.

Temel olarak bu hack işlemi, kartın programlama konnektöründeki voltajı sınırlamayı gerektirmektedir. Kartın yeniden programlanması veya karta yeniden yazılması için bu konnektördeki gerilim 21 V bölgesinde olmalıdır. Bu konnektöre giden gerilimi kesmek, kartın ve bu yüzden de kod çözücünün çalışmayacağı anlamına gelmektedir. Bunun yerine bu gerilim, tipik olarak 15 V gibi bir değerde sınırlanmıştır. Bu gerilim değeri, kartın çalışmasını sağlamaktadır. Fakat, karta yazma işleminin başarılı olmasına izin vermemektedir.

Infinite Lives hack işleminde, kartın EPROM belleğine yazılması engellenmiştir. Bundan dolayı Sky kanalı bu korsan kartları kapatamamıştır.

Asıl problem, Sky'ın Quickstart kartlarında bulunmaktaydı. Bu kartlar, ödemeli televizyonların güvenliği hakkında bilgisi olmayan kişiler tarafından bulunmuş olan bir pazarlama yöntemiydi. Bu kartlar Sky tarafından havadan gönderilen sinyaller ile aktif hale getirilebiliyordu. Bunlar, bir müşterinin bu kartı bir mağazadan almasına, abone olmasına ve birkaç saat içinde bu karta Sky tarafından yetki verildikten sonra kartını kullanabilmesine imkan tanımaktaydı. Fakat bu kart satın alınırken çok sayıda kişi sahte isim ve adres kullanmıştı.

Bu Quickstart akıllı kartlarının büyük bir kısmının Avrupa'da kullanılması planlanmıştı. Bu karta uygulanmış olan Infinite Lives hack prosedürü, ilk önce karta Sky tafafından yetki verdirilmesini ve daha sonra bu kart kod çözücüden çıkarılarak birkaç ay için kod çözücüye yerleştirilmemesini kapsamaktaydı. Abonelik süresi bittiği zaman Sky, çeşitli zamanlarda bu kartın kimlik numarasını kara listede havadan gönderecek ve bu kart, kod çözücüye

yerleştirilmediği için kapatılamayacaktı.

Infinite Lives hack işlemi, Avrupa'da Quickstart akıllı kartlarının çok sayıda satmasını sağlamıştır. Çünkü, Sky tarafından kapatılamayan veya süresiz olarak geçerli kalan bir kart hazırlamak mümkündü. Bu hack işlemi, kartların kanal tarafından kapatılma riskini minimuma indirmiştir.

Sky Channel, yeni bir kart serisini kullanmaya başladı. 06 serisi akıllı karttan sonrakiler EEPROM'du. Karta bir gerilim katlayıcı dahil ettikleri için artık V_{pp} gerilimine ihtiyaç kalmamıştır. Bu durum, Infinite Lives hack problemini çözmüştür.

Sky Channel'ın Infinite Lives hack'ten sonra iyileştirilmesi, akıllı kartların gerçek gücünün kanıtıdır. Çünkü akıllı kartlar, korsanlık tehlikesi ile karşı karşıya olan bir sistemin iyileştirilmesine izin vermektedir. Bununla birlikte, akıllı kartların ters mühendislik işlemine tabi tutulması imkansız değildir. Fakat bu işlem, pahalı ve gerçekleştirilmesi zor olan bir işlemdir. Akıllı kartların peryodik olarak değiştirilmesi, kartın hack edilmesini engellemekten ziyade sistem korsanlık tehlikesi ile karşı karşıya olduğu zaman gerçekleştirilen bir kart değiştirme işlemi haline gelmiştir.

Kartın yazılmış olup olmadığını kontrol etmek için sadece kodun birkaç baytı gerekmekteydi. Fakat Sky bunu yapmadı. Aynı tür bir hack işlemi, KENtucky Fried Chip hack işleminin kullanılıp kullanılmadığını kontrol etmek için de kullanılabilmektedir.

Kripto işlemciye, kartın belleğindeki belirli bir adresi okuması ve sonucu depolaması (A) için havadan gönderilen sinyaller ile talimat verilmektedir. Daha sonra, yeni veriyi (B) bu adrese yazması için talimat verilmektedir. Sonraki adım, bu adresten gelecek olan yeni verinin okunması ve sonucun depolanmasıdır (C).

Kontrol etme işlemi, sadece bir dizi karşılaştırmadan ibarettir;

1. (A) should not equal (C)
2. (B) should equal (C)

6.1.11.3 KENtucky Fried Chip hack işlemi

KENtucky Fried Chip hack işlemi, Phoenix hack işlemlerinin ve Genesis bloke edicilerinin başlangıç noktasıydı. Bu, kod çözücüdeki 8052 mikrokontrolörünün yerini almıştır. KENtucky Fried Chip hack'indeki mikrokontrolörün içindeki program orijinal akıllı kartın seri numarasını okumakta ve bu kartın seri numarasının bulunduğu paketleri aramaktaydı.

Daha sonra bulduğu bu paketleri, akıllı karta ulaşmamaları için bloke etmekteydi. Bu yüzden, Sky Channel bu akıllı kartı kapatamamaktaydı.

VideoCipher-II ve EuroCypher karıştırıcı sistemlerinde, dahil edilmiş güvenli mikrokontrolör tekniği kullanılmıştır. VideoCrypt sisteminde ise ayrılabilir güvenli mikrokontrolör tekniği kullanılmıştır ve kod çözücü akılsız bir terminal statüsüne düşürülmüştür.

VideoCipher-II sisteminin ve FilmNet'in kullanmış olduğu dijital ses karıştırıcı sisteminin hack edilmiş olması dahil edilmiş güvenli mikrokontrolör yaklaşımının yetersiz olduğunu kanıtlamıştır.

VideoCrypt kod çözücüsünde KENtucky Fried Chip hack işlemini olanaklı kılan tehlikeli kusur, korumasız 8052 mikrokontrolörüydü. Bu mikrokontrolör, kod çözücünün idaresini sağlamaktaydı. Ayrıca, güvenli mikrokontrolör-kart arabirimi arasındaki trafiği yönetmekteydi. Bu, kod çözücüdeki mikrokontrolörlerin okuma sigortalarını yakmak için standart bir prosedürdür. Bu sigorta, mikrokontrolörde depolanmış olan programın yetkisiz olarak incelenmesini önlemektedir.

Güç kaynağı kısmından ayrı olarak, VideoCrypt kod çözücülerinde en fazla arızalanan parça 8052'ydi. Bu yüzden, orijinal bir kod çözücü satın almaya gerek kalmadan bu mikroçipin değiştirilmesinin mümkün olması gerekirdi. Servis merkezlerinin birçoğu arızalı bir 8052 durumunda, ya hurdaya ayrılmış bir kod çözücüden söktükleri 8052 ile ya da orijinal bir 8052'deki program ile programlanmış olan bir 8752 ile bu arızalı mikroçipi değiştiriyordu. Muhtemelen Thomson ve News Datacom yakılamayan okuma sigortalarını seçtikleri zaman bu düşüncedeydi.

Sky ve News Datacom, KENtucky Fried Chip hack işleminin 1.0 versiyonuna başarılı bir şekilde karşı koymuştur. Sky, 07 serisi yeni akıllı kartına geçtiği zaman bu hack işleminin 1.1 versiyonu kullanıma hazırdı. Fakat yeni kart grubundaki (batch) yazılım öncekinden farklı olduğu için bu yeni versiyon hack işlemi çalışmamıştır.

İlk KENtucky Fried Chip hack işlemlerinden bir tanesi, EPROM için bir düzen kullanmıştı. Korsan EPROM ve orijinal EPROM, bir çoklayıcı ve bir DIL soketi ile bir baskılı devre kartına monte edilmiştir. Her ne zaman gerekli olursa bu orijinal EPROM, devreye yeniden sokulabilmekteydi.

KENtucky Fried Chip hack'inde kullanılmış olan prensiplerin tamamı, Sky 09 bloke edicileri için yeniden kullanılmıştır. Fakat bunun gibi hack işlemleri sadece ikinci evre hack

işlemleriydi. Günenilir korsan kartlar piyasada mevcut olduğu zaman, bloke ediciler ve KENtucky Fried Chip gibi hack işlemleri önemini yitirmiştir.

6.1.11.4 McCormac hack işlemi

VideoCrypt sistemindeki ilk McCormac hack işlemi, sadece onbeş saniye içinde gerçekleştirilmiştir. İlk beş saniye bunu çalıştırmak, on saniye ise sonuçları yazmak için gerekmekteydi. Basit olması bakımından bu çok iyi bir hack işlemiydi. Güvenlik bakımından bu hack işleminin hiçbir zaman gerçekleşmemesi gerekirdi. Fakat bu hack işlemi, VideoCrypt sisteminden çok daha ileri uygulamalara sahipti.

Bu, bir telefon konuşmasını gizlice dinlemeye benzemektedir. Çünkü, akıllı kart ve kod çözücü arasında akan veri alınmakta ve bir bölge civarında iletilmekteydi. Diğer kod çözücülerin herbiri, akıllı kart soketine yerleştirilmiş olan küçük bir radyo alıcısına sahipti. Herbir kod çözücüye sanal olarak bir kart yerleştirilmişti ve daha sonra herbir kod çözücü televizyon kanalını düzeltmeye devam etmekteydi. Bu teori, iki kod çözücüyü üç adet kablo ile bağlayarak test edilmiştir ve bu hack işlemi çalışmıştır. Bu kablolar, bir topraklama kablosu, bir veri kablosu ve bir resetleme kablosudur.

Bu hack işlemi, VideoCrypt sisteminin güvenliğini yıkmıştır. Fakat bundan sonra ortaya çıkmış olan ticari amaçlı hack işlemleri daha mahvedici olmuştur. Bu yeni hack işlemleri ile korsan akıllı kartlar kullanılabilir duruma geldiği için McCormac hack işlemi önemini yitirmiştir.

Korsan bir 10 serisi akıllı kartın olmayışından dolayı bu teori değersiz hale gelmiştir. Çekirdek anahtarlarının dağıtımındaki temel problem, internet sayesinde çözülmüştür. Bu hack işlemi, bir akıllı kartın bir televizyon kanalının şifresini çözmeye kilitlenmesini ve veri akışının izlenmiş olmasını ve bu veri akışının internet üzerinde yayımlanmasını gerektirmekteydi.

Bu hack işleminin 1989 yılında gerçekleştirilmiş olan eski versiyonundan başlıca farkı, çekirdek anahtarlarının internet üzerinden gönderilmiş olmasıdır. Orijinal teori, anahtar dağıtımı için bir radyo vericisi kullanmaktaydı.

1996 yılında çıkarılmış olan yeni versiyonundaki teori, orijinal bir akıllı kart ve bir kod çözücü arasındaki veri akışının Season tipi bir arabirim aracılığıyla izlenmesiydi. Daha sonra bilgisayar, bu anahtarları internet aracılığıyla birkaç uydu bilgisayara yeniden yayımlamaktaydı. Bu uydu bilgisayarlarının, aynı televizyon kanalında master olarak çalışan

bir kod çözücüye kilitlenmesini sağlayacak Season tipi bir arabirimine sahip olması gerekmekteydi. Bunun dezavantajı, herhangi bir zamanda sadece bir televizyon kanalını kullanabilmesiydi. Fakat aynı türde bir düzenin herbir kanal için tekrarlanması mümkündür. Böylece, bütün kanallar hack edilebilmektedir.

Böyle bir işlemi çalıştırmak için bir bilgisayara, DOS veya Windows gibi çok görevli bir işletim sistemi gerekliydi. Fakat bu tip çalışma için ideal sistem Linux'tur.

Böyle bir hack işleminin en kritik yaklaşımı, sunucu (server) bilgisayar ile uydu bilgisayarlar arasındaki veri gönderme süresiydi. Eğer bu süre çok büyük ise, çekirdek anahtarları zamanında ulaşamayacaktı.

İnternetin o günkü durumu, böyle bir hack işleminin uluslararası bir alanda çalışmasını engellemekteydi. İnternet henüz yeterince hızlı değildi. İrlanda'da bile bazı internet servis sağlayıcıları arasındaki yönlendirme süresi yeterince hızlı değildi. İngiltere ve Amerika arasında bir internet servis sağlayıcısından diğerine geçerken problemler çıkmaktaydı.

Bu problem, bir BBS yaklaşımı ile çözülebilmekteydi. Bir BBS, aynı zamanda yapılan birkaç bağlantıyı problemsiz bir şekilde yönetebilmekteydi. Bu yüzden, bir SEASON kurulumu kullanılarak BBS'in herbir çevirmeli (dial-up) portunun bir SEASON arabirimi çalıştıran diğer bir bilgisayarı bir seri portunu beslemesi mümkündü. Bu uygulama DOS altında yazılabilmesine rağmen sunucu, Linux veya Unix'te daha iyi çalışmaktadır.

Bu bağlantıdaki en önemli trafik, çekirdekler ve Fiat-Shamir Sıfır Bilgi Testidir. Bununla birlikte, News Datacom'un 74h paketlerini birbirinden bağımsız yapması ve zamanlamayı da daraltması mümkün olabilmekteydi. Bu durum, VideoCrypt-II sisteminde yapılmış olan değişikliklerden bazıları ile benzerdir. Bununla birlikte, programlamanın en önemli kısmı VideoCrypt-I aracılığıyla iletilmekteydi. Bu sistem, ilk teknik şartnamenin bir parçası olmasına rağmen kod çözücünün bir kimlik numarasına sahip olmamasından dolayı kusurluydu.

Sky Channel Avrupa'da, hiçbir görüntü başına ödemeli yayınının gösterimini riske atmamıştır. Sky tarafından görüntü başına ödemeli ilk yayın 1996 yılında yapılmıştır. Bu, korsanlar tarafından hack edilmiştir ve korsan kartlarının, bir Phoenix arabirimi ile güncellenmesi de mümkün olmuştur. Bu durum, eskiden beri görüntü başına ödemeli kanallara sahip olan DirecTv DSS sisteminde farklıydı. Çünkü DirecTv sistemi, bir kod çözücü seri numarası sistemi kullanmaktaydı.

6.1.11.5 07 Ho Lee Fook hack işlemi

BSkyB televizyon kanalının en büyük geliri VideoCrypt karıştırıcı sistemi sayesinde gelmekteydi. Yani BSkyB, abonelerinden para kazanmaktaydı. Abone olan kişiler, üye olmak için para ödemekte ve bir akıllı kart almaktalardı. Bu akıllı kart VideoCrypt kod çözücüsüne yerleştirildiği zaman, parası ödenmiş olan kanallar için kod çözülmekteydi. Ayrıca BSkyB, parasını ödemeyen abonelerinin akıllı kartlarını havadan gönderdiği sinyaller ile kapatabilmekteydi.

VideoCrypt sistemini kullanmış olan diğer uydu televizyon kanalları da korsanlar tarafından hedef alınmıştı. Yani Adult Channel, JSTV ve TV Astra kanalları da tehlike altındaydı.

Bu hack işlemi, bu sistemde gerçekleştirilmiş olanların en tehlikelisiydi. Çünkü bu, bütün Sky kanallarına erişimi sağlayan yeni bir korsan akıllı karttı. Sky için problem, bunun gerçek bir Sky akıllı kartı olmamasıydı.

Korsan kart, orijinal Sky kartından yaklaşık 16 mm daha uzundu. Bu kart, tek tarafına monte edilmiş mikroçiplere sahip olan bir baskılı devre kartıydı. Bu özellikteki bir kart için standart kontrol, orijinal bir akıllı karttan gelen bir tabana (wafer) bakmaktı. İlk başta, mikroçip ve konnektör padini geçerli bir Sky kartından ayıran iyi hazırlanmış olan bir yöntem mevcuttu. Bu yöntem, plastiği kesmek ve daha sonra bu mikroçipi bir DIL başlığına yerleştirmektir. Daha sonra bu DIL başlığa, bir entegre devre gibi görünmesi için siyah bir reçine damlatılıyordu. Baskılı devre bordunun üzerindeki mikroçip bir PIC16C54 mikrokontrolörüydü. Bu mikroçip, şimdi artık sıradan olan PIC16C84'ün EPROM versiyonudur.

Aslında 07 Ho Lee Fook hack işleminin iki değişik versiyonu mevcuttur. Bunun kart versiyonu daha sonra çıkmıştır. İlk versiyonu, kod çözücüdeki 8052'nin yenisiyle değiştirilmesinden ibarettir. Kod çözücüdeki 8052 için orijinal VideoCrypt ismi doğrulayıcıydı (verifier). Bu mikroçipin kod çözücüden çıkarılması ve bunu yerine korsan 8752 mikroçipinin konulması gerekliydi. Daha sonra kod çözücü, BSkyB akıllı kartına ihtiyaç duymaksızın karıştırılmış kanalları düzeltmekteydi. Akıllı kartsız bir korsan Sky kod çözücüsü olan bu hack işleminin güncelleştirilmesine imkansız gözüyle bakılmaktaydı.

Eğer bu doğrudan orjinalinden kopyalanmış bir Sky kartı olsaydı, Sky bunu havadan gönderdiği sinyaller ile kapatabilecekti. Fakat 07 Ho Lee Fook kartları, belirli bir kart kimlik numarasını etkisiz hale getirmekle kapatılamıyordu. Çünkü korsan akıllı kartların kart kimlik numarası yoktu. Bunlar resetlendikleri zaman kart kimlik numarası olarak sıfırlardan oluşan

bir diziyi kod çözücüye göndermekteydi. Kart sadece, sinyalleri düzeltmek için gerekli olan veriyi ve algoritmaları içermekteydi. Sinyali düzeltmek için sadece yeterli bilgi içeren bir kart, VideoCrypt sistemini SAVE gibi bir sistem konumuna düşürmekteydi.

Fiat-Shamir Sıfır Bilgi Testi, bu sistemde uygulanmamıştı. Eğer uygun bir şekilde uygulanmış olsaydı, bütün bu korsan kartlar devre dışı bırakılabilecekti.

VideoCrypt sistemindeki eski teorilere göre, akıllı kartın kendisinin gerçek bir akıllı kart olduğunu kod çözücüye ispat etmesi gerekmekteydi. Eğer bu özellik kullanılmış olmasaydı, sadece karma fonksiyona ve anahtar tablolarına sahip olduğu için Ho Lee Fook kartı kesinlikle devre dışı bırakılabilecekti. VideoCrypt kod çözücülerinin eski modellerinde, Sıfır Bilgi Testi uygulaması hatalıydı. Bu yüzden, Sky ve News Datacom'un istemediği bir durumla sonuçlanan Sıfır Bilgi Testi görmezden gelindi.

07 Ho Lee Fook hack işlemi, 1993 yılının Nisan ayından 18.05.1994 tarihine kadar çalışmıştır [1]. News Datacom, elinden gelen bütün elektronik karşı tedbirleri denemiştir. Fakat bilgisayar korsanları, genellikle birkaç dakika içinde bu karşı tedbirlerin üstesinden gelmiştir. Bu yüzden, News Datacom'un yeni bir akıllı kart kullanımına geçmekten başka bir seçeneği kalmamıştır. Bu yeni akıllı karta geçtikleri zaman, kullanılmaya başlandıktan bir ay sonra bu kart da hack edilmiştir. Bunun sebebi, meşhur Dorchester kodudur. Fakat bu hack işlemi piyasaya çıktıktan bir hafta sonra News Datacom tarafından etkisiz hale getirilmiştir. Bundan sonra, çalışan korsan 09 kartları ancak 1994 yılı Kasım ayında ortaya çıkabildi.

VideoCipher-II sisteminin, o zamana kadar çıkmış olan sistemlerin en güvenlisi olduğu ilan edilmişti. Birkaç ay içinde bilgisayar korsanları, sadece bir kanal için ödeme yaparak bütün kanallara yetki vermesi için kod çözücüyü kandırmanın mümkün olduğunu keşfetmişti. Buna, EPROM hack veya Musketeer hack ismi verilmişti. Sky ile paralel olarak, Zener diode hack veya Infinite Lives hack olarakta değişik isimler almıştır. VideoCipher-II sistemi şu an üçüncü şeklindeydi. VideoCrypt sistemi de, dijital bir televizyon sistemi ile değiştirilinceye kadar benzer şekilleri almıştır.

VideoCrypt sisteminin dayandığı teknik, ayrılabilir güvenli mikrokontrolördür. Bunun anlamı, eğer sistem hack edilmişse, bu hack işlemini durdurmak için yeni bir kart serisinin kullanılmasının gerekli olduğudur. VideoCrypt sisteminin merkezi bir akıllı karttır. Bu kartın korsan bir akıllı kart ile değiştirilebilmesinin imkansız olduğu düşünülmekteydi. Fakat korsanlar bunu gerçekleştirdi. Kesin olan tek şey televizyon kanallarının bir karıştırıcı sistemin, sık sık güncellenmesi gereken geçici bir koruma yapısına sahip olduğunu

görmelerinin gerektiğiydi.

VideoCrypt sistemindeki PIC16C84 hack işlemleri için kaynak kodları internet sitelerinden ve BBS'lerden elde edilebilmektedir. Bu kodlar artık Sky kanallarında kullanılmamasına rağmen Adult Channel tarafından hala kullanılmaktadır.

6.1.11.6 07 OMIGOD Hack işlemi

OMIGOD hack işlemi Ho Lee Fook hack işleminin lojik olarak gelişmiş biçimidir. Bu, VideoCrypt sistemi için bir bilgisayar emülatör programıdır. Bu program ücretsiz olarak dağıtılmış olan bir yazılımdır. Bu hack işleminin ismi aslında SEASON7'dir. Fakat bilgisayar korsanlarının büyük bir kısmı bu hack işlemini OMIGOD hack'i olarak bilmektedir.

Bu hack işlemi, bir bilgisayarın orijinal bir Sky 07 kartını emüle etmesini sağlamaktaydı. Bu bilgisayar, VideoCrypt kod çözücüsünün kart slotuna bir arabirim olarak bağlanmaktaydı. Evinde bilgisayar olan kişiler bu hack işlemini çok kolay uygulayabilmekteydi. Bu emülatör programın Apple MAC versiyonu da mevcuttur. Bu programn piyasaya çıktığı zaman çok hızlı bir şekilde yayılmıştır. Çünkü bu program ücretsiz olarak dağıtılmıştı.

Bu arabirim bir MAX232 ve bir 74LS07 mikroçipi içeren çok basit bir devredir. MAX232 mikroçipi, RS232 ve TTL arasındaki düzeyleri birbirlerini anlayacak biçime dönüştürmekteydi. 74LS07 mikroçipi ise açık kollektörlü bir tampondur. MAX232 mikroçipi, iki pozitif ve negatif RS232 gerilimini dahili olarak üretmektedir. Yani kod çözücüden gelen kart besleme gerilimi hattı, arabirimi direkt olarak sürebilmektedir.

Bu arabirim, bir baskılı devre kartı üzerine kurulabilmekteydi. Bazı kişiler için bunun başlıca dezavantajı, bu arabirimin kod çözücüye bağlantısıydı. Bunu bağlamanın en mantıklı yolu, bir kart soketi üzerinden bağlamaktır. Fakat bundaki problem, bu sahte akıllı kartın biraz aşındırılmasının gerekli olmasıydı.

Standart bir fiberglas baskılı devre kartı malzemesinin kalınlığı 1.6 mm'dir. Akıllı kartın kalınlığı ise yaklaşık olarak bunun yarısı kadardır. Bu kalınlıktaki baskılı devre kartı bulunamaması durumunda, bu kartı 1.6 mm oluncaya kadar zımparalamak çok yaygın bir yöntemdir. Fakat ortaya çıkacak olan baskılı devre kartı, orijinal akıllı karttan daha uzun olacağı için bunun yerine artık çalışmayan bir korsan kartın kullanılması tavsiye edilmektedir.

Ayrıca bu arabirimin kod çözücüye direkt olarak bağlanması da mümkündür. Kod çözücüye bağlanması gereken sadece veri hattı, 6 V'luk V_{cc} hattı, topraklama ve resetleme hatlarıdır.

Fakat bu seçenek, devre yapısını bilmeyen kişiler için riskli bir tercihtir.

Bu hack işlemi, arabirim imalat endüstrisinin ortaya çıkmasına yol açmıştır. En iyi ticari amaçlı arabirimlerden bazıları Bölüm 4'te detaylı bir şekilde incelenmiştir. Ayrıca bu hack işlemi, 09 Season programlarının ve D2-MAC EuroCrypt Season programlarının temelidir.

6.1.11.7 Delayed Data Transfer hack işlemi

Bu hack işlemi, şuan VideoCrypt sistemindeki en güvenilir hack işlemidir ve VideoCrypt uygulamalarının hepsinde sorunsuz olarak çalışmaktadır. Bu hack işleminin VideoCrypt sisteminde çalışmasını sağlayan kusur, bu sistemdeki kontrol paketlerinin oranının yaklaşık olarak 1 kbaud olmasıdır. Bu veri oranı, sinyalin standart bir video kayıt cihazında banda kaydedilebilmesi için yeterince yavaştır. Fakat, veriyi taşıyan düşey karartma aralığı satırlarını kaydedemeyen bazı video kayıt cihazları da mevcuttur.

Bu hack işleminin çalışma prensibi, geçerli bir karttan gelen anahtar akışının kaydedilebilmesi ve depolanabilmesidir. Daha sonra bu anahtar akışı, televizyon programının karıştırılmış video bant kaydı ile beslenmiş olan kod çözücüye pleybek yapılabilmektedir. Pleybek yapılan bu anahtar akışı geçerli bir akıllı karttan gelen ile aynı olduğu için, kod çözücü bu karıştırılmış sinyali düzeltecektir. Çeşitli televizyon programları için anahtar akışları, ilgili internet sitelerinde ve BBS'lerde mevcuttu.

09 SEASON emülatör programlarının hepsine, Delayed Data Transfer (DDT) kodu dahil edilmiştir. Bu nedenle, bu hack işlemi için kullanılabilmektedirler. Gerekli olan tek şey, VCL (VideoCrypt Log) dosyalarının ilgili internet sitelerinden veya BBS'lerden temin edilmesiydi.

Delayed Data Ttansfer hack işleminin modifiye edilmiş bazı versiyonları da mevcuttur. Bunların en mükemmellerinden biri VBL (Video Broadcast Log)'tur.

Karıştırılmış VideoCrypt sinyalini düzeltmek için gerekli olan veri 74h/78h çiftidir. Bunların biri mesaj bloğu paketi diğeri ise anahtar paketidir. Veri trafiğinin geri kalanının büyük bir kısmı karta yetki verme ve kartı kapatma verisidir.

VCL formatı bu fazlalığı, depolama alanını kaydetmek için kullanmaktadır. Yüksek entropinin (hemen hemen sıkıştırılamaz anlamında) sadece 12 baytı her 2.5 saniyede bir depolanmaktadır. Bu yüzden, bir saatlik bir televizyon programının VCL dosyası yaklaşık olarak 17 kb büyüklüğündedir. Buna ilaveten 70h ve 7Ch paketlerindeki kayıt (log) dosyalarında normal olarak bulunan VCL dosyaları, kart sahibi hakkında bilgi (özellikle kart

seri numarası) içermemektedir. Burada bununan güvenlik yarığı sadece 78h paketindeki kalan nybble'ıdır. Bu nedenle, kartın özel bilgilerinin VCL dosyasına sızmasını önlemek için bunun temizlenmesi şarttır.

VCL dosyaları, 128 baytlık bir başlık ve 12 baytlık kayıtların belirli bir miktarını içeren çok basit bir ikili (binary) formattır. Bitimde VCL dosyaları, işletim sisteminin disk sektörü büyüklüğünün birkaç katı bir büyüklükte sıfır baytları ile doldurulmaktadır. Böylece MS-DOS gibi güvenli olmayan bir işletim sisteminden, hiçbir RAM içeriğinin VCL dosyasına sızmaması sağlanmış olur. VCL dosyalarının veya bunların içeriklerinin kullanılamaz hale getirilmesi için ikili bir modun kullanılması gereklidir.

128 baytlık VCL dosyasının başlık formatı şu şekildedir:

1) 0-3 arası baytlar

Formatın dosya tipini ve versiyonunu tanımlayan VCL1 ASCII dizisi.

2) 4-7 arası baytlar

12 baytlık kayıtların sayısı, 32 bit işaretlenmemiş tamsayı değeri olarak (ilk önce en soldaki bayt) kodlanmış bir şekilde bu dosyada depolanmaktadır.

3) 8-23 arası baytlar

Kayıt etme işleminin başladığı tarih ve saat.

Format: yyyymmddThhmmssZ

Buradaki yyyymmdd sırasıyla yıl, ay ve gündür. Örnek: 19940618

Buradaki hhmmss sırasıyla saat, dakika ve saniyedir. Örnek: 235959

Buradaki T ve Z sadece birer ASCII harftir. Basamaklar, ASCII karakterlerdir.

4) 24-55 arası baytlar

Kayıt işleminin yapıldığı uydu veya kablolu televizyon sisteminin ismidir. Bu, sadece 20h ve 7Eh arasındaki karakterlerden oluşan ve sonu sıfır ile biten bir ASCII dizisidir. Gerekli olduğu taktirde 32 baytı doldurmak için istenildiği kadar sıfır baytı eklenebilmektedir. Ayrıca bu fırmat, sonraki iki metin alanı için de kullanılmaktadır. Örnek: Astra

5) 56-63 arası baytlar

Kayıt işleminin yapıldığı transponderin ismi veya numarası. Örnek: Astra uydusundan yayın yapan Sky One kanalı için 08

6) 64-127 arası baytlar

Kaydedilmiş olan şeylerin tanımlanması. Örnek: Star Trek: TNG, episode 123

4-7 baytları arasında açıkça belirtilmiş olan 12 baytlık kayıtların birçoğu, ilk 128 baytı takip etmektedir. Herbir kayıt, bir 74h/78h VideoCrypt protokolü çiftini temsil etmektedir ve iki alanı içermektedir. İlk 4 bayt, 74h mesaj paketi bölümünün son 4 baytıdır ve kalan 8 bayt ise 78h anahtar paketine benzer olan veri bölümüdür. Herbir 74h paketinin 4 baytı, kart emülatörünün hızlı ve güvenilir bir şekilde kod çözücünün sorgulamaları ile senkronize edilmesini sağlamak için yeterlidir. 74h komutlarının son 4 baytı, yüksek entropilerinden (imza ve kontrol işlemi) dolayı seçilmektedir.

6.1.11.8 09 versiyonu Delayed Data Transfer hack işlemi

VBL, DDT kayıt formatının arttırılmışıdır. Bu, daha güvenilir VCL dosyası sağlama metoduna izin verdiği için DDT'den farklıdır. VCL dosyası, 74h paketleri için doğru anahtar cevaplarının etkili bir şekilde yayımlanmasıdır.

İlk dosya olan VBL, ihtiyaç duyan televizyon programı için geçersiz bir kart ve kod çözücü arasındaki trafiğin bir kaydıdır. Kullanıcı (Şahıs A), bu dosyayı bilgisayarına ve kodlanmış televizyon programını da video kasetine kaydedecektir. Daha sonra, geçersiz kart ile yapılmış olan bu veri kaydı geçerli kartı olan bir kullanıcıya (Şahıs B) geçecektir. Daha sonra bu kullanıcı, bu VBL veri kaydındaki geçersiz cevapların yerine doğru cevapları koyarak bir VCL dosyası hazırlar. Bundan sonra, düzeltilmiş olan bu VCL dosyası şahıs A'ya geri gönderilebilir.

Bu planın güvenliği, bu iki kişinin arasındaki güvene dayalıdır. Eğer bu VCL dosyaların herkes tarafından değiştirilmesi sağlayacak yasal bir iskelet (internet servis sağlayıcısı) olsaydı, o zaman bu hack işlemi mükemmel bir alternatif olurdu.

Bu hack işleminin kullanımı çok düşük düzeydeydi. Bunun sebebi, bu işlemin biraz karmaşık olmasıydı. Bu hack işlemi, bir video kayıt cihazının ilk önce uydu alıcısına, sonra da kod çözücüye bağlanmasını gerektirmekteydi. Karıştırılmış videonun uygun bir biçimde düzeltilmesi için bazı video kayıt cihazlarının pleybek kalitesi yeterince iyi değildir. Fakat video kayıt cihazlarının büyük bir kısmında yeterince iyi çalışmaktadır. Düzeltilmiş olan

videonun kalitesi, orijinal bir kod çözücü ile elde edilenden çok farklıdır.

6.1.11.9 Phoenix arabirim programı ile hack işlemi

VideoCrypt sisteminin temel paketi 74h paketidir. Bu paket, çekirdek (seed) veri iletimini ve kart adresleme görevlerini yönetmektedir. Bu paketin, bu iki görevi birleştirme davranışı mükemmeldir. 74h paketinin tamamı karma algoritma tarafından anahtar üretiminde kullanılmaktadır.

Bu paketin son beş baytı, kontrol işlemlerine ayrılmıştır. Son bayt, bir modülo kontrol toplamıdır ve bu, toplamanın sonucunun 256'nın bir katı olmasını garantiye almak için baytların toplamına ilave edilmekte olan bir değerdir. Diğer dört bayt ise karma fonksiyon imzası veya kontrol işlemidir. Eğer bu baytlardan herhangi biri yanlış ise, bu paket kart tarafından reddedilmektedir. Bu modülo kontrol toplamı önemsizdir. Fakat karma fonksiyon kontrol toplamı, geçerli bir karma algoritma ve geçerli bir anahtarlar kümesi gerektirmektedir. Bu, o kadar da önemsiz değildir.

09 kartının zayıf noktası, uygun bir biçimde kontrol işleminden geçirilmiş bir paketi üretmek için sadece geçerli bir anahtar tablosuna ihtiyaç duymasıydı. Hatta bu anahtar tablosunun, o anda kullanılmış olması da gerekmemekteydi. 09 kartı, 07 kartındakine benzer bir biçimde seçilmiş olan bir grup anahtar tablosuna sahiptir.

Phoenix programı, karttaki bütün kanalları aktif hale getirmek için bir açma (turn on) komutu ile açılması gereken kartın seri numarasını içeren geçerli bir 74h paketi yaratmaktadır. Phoenix programının çalışma şekli aşağıda verilmiştir.

1) Kartın seri numarası okunur

2) Bu kartın seri numarasıyla bir açma (turn-on) paketi yaratılır

3) Bu açma paketi karta gönderilir

4) Kartın açıldığının doğruluğu kanıtlanır

Yukarıda verilmiş olan adımlar çok basitleştirilmiştir. Bu çalışma şekli için iskeleti DECOEM.C isimli C programlama dilinde yazılmış olan bir programdır. Bu program, bir VideoCrypt kod çözücüsünü emüle etmek amacıyla Markus Kuhn tarafından yazılmıştır. Bu işlemdeki sonraki adım, kart seri numarasını okumak için rutinler ile entegre etmek ve bunu geçerli bir açma paketiyle kodlamaktır.

Açma (turn-on) paketi sadece, belirli bir kanal veya bir grup kanal için bir akıllı kartı aktif hale getirecek bir değere sahip olan kart komut baytını içeren bir pakettir. Buna benzer olarak bir kapatma (turn-off) paketi, belirli bir kanalı veya bir grup kanalı kapatacak bir değere sahip olan komut baytını içeren pakettir.

Bütün bunların içindeki en önemli gereksinim, geçerli bir algoritmaya ve anahtarlar grubuna sahip olunmasıdır. Bu çalışma için gerekli olanların tamamı temel algoritma ve anahtarlardır. Dorchester kodu, bunun için kullanılmıştır. Fakat, News Datacom'un bu temel algoritmanın yeniden kullanılmasına izin vermiş olması tehlikeli bir hataydı. Televizyon kanallarının akıllı kartta açılmasını ve kapatılmasını sağlayan komutlar Çizelge 6.3'te verilmiştir.

Çizelge 6.5 Televizyon kanallarının akıllı kartta açılmasını sağlayan komutlar [1]

Komut	Görevi
00h	Akıllı karttaki bütün kanalları kapat
01h	Sky Movies kanalını kapat
02h	Movie Channel'ı kapat
03h	Sky Movies Gold kanalını kapat
06h	Sky Sport kanalını kapat
08h	TV Asia kanalını kapat
0Ch	Multichannels'ı kapat
20h	Akıllı karttaki bütün kanalları aktif hale getir
21h	Sky Movies kanalını aktif hale getir
22h	Movie Channels'ı aktif hale getir
23h	Sky Movies Gold kanalını aktif hale getir
26h	Sky Sport kanalını aktif hale getir
28h	TV Asia kanalını aktif hale getir
2Ch	Multichannels'ı aktif hale getir
40h	Görüntü başına ödeme (PPV) hesabı yönetimi
44h	Görüntü başına ödemeye yetki verilmesi

Çizelge 6.3'te verilmiş olan son iki komut, Sky 09 serisi karttaki görüntü başına ödeme olayları için kullanılmıştır. 44h komutu, Sky Sport kanalının görüntü başına ödemeli yayınlarını sadece halka açık yerlerde aktif hale getirmek için kullanılmıştır. Bu, 09 serisi karta geçildikten sonra Sky Channel'ın yapmış olduğu ilk görüntü başına ödeme denemesidir ve fiyatı çok yüksek olduğu için korsanlar tarafından hack edilmiştir.

6.1.11.10 Battery kartlar ile hack işlemi

PIC16C84 kartlarındaki güncelleme problemi ticari amaçlı korsanların işini engellemekteydi. Korsan kart müşterileri, televizyon kanalı yeni bir karşı tedbir uyguladıktan sonraki 2-3 hafta

sonra bu korsan kartı güncellemesi için satıcıya göndermekteydi.

Bu problem, battery kartlar çıktıktan sonra çözülmüştür. Bu kartlar, on yıldan uzun bir süredir mevcut olan bazı planların geliştirilmesinden ibarettir. Amerika'da, kodları ve anahtarları güncellemek için kullanılmış olan tuş takımı VideoCipher-II sistemindeki korsanlıkta geniş çaplı olarak kullanılmıştır.

Avrupa'da bu durum bundan biraz farklıydı. VideoCipher-II sisteminde yapılan tek şey aylık anahtarların güncellenmesiydi. Fakat VideoCrypt sisteminde bu durum daha karmaşıktı. Kartın kopyasının bölgelerinin veya emülatör programının çalışmasının modifiye edilmesi gerekliydi. Ayrıca bu durum, bu tür bir güncelleme prosedürünün bir akıllı kart üzerinde ilk defa kullanılasıydı. Ortaya çıkarılan aygıt, herhangi bir orijinal akıllı karttan daha gelişmişti.

Battery kart olarak bilinen bu yeni korsan kartın en önemli kısmı Dallas 5002FP mikrokontrolörüydü. Bu mikroçip, bu tarihe kadar çıkmış olan en güvenli mikrokontrolördü. Bu mikroçip, bir 8051 mikrokontrolörünü baz almaktadır.

Battery kart, kartın hafızasını desteklemek için bir Lityum bataryaya (pile) sahipti. İlk başta bu kart Pacemaker olarak adlandırılmıştır. Daha sonra bir batarya kullanmış olduğu için Battery Card tabiri kullanılmaya başlanmıştır. Bundan sonra, her Dallas mikroçipi bazlı kart için bu tabir kullanılmaya başlanmıştır.

Dallas 5002FP mikrokontrolörü, PIC16C84'ten daha pahalı olmasına rağmen güvenlik bakımından korsanlar için idealdi. Çünkü PIC16C84 mikrokontrolörü tamamen tehlikedeydi. Bu mikrokontrolörün çıkışı, korsanların daha güvenli bir mikrokontrolör kullanmaya yönelmesi için bir başlangıç olmuştur.

Battery kart, çok gerekli bir özelliğe sahip olduğu için önemlidir. Bu özellik, akıllı kartın güncellenmesi görevini korsan kart satıcısından alınmasıdır. Çünkü televizyon kanalı tarafından bir karşı tedbir gerçekleştirildiği zaman kart kullanıcıları, bu güncelleme kodunu karta tuş takımı üzerinden girebilmekteydi. Battery kartlara yeni güncelleme kodlarının girilmesi çok basit bir işti. Bu, herkesin kolayca kullanabileceği bir arabirimdi. Bu güncelleme kodları, ilgili internet sitelerinden veya BBS'lerden temin edilebilmekteydi.

Artık herhangi bir elektronik karşı tedbirin ömrü sadece birkaç dakikaya düşmüştü. Bu karşı tedbir uygulandıktan sonra kartların korsan kart satıcısına gönderilmesi prosedürü tamamen ortadan kalkmıştı. Bununla birlikte News Datacom, Battery kartlara karşı önemli başarılar kazanmıştır. Bu başarılardan bir tanesi, battery kart belleğinin bir kısmının üzerine yazmak

için kullanmış olduğu bir karşı tedbirdir. Bunun sonucunda kart kullanıcıları, korsan kartlarının yeniden programlanması için kartlarını satıcıya göndermek zorunda kalmıştır. Fakat bu tür olayların sayısı çok sınırlıdır ve korsanlar bu karşı tedbirlerin de üstesinden gelmiştir.

6.1.11.11 VideoCrypt Vampire hack işlemi

09 kartının çöküşünün nedeni bu kartta nanokomutların kullanılmış olmasıyla ilgilidir. Bilgisayar korsanlarının bu konudaki bilgisi artmış olduğu için nanokomutların uygulamaları anlaşılır hale gelmişti. Korsanların, havadan gelen paketleri gözden geçirmesi ve News Datacom ve Sky kanallarının bu komutları nasıl kullandığını izlemesi gerekliydi. Bu şekilde bu nanokomutların bir listesinin yapılması mümkündür. Bununla beraber, ticari amaçlı korsanlar farklı bir yol izledi. Bu korsanların büyük bir kısmı akıllı kartın içindeki bilgileri tamamen boşaltmış olduğu için sıradan korsanlara göre daha avantajlılardı. Çünkü sıradan korsanların bu paketlerin nasıl kullanıldığını anlamak için beklemesi ve görmesi gerekliydi.

News Datacom, akıllı kartın adres bölgesinin herhangi bir yerinden gelen bir baytın karma fonksiyona giriş olarak kullanılmasını mümkün hale getirebilirdi. Bu tür bir algoritma kullanılmasının bazı tehlikeleri mevcuttur. Bunun en önemli sebebi, algoritma tehlike altındayken bellek bölgesindeki bilgilerin boşaltılmasının mümkün olmasıydı. Bu, 09 kartında ve nanokomutlarda neler olduğunu açıklamaktadır.

Vampire hack, akıllı kartın en önemli noktası olan bellek bölgesinin elde edilmesini sağlamıştır. Bu hack işleminin diğer bir ismi Count Zero hack'idir. Bu hack işleminin bazı yönleri, Phoenix hack işlemi boyunca elde edilmiş olan bilgilerin ışığında geliştirilmiştir. Burada birçok benzer kaynak kodu kullanılmıştır.

Vampire hack işlemi için gerekli olan dört şey vardır. Bunlardan birincisi, karma fonksiyonun çalışan bir uygulamasıdır. Bu, cevap baytlarının konumunun bütün işlem boyunca izlenmesi gerektiği için önemlidir. Ayrıca karma fonksiyonu uygulaması, paket için geçerli bir karma imza üretmek için de gerekmektedir.

İkinci gereksinim, EXOR tablolarını üretmek için gerekli olan algoritmadır. Bu kodlar, kontrol işlemi üretilmeden önce paket verisi ile EXOR'lanmaktadır. Vampire hack işleminin ilk versiyonlarının bazılarında, EXOR tablosunun üretilmesi için gerekli olan bu algoritma mevcut değildi. Bu nedenle, o ay için gerekli olan bütün EXOR tablosu kaynak koduna dahil edilmiştir.

Üçüncü gereksinim, nanokomutların çalışma bilgisidir. Vampire hack işlemindeki temel komutlar 09h adres yükleyici komutu, 30h veri işlemci komutu ve 03h bitiş komutudur. fakat, herbir nanokomut tarafından kaç tane karma iterasyonunun gerçekleştirildiğinin bilinmesi gereklidir.

Dördüncü gereksinim, kurtarma rutininin birkaç tipidir. Bu rutin, 30h komutunda kullanılmış olan veri baytı için ayrıntılı olarak arama yapmaktadır. Bu belkide algoritmanın en yoğun bölümüdür ve korsanların büyük bir kısmı karttan sonuçlar elde edilinceye kadar bu aşamayla uğraşmamıştır.

Aşama 1: Nanokomut üretimi

Temel olarak bu aşama, 09h komutunu izleyen adres baytlarının gerçekleştirilmesini gerektirmektedir.

Aşama 2: Paket verisinin kodlanması

Bu aşama, nanokomut kod çözme anahtarı algoritmasının paket verisine uygulandığı yerdir. Bu, kodlama algoritmasının çıkışı ile nanokomutlar ve diğer verileri EXOR'lamaktadır.

Aşama 3: Karma imza üretimi

Karta verilmiş olan paketin, geçerli bir karma imzaya sahip olması gerekmektedir. Aksi taktirde kart bu paketi reddetmektedir. Ayrıca, karma fonksiyonun çalışan bir uygulaması gerekmektedir. Bu işlem, orijinal Phoenix programı ile birçok bakımdan birbirine benzemektedir.

Aşama 4: Karta gönderilmiş olan paket

Vampire hack işleminde kullanılmış olan paket karta gönderilmektedir. Bu aşama için kullanılmış olan devre yapısı Phoenix hack işleminde kullanılan ile aynıdır.

Aşama 5: Kaydedilmiş olan cevap paketi (78h)

Karttan gelen cevap paketi verinin adresi, kullanılmış olan nanokomutlar ve nanokomutların uygulanmasından hemen önceki cevap baytlarının durumu ile birlikte bir dosyaya kaydedilmektedir. Alternatif olarak bu işlem, sonraki bayta ilerlenmeden hemen önce uygulanabilmektedir.

Aşama 6: Veri kurtarma

Teorik olarak bu basit bir aşamadır. Fakat pratikte, bu biraz karmaşıktır. Nanokomutların

uygulanmasından önceki cevap baytlarının konumu bilinmektedir. Bundan dolayı, aynı sonuçları elde etmeyi denemek için karma fonksiyonun yinelenmesi ile veriyi bir dereceye kadar kurtarmak mümkündür. Burada kullanılmış olan işlem, ayrıntılı bir arama işlemidir. Hata yapılması ihtimali mevcuttur. Fakat bu, kart belleğinin içeriklerinin elde edilmesinin en basit yoludur.

Sky 09 kartının içeriğinin boşaltılması için en az üç farklı program mevcuttur. Bunların en yaygın olarak kullanılanlarından biri GETROM isimli programdır.

6.1.11.12 Megatek 10 Battery kartı ile hack işlemi

Televizyon kanalları tarafından 09 serisi kartlarda bir elektronik karşı tedbir gerçekleştirilmişti. Fakat bu, sıradan bir karşı tedbir değildi. Tarih kodu daha önce 51h iken 86h ile değiştirilmişti. Hiçbir Season programı bu yeni kodu düzeltemiyordu.

Daha güvenli mikrokontrolörler kullanılarak bu yeni kodun güvenli kalmasının sağlanması düşünülüyordu. Çünkü korsanların kendi aralarında da bir takım problemler mevcuttu. Bu sıralarda, içeriği okunamayan tek mikroçip Dallas Semiconductor 5002FP mikrokontrolörüydü. Bu yüzden Megatek, Cardtronics ve Benedex tarafından bu mikrokontrolör kullanılmıştı.

Kanalın yeni koda geçmesinden birkaç saat sonra Megatek firmasının internetteki web sayfasında, 31.10.1995 tarihinde Sky 10 kodunun kullanılmaya başlanacağı ilan edilmişti. Bu, Megatek'in battery kartlar için gerekli olan yeni kodu kısa bir süre sonra verebileceğini gösteriyordu. Çalışan ilk Megatek Battery kartı, 05.04.1996 tarihinde ortaya çıkmıştır. Artık Sky 10 serisi kart da hack edilmişti.

Sky 10 serisi kartta iki adet mikroçip mevcuttur. Bu, ilave padlerin olmasının sebebidir. Elektriksel olarak ISO uyumlu olan bu padler sadece, 10 serisi kartların mikroçiplerinin işgal ettiği daha büyük alanı karşılamaktaydı.

Bu mikroçiplerden bir tanesi Siemens akıllı kart mikrokontrolörüdür. Diğer ise uygulamaya özgü bir entegre devredir (ASIC). Bu ASIC, kartı ters mühendislik işlemlerinden geçirmek isteyen bir bilgisayar korsanı için problem çıkartmaktaydı. Bu mikrokontrolörün ters mühendislik işlemlerinden geçirilmesi, 10 serisi kartların Sky tarafından kullanılmaya başlanmasından önce tamamlanmıştır. Fakat ASIC'ın ters mühendislik işlemlerinden geçirilmesi biraz daha uzun sürmüştür.

Bu kart, bir Siemens mikrokontrolörünü baz almaktaydı ve bu mikroçip Dallas 5002FP ile birtakım ortak özelliklere sahipti. Siemens akıllı kartları ve Dallas 5002FP mikroçipinin her ikiside 8051 mimarisini ve çalışma kodlarını baz almaktadır. Dallas 5002FP mikrokontrolörü, güvenlik elemanları ile üstün olmasına rağmen Siemens mikroçiplerinde, komutların daha hızlı uygulanmasını sağlamak için bu mimari modifiye edilmiştir. Ayrıca bu mikroçipler 1.0 ile 7.8 MHz aralığında da çalışabilmektedir. Muhtemelen çalışma kodlarında da bazı değişiklikler yapılmıştı. Çünkü müşteriye özel mikrokontrolörlerde bazı komutların davranışlarının değiştirilmesi yaygın olarak yapulan bir taktiktir. Bu durum, bunların klasik bir mikrokontrolör ile emüle edilmesini daha karmaşık yapmaktadır. Çünkü akıllı karttaki bir komut korsan emülatörde iki veya üç komut olabilmekteydi.

VideoCrypt kod çözücülerindeki arabirimin clock hızı, reset cevabı (ATR) tarafından belirlenmekteydi. Bu, kart kod çözücüye yerleştirildiği zaman kart tarafından kod çözücüye geri gönderilen pakettir ve sürekli 3.5 MHz'lik bir clock hızındadır.

İlk önce ASIC çalışmakta, daha sonra ise seri veri hattı çalışmaktadır. Seri veri hattı, mikrokontrolöre akan veri için bir UART veya tampon gibi davranmaktadır. Bu şekilde mikrokontrolör, veriyi çok düzgün bir biçimde işleme tabi tutabiliyordu. Baytları işleme tabi tutmaya hazır olduğu zaman ASIC'ten baytları istiyordu. Bunun sonucunda çevrimler, 07 ve 09 serisi kartlarda kullanılmış olan algoritmalardan çok daha fazla karmaşık bir algoritmaya bağlıydı.

ASIC'in kullanılmış olması çekirdek üretimini sınırlamamıştır. Yetki verme ve yetki alma prosedürlerinin şiddetli olarak ASIC'e güvendiğine inanılmaktaydı. Bunun anlamı, 10 serisi kart için bir Phoenix arabiriminin düzenin bir parçası olarak çalışan bir Sky 10 ASIC'ine sahip olmasının gerektiğidir. Bu, daha önceden de bu kart ile çalışmış olan kişiler için zor değildir.

Eğer kartın mikrokontrolörü bir Siemens mikroçipi ise, doğru mikroçipin incelenmiş olması gerekmektedir. Kullanılabilecek dört mikrokontrolör vardır. Bunlar, Çizelge 6.6'da gösterilmiştir.

Çizelge 6.6 Sky 10 serisi akıllı kart için kullanılabilecek Siemens mikrokontrolörler [1]

Tip	ROM	EEPROM	RAM	PROM
SLE 44C10	8K	1K	256 bayt	32 bayt
SLE 44C40	8K	4K	256 bayt	32 bayt
SLE 44C80	16K	8K	256 bayt	32 bayt
SLE 44C200	8K	2.5K	256+350 bayt	32 bayt

Siemens'te, daha gelişmiş bir işlemci tipi de mevcuttur. Bu mikrokontrolör, RSA hesaplamalarını yönetmek için bir kripto işlemci içermektedir. Fakat bu, daha pahalı bir seçim olduğu için Sky tarafından kullanılmamıştır.

Bu seçenekleri daraltmayı denemek zor olmasına rağmen imkansız da değildir. Yeni bir kart için en belirgin tercih SLE 44C80 olacaktır. Bunun nedeni, SLE 44C40'ın 09 serisi kartta kullanılmış olan Motorola entegre devresine çok benzer olması ve SLE 44C200'ün çok pahalı olmasıdır.

Megatek battery kartı, Dallas 5002FP mikrokontrolörünü baz almaktadır. Bu mikrokontrolör, güvenlik bakımından en güçlü mikrokontrolörlerden biri olduğunu ispatlamıştır ve bunun içeriğinin okunması girişimlerinin büyük bir kısmı başarısız olmuştur. Bu durum, bu mikrokontrolörü içeriği kolayca okunabilen PIC16C84'ten kesinlikle ayırmaktadır. Fakat Dallas 5002FP bile Sky 10 kartını emüle etmek için yeterli değildir.

Sky 10 kartındaki ASIC, korsan 10 serisi kartların piyasaya çıkmasında gecikmeye yol açan başlıca faktörlerden biriydi. Bu ASIC bir 4500 kapı entegre devresidir. Hack işleminin çalışması için bu ASIC'in ters mühendislik işlemlerinden geçirilmesi ve emüle edilmesi şarttır. Megatek, Skylark mikroçipi ismini verdiği özel olarak geliştirilmiş bir entegre devreyi devre kartına monte etmişti.

Megatek'in Skylark mikroçipi, bir ACTEL A1280XL'dir. Bu, 8000 kapıya sahiptir. Bu mikroçipin teknik özellikleri ACTEL şirketinin web sayfasından temin edilebilmektedir. Megatek, bu entegre devrenin kimlik numarasını mikroçipin üzerinden silmişti. Bu, orijinal Sky ASIC'i ile büyük benzerliklere sahipti. Korsanlar, orijinal Sky kartının ASIC'ini kendi kartlarında kullanabilmekteydi.

Mevcut bir battery kartının güncellenmesi, Dallas 5002FP'nin yeniden programlanmasını da gerektirmektedir. Fakat bunun sonucunda, güncellenmiş olan bu kart artık D2-MAC EuroCrypt kanallarını düzeltemiyordu.

Daha sonra, mahkeme kararıyla Megatek şirketinin bu korsan kartları satması yasaklanmıştı. Fakat bu, kullanıcılardaki korsan 10 serisi kartların artık çalışmayacağı anlamına gelmiyordu. Ayrıca Cardtronics isimli şirket korsan piyasada Megatek'in yerini almış gibi görünüyordu.

News Datacom 05.08.1996 tarihinde battery kartlarını durdurmak için bir elektronik karşı tedbir gerçekleştirdi. Bu karşı tedbir etkili oldu ve Avrupa'daki bütün battery kartlarının çalışmasını engelledi. Fakat, Phoenix arabirimli korsan 10 serisi kartlar hala çalışmaktaydı.

Ayrıca, battery kartları için yeni güncelleme kodları kısa bir süre içinde hazılanabilmekteydi.

6.2 VideoCrypt-II Sistemi

VideoCrypt-II sistemi, sadece İngiltere ve İrlanda'da kullanılmış olan VideoCrypt-I sisteminin aksine Avrupa'da kullanılmak üzere geliştirilmiştir. Bu sistem, VideoCrypt-I sisteminin geliştirilmiş bir biçimidir ve teknolojisi ile kullanmış olduğu protokoller çoğunlukla aynıdır.

Bu sistemin geliştirilmesindeki en önemli sebep, büyüyen Avrupa pazarına hizmet vermekti. VideoCrypt-II sisteminin gücü, veri akışının eşzamanlı olarak bir VideoCrypt-I kodlanmış televizyon kanalı üzerinden taşınabilmesidir. Bu nedenle bir televizyon kanalı, değişik akıllı kartlar kullanarak iki lisans bölgesine yayın yapabilmekteydi.

VideoCrypt-II sistemi, VideoCrypt-I sistemi ile karşılaştırılırsa biraz faklı paket büyüklüklerine sahip olduğu görülmektedir. Bu durum, News Datacom'un VideoCrypt-I sisteminde Fiat-Shamir Sıfır Bilgi Testinin uygulanmasında karşılaştıkları problemlerin bazılarını çözdüğünü kanıtlamaktadır. Fiat-Shamir Sıfır Bilgi Testi, çekirdek üretiminde kullanılmıştır. Bunun sonucu, doğru çekirdek sonucunu elde etmek için karma fonksiyon çıkışı ile EXOR'lanmaktadır. Bundan dolayı, eğer Fiat-Shamir Sıfır Bilgi Testinin çalışma yöntemi korsanlar tarafından tamamen anlaşılamazsa, o zaman korsan kart karma fonksiyondan doğru sonucu üretse bile düzgün bir biçimde çalışmayacaktır.

Fiat-Shamir Sıfır Bilgi Testinin çekirdek üretimi ile bütünleştirilmesinden başka bir takım yararlı ilaveler de mevcuttu. VideoCrypt-II sisteminde kullanılmış olan kartın veri hızı 38.4 kbaud'dur. Bu oran, verinin daha yüksek bir hızda iletilmesini sağlamaktadır. Ayrıca bu, zamanlama daha kritik olduğu için korsan bir kartın geliştirilmesini çok zor hale gelirmektedir. Korsan kartlarda kullanılmış olan PIC16C84 mikrokontrolörü bir çarpma komutuna sahip değildi ve Fiat-Shamir Sıfır Bilgi Testi, bu gibi birçok hesaplamayı kapsadığı için bu durumdan faydalanılmıştı. Bu nedenle, orijinal kartlardaki Fiat-Shamir Sıfır Bilgi Testi rutinleri daha hızlı olacaktı.

VideoCrypt-II sisteminde gerçekleştirilmiş olan hack işlemlerinin büyük bir kısmı Battery kart bazlıdır. Bununla birlikte, PIC16C84 bazlı hack işlemleri de gerçekleştirilmiştir. Fakat PIC16C84'teki programın boşaltılmasını durdurma girişiminde, seri programlama prosedüründe gerekli olan pinlerden birinin entegre devre kılıfının matkap ile delindikten sonra hat kesilerek ayrılması gerekmektedir. Bu işlem, elektronikten anlayan kişiler için mikroçipin üst kısmının çıkarılması ve pinin iyi bir havya ile yeniden lehimlenmesi işi kadar

kolaydır. Bu durum, VideoCrypt-II sistemindeki PIC16C84 mikroçipinin içeriğinin korsanlar tarafından nasıl okunduğunu göstermektedir.

VideoCrypt-II sistemi, farklı bir anahtar grubuna sahip olan bir Sky 07 algoritması kullanmaktadır. Bu işlemde Fiat-Shamir Sıfır Bilgi Testinin kullanılması, anahtar grubunun yeniden elde edilmesinde alışılmış kriptografik yaklaşımın işe yaramayacağı anlamına gelmektedir. Çünkü Fiat-Shamir Sıfır Bilgi Testinin sonucunun, çekirdeği denklemden çıkarmak için buna ters yönde EXOR'lanması gerekmektedir. Eğer bunu yapmak için veri grupları bilinmiş olsaydı, o zaman bu anahtarı yeniden elde etmeyi denemek için hiçbir sebep olmayacaktı.

VideoCrypt-I ve VideoCrypt-II sistemi arasındaki en önemli farklılık paket boyutlarıdır. VideoCrypt-II sistemindeki 72h ve 7Ch paketleri 64 bayt (40h) uzunluğundadır. Bu, VideoCrypt-I sistemindeki paket uzunlukları ile kıyaslandığında burada ilave bir doğruluk kanıtlama ve sıralama düzeyi olduğunu göstermektedir.

6.3 VideoCrypt-S sistemi

VideoCrypt-S sistemi News Datacom, Thomson ve BBC tarafından geliştirilmiştir. Bu sistemin ilk kullanıcısı BBS Select servisiydi. Bu, belirli bir saatten sonra yayına geçen bir ödemeli televizyon servisiydi. Televizyon programlarının yayınlandığı zaman aralığı başlıbaşına bir problemdi. Çünkü asıl kanalın yayını bittikten sonra BBS Select servisi yayına başlıyordu ve bu saat pek çok izyelici için çok geç bir saatti.

Karıştırıcılardaki kes ve yer değiştir tekniği de problemliydi. Büyük çaplı kablolu televizyon servislerinde sinyal, ilk önce demodüle edilmekte ve sonra tekrar modüle edilerek dağıtım için dönüştürülmektedir.

Kes ve yer değiştir tekniğini kullanan bir sisteminin zayıf noktası oluşan eğimdir (tilt). Bu eğim, düzeltilmiş sinyaldeki birleşme noktalarının birbirine tam olarak uymadığı zaman oluşmaktadır. Bunun sonucunda, birçok düşük frekans gürültüsü oluşmaktadır. Bir kablolu sistemdeki non-lineerlik, bu eğim problemini vurgulamaktadır. VideoCrypt sisteminde bu problemin üstesinden gelinmiştir ve uydu iletimindeki sinyaller oldukça temizdir. Bir kablolu sistemde, bu sinyal ortamı kontrol altındadır. En önemli kuvvetlendiriciler, kazanç kontrollü olduğu kadar da sıcaklık kontrollüdür.

VideoCrypt sisteminde çalışmış olan hack işlemlerinin bazıları VideoCrypt-S sisteminde de çalışmaktadır. Burada, eğer aynı tür bir kart kullanılmışsa EPROM kart okuma gerilimi hack

işlemi çalışacaktır. 8052 idareyi sağlayan mikrokontrolöründeki programların büyük bir kısmı sıradan bir VideoCrypt kod çözücüsündekiyle aynı olduğu için bu hack işlemi muhtemelen çalışacaktır.

Satır karıştırma, bir satır bloğunun sırasının değiştirilmesidir. Karıştırılmış sırada, birinci satır onuncu satır haline gelebilmektedir. Daha sonra bu satırlar, gerçek sıralarına geri çevrilmektedir. Bu işlem basit gibi görünsede aslında oldukça karmaşıktır.

VideoCrypt-S sistemi, blokların karıştırılmasını baz almaktadır. Herbir blok, alan başına 6 blok olmak üzere 47 satırdır. Herbir alandaki diğer satırlar teletekst, VBI ve erişim kontrol verisi için ayrılmaktadır.

Üç farklı karıştırıcı modu mevcuttur. Bunlar;

- 282 satırın tamamen karıştırılması
- Kısmen karıştırma (Diğer alanların hepsi karıştırılmıştır.)
- Temiz video (blok) geciktirmesi

Tamamen karıştırma ve kısmen karıştırma, gerçekten görüntüyü mahvetmektedir. Blok geciktirme, Discret sisteminde görüleceği gibi güvenli değildir. Bu modların hepsi aynı anda kullanıldığı zaman görüntü üzerindeki sonuç etkileyicidir. Temiz blok geciktirme, bloğun ana hatlarını çıkarabilir ve analiz edilmesini kolaylaştırır.

Bu sistemin erişim kontrol sistemi, VideoCrypt sistemindeki gibi akıllı kart bazlıdır. Bu karıştırıcı, bir permütasyon üreteci ile yönetilmektedir. Bu üreteç için çekirdek, kodlanmış biçimde havadan iletilmekte olan veriden elde edilen 20 bitlik bir sözcüktür.

Akıllı kart; yetki verme verisini, kullanıcı profilini ve havadan gönderilen veriyi düzeltmek için gerekli olan kod çözme algoritmasını tutmaktadır. Bu bakımdan akıllı kart, sıradan bir VideoCrypt akıllı kartı ile aynıdır.

VideoCrypt-S ve VideoCrypt sistemleri arasındaki temel farklılık, karıştırıcı tekniğin türüdür. VideoCrypt-S sistemi, satır karıştırma kullanır ve bu yüzden daha büyük bir RAM gerektirir. Bu karıştırma, bir ASIC ile yönetilmektedir. Bu ASIC, Thomson tarafından geliştirilmiştir.

Bu sistemin orijinal dökümantasyonuna göre bu sistemin merkezi bu ASIC'tir. Bu ASIC veri elde edilmesini, bellek tahsis edilmesini ve permütasyon üretimini yönetmektedir. Bu veri, düşey karartma aralığı satırlarından elde edilmektedir ve işlenmektedir. Daha sonra bu veri, kod çözücü mikrokontrolör yolunu (bus) beslemektedir.

VideoCrypt-S sisteminin kod çözücüsündeki idareyi sağlayan mikrokontrolör bir 8052'dir. Bu

mikrokontrolördeki program korumasızdır ve sıradan bir VideoCrypt kod çözücüsündeki 8052'den farklı değildir. Video analog-dijital konverteri ve video dijital-analog konverteri aşamaları da sıradan bir VideoCrypt kod çözücüsündekiler ile aynıdır.

6.4 Cryptovision Sistemi

Cryptovision sistemi uydu üzerinden yayın yapan kanallarda geniş çapta kullanılmamasına rağmen, Avrupa'daki kablolu televizyon kanallarında yaygın olarak kullanılmış olan bir dijital karıştırıcı sistemdir.

Bu sistem, seksenli yılların sonunda güvenli bir karıştırıcı sistem olarak geliştirildiğinde dijital video tekniklerinin üstünlüğüne sahipti. Bu dönemdeki pek çok sistemden farklı olarak bu sistem, geniş çapta korsanlığa maruz kalmamıştır. Bunun başlıca sebebi, erişim kontrol sisteminin oldukça güvenli olarak tasarlanmış olması ve prim yapan uydu televizyon programlarında kullanılmamış olmasıdır. Bununla birlikte, içine yerleştirilmiş güvenli mikrokontrolör yaklaşımını kullanmış olduğu için muhtemelen çok güçlü bir saldırıya karşı koyamayacaktı.

Bu sistem Tandberg tarafından imal edilmiştir. Tandberg, uzun bir süre ödemeli televizyon sistemleri ile ortak çalıştı ve bu firma, ilk MAC kodlayıcılarını ve kod çözücülerini kullananlardan biriydi. Daha yeni kod çözücü modelleri PACE firması tarafından üretilmektedir.

Bu sistem hala Intelsat uydusu üzerinden 27.5 Derece Batı'dan yayın yapmakta olan British Services Channel tarafından kullanılmaktadır. İlk bakışta herkes bu kanalın VideoCrypt sistemini kullandığını zannetmişti. Bu yanılgı, bu sistemin erişim kontrol sisteminin tamamen farklı olmasına rağmen VideoCrypt sistemindeki ile benzer temel teknikler kullandığı için ortaya çıkmıştır.

Cryptovision sisteminde kullanılmış olan video karıştırıcı teknik, kes ve yer değiştir tekniğidir. Video satırı parçalara ayrılmıştır ve kesilmiştir. Daha sonra bu kesme noktası etrafında bu parçalar yer değiştirmiştir. Örnekleme oranı VideoCrypt sisteminden daha yüksektir ve bunun sonucunda, düzeltilmiş görüntünün kalitesi biraz daha iyidir.

Herbir satırdaki bu kesme noktası etkili bir şekilde maskelenmiştir (masked). Bundan dolayı bu noktada transiyent yoktur. VideoCrypt sisteminin hack edilmesindeki ilk denemelerden biri, bu kesme noktasını vurgulamak için bir indüktör kullanmıştır. Maskeleme yapılarak bu kesme noktası ortadan kaldırılıyordu. Görünüşe göre bu maskeleme işlemi, örnek

pencerelerinin (windows) gerekenden daha uzun olduğu yerlerde aşırı örneklemenin bir biçimini gerektirmektedir.

Bu sistemin teknik özellik dökümanlarına göre, Digit 2000 serisi analog-dijital konverterler ve dijital-analog konverterler kullanılmıştı. Fakat pratikte bu sistemde TDA8702 ve TDA8703 entegre devrelerinin kullanılmış olduğu düşünülmektedir. Örnekleme frekansı 17.73 MHz veya PAL renk alt taşıyıcısı frekansının dört katıdır. Bu, geliştirilmiş bir görüntü kalitesi vermektedir.

VideoCrypt sisteminde olduğu gibi bu sistemde de, herbir satırda 256 kesme noktası vardır. Bu, 921 örneğin bir toplamından gelmektedir. Örneklerin bazıları kullanılmamaktadır. Bu durum, karıştırılmış videodaki kesme noktalarının tespit edilmesini zorlaştırmaktadır.

Erişim kontrol sistemi esnek olarak tasarlandığı için havadan adreslemeden akıllı kartlara kadar bir takım metotları destekleyebilmektedir. İrlanda'da kullanılmış olan sistem, içine yerleştirilmiş güvenli mikrokontrolör ile havadan adresleme kontrolü kullanmaktaydı.

Bu sistemde kullanılmış olan mikrokontrolör bir 8051'di. Bu mikroçipin içeriğinin okunabilmesi için pekçok hack işlemi mevcuttu. Fakat bu sıralarda, orijinal kod çözücüyü modifiye etme riskini göze alacak kadar fazla sayıda kod çözücü yoktu. Ayrıca İrlanda'da, kablolu televizyon ve MMDS korsanlığı oldukça ciddi bir suçtur ve bir orijinal kod çözücüyü modifiye eden bir kişi yakalanırsa çok büyük para cezalarına çarptırılmaktadır.

Kod çözücülerin bazıları bir EEPROM'a sahiptir. O zamanlarda bu EEPROM'un sıralama ve abone numarası gibi herhangi bir erişim kontrol verisini kontrol altında tuttuğu bilinmiyordu. Eğer bu gibi verileri tuttuğu bilinseydi, o zaman bu yaklaşımda bir hack etme ihtimali mevcut olabilecekti. Ayrıca bu, kesme noktası maskelemek için gerekli olan veriyi kaydırma yazmaçlarında tutabilmektedir.

Kullanımda olan bu kod çözücüler, asıl güvenli mikrokontrolörleri olarak bir 68301'i de diğerine ilaveten kullanmaktadır. Yani kod çözücü, tipik bir ikili mikrokontrolör yaklaşımı kullanmaktadır. Bununla birlikte bu mikroçip, 68705 ve 68HC11 kadar güvenli olmayabilmektedir. Ayrıca, güvenli olduğu iddia edilen bu mikrokontrolörler bile hack edilmiştir.

Kod çözücünün hangi mikrokontrolörleri kullanmış olduğu konusundaki karışık durum, piyasada iki farklı kod çözücü tasarımı olduğuna bağlanmaktadır. Orijinal tasarım İrlanda'da üretilmiştir. Daha sonraki tasarım ise PACE firması tarafından üretilmiştir.

Düşey karartma aralığı, gerekli kripto veriyi ve onaylama düzeylerini kodlanmış bir formatta taşımaktadır. Bu veri, görünüş olarak teletekst ile aynı olsa bile teletekst satırlarını kullanmaz. Teletekste benzer bir veri formatının kullanımı, ucuz teletekst entegre devrelerinin kullanımına imkan tanımaktadır.

Headend kullanan kanalların, havadan gönderilen sinyaller ile kod çözücüleri açılması mümkündür. Bu özellik, bir sistemdeki korsanlığı çok zor hale getirse de imkansız hale getirmemektedir. Havadan gönderilen veriyi kodlamak için hangi kripto sistemin kullanılmış olduğu tam anlamıyla bilinmemektedir. Bu kripto sistem muhtemelen bir DES varyantıdır. Amerika'da kullanılmış olan VideoCipher sisteminde DES algoritması kullanılmıştı. Bu algoritmanın ters mühendislik işlemi başarısız olmuştur. Bilgisayar korsanları hack işleminde, bu sistemin erişim kontrol bölümündeki zayıf bir bağlantıyı kullanılmıştır. Fakat Cryptovision, VideoCipher sisteminde gerçekleştirilmiş olan bu hack işlemlerini incelemişti ve kendi sistemini bu tür hack işlemlerine karşı kuvvetlendirmişti.

Hack etme tekniklerindeki ilerlemeler ve son birkaç yılın bilgi birikimi, bu sistem için de bir risk oluşturmaktaydı. İçine yerleştirilmiş güvenli mikrokontrolör prensibine duyulan güven tamamen sarsılmıştı. Bu sistemde gerçekleştirilecek bir hack işlemi çok ciddi bir tehlikeydi. Çünkü bunun sonucunda, piyasadaki bütün orijinal kod çözücülerin güncellenmesi gerekecekti.

Bu sistemde meydana gelebilecek yaygın bir hack işleminin, sistemin erişim kontrol verisinin modifiye edilmesini baz alması gereklidir. Video karıştırıcı sistem, güvenli kalmak için yeterince esnek olduğu için en az birkaç yıl daha güvenli kalabilirdi.

Kablolu bazlı karıştırıcı sistemler süratle geliştirilmediği için bu sistemin güvenliği de tehlikeye altındaydı. Çünkü kablolu televizyon sistemlerinde kullanılmış olan teknoloji değişmeden kalıyorken korsanların teknolojisi hızla ilerlemekteydi. En sonunda Cablelink ve Cryptovision sistemini kullanan diğer kanallar bu konudaki yasalara güvenmek zorunda kalmışlardır.

Cryptovision kod çözücülerinde, şu ana kadar kullanılmamışta olsa bir ses karıştırıcı özelliği mevcuttur. Görünüşe göre burada birkaç seçenek mevcuttu ve kodlanmış uyarlanabilir delta modülasyonu, kodlanmış NICAM ve spektrum inversiyonundan söz edilmekteydi.

Bir ses karıştırıcının kullanımı, kod çözücü başına maliyeti çok arttırmaktadır. Böyle bir fiyat artışı, Cryptovision sistemini kullanmak isteyen küçük çaplı kablolu televizyon çirketleri için cazip değildir. Bu yüzden, bu sistemin standart uygulanma şekli sadece videonun

karıştırılmasından ibarettir.

6.5 Digicrypt Sistemi

Digicrypt sistemi, Sat-Tel VideoCode sistemi olarak kullanılmıştır. DCE firması, Sat-Tel firmasının işini devralmıştır. VideoCode, bu firmanın en önemli geliştirmelerden biriydi. Bu sistem, Zenith ve Sat-Tel/DCE firmalar tarafından ortak geliştirilmiştir. Zenith, havadan erişim kontrol sistemini, Sat-Tel ise yazılım ve donanımı geliştirmiştir. Bu sistemin hala geliştirildiğine dair herhangi bir bilgi yoktur.

Digicrypt sisteminde video karıştırıcı için satır geciktirme ve satır karıştırma olmak üzere iki teknik kullanılmıştır. Kullanılmış olan satır gecikmesi, tek birimlik bir gecikmedir. DCE firması tarafından yayınlanmış olan Digicrypt tanıtım dökümanlarında bu özellikten bahsedilmemiştir. Bunun sebebi, bu özelliğin kullanılmamış olması veya bunun yedek bir özellik olmasıdır.

Kullanılmış olan satır karıştırma, 32 satır karıştırma veya 128 satır karıştırmadır. Satır sayısı bu kadar az olduğu için karıştırma türü muhtemelen kayan çubuk tipidir.

Video kod çözücü mimarisi, satır karıştırma bazlı diğer kod çözücülerin büyük bir kısmı ile benzerdir. Bunun temel farklılığı, erişim kontrol bölümündedir. Bu bölüm, Zenith tarafından geliştirilmiştir ve havadan kapatılabilir bir modül içermektedir.

Kullanılmış olan ses karıştırıcı, BBC kanalının kullanmış olduğu SAVE sistemindekiyle aynıydı. Daha sonra Sat-Tel bu düzelticileri üretmeye başladı ve ses karıştırıcı da Sat-Tel tarafından geliştirildi.

Ses karıştırıcı sistem, yukarı doğru olan bir spektrum kaydırmasıdır. Bu spektrum kaydırma, 170 Hz ile 3.1 KHz arasında değişmektedir. Ayrıca bu AudioCode sistemi, 12 farklı frekans kaydırması yapabilmekteydi.

Digicrypt tarafından kullanılmış olan erişim kontrol sistemi, havadan gönderilen bir tipti. Adresleme verisinin iletilmesi için düşey karartma aralığının dört satırı kullanılmıştır. Bu sistem, dakikada 9000'den fazla kod çözücüyü adresleyebiliyordu.

Bir sistemde adreslenebilecek kod çözücülerin sayısı 16.7 milyondur. Dizi yapısı 256 düzey genişliğindedir. Video karıştırıcı, hack edilemeyecek kadar güvenlidir ve kesinlikle bu sistemin zayıf noktası değildir. Bu sistemin zayıf noktası, erişim kontrol sistemidir. Devre yapısının büyük bir bölümüne böyle bir hack işlemine karşı tedbir olması için ASIC dahil

edilmiştir.

6.6 Nagra Kudelski Syster Sistemi

Bu sistem, tamamen hack edilmiş olan Discret sisteminin yerini alması için geliştirilmiştir. Avrupa'daki en büyük kanal ağını Canal Plus yönetiyordu. Bu kanalın sadece Fransa'da üç milyonun üzerinde abonesi vardı [1].

Asıl karıştırıcı sistem İsviçre'de Nagra Kudelski tarafından yaratılmıştır. Kod çözücüler ise Eurodec tarafından üretilmiştir. Daha sonra Eurodec, Canal Plus ve Sagem tarafından satın alınmıştır.

Bilgisayar korsanlarının büyük bir bölümü bu sistemi Nagra Kudelski Syster sistemi, Nagravision sistemi veya sadece Nagra olarak bilmektedir. Syster tabirinin kökeni Fransızcada SYSteme TERrestrial'a karşılık gelmektedir. Bu sistem şu an, uydu üzerinden yayın yapan kanallar tarafından kullanılmaktadır ve çoğunlukla Nagra olarak isimlendirilmektedir.

Bugüne kadar bu sistem Canal Plus, Premiere, Canal Plus Espanga ve Teleclub tarafından kullanılmıştır [1]. Ayrıca bu sistemi Fransa'da kullanmış olan Canal Plus, bu sistemi Avrupa'da en yaygın olarak kullanılan sistem yapmıştır.

Diğer sistemlerden farklı olarak, alıcı ile bütünleşik kod çözücülerde (IRD) bir kıtlık başgöstermişti. Gerçektende Syster sistemi için piyasada hiç IRD yoktu. Ayrıca, orijinal kod çözücülerin dağıtımı da kontrol altında tutulmaktaydı. Bu, Syster sisteminin sahip olduğu en büyük güçtür. Çünkü bu, televizyon kanalının sistem üzerindeki kontrolünü korumasını sağlamaktadır. Eğer IRD'lerin satılmasına izin verilmiş olsaydı, bu kanal sistem üzerindeki kontrolünü kaybedecek ve korsan piyasa büyük bir problem haline gelecekti. Bu durumun en iyi örneği, VideoCrypt sisteminde gerçekleştirilmiş olan korsanlık olaylarıdır.

Video karıştırıcı, Nagra sisteminin asıl gücüdür. Bu, karıştırıcı metod olarak satır karıştırma kullanmaktadır. Satır karıştırma tekniğinin iki formu vardır. Bunlar sabit form ve kayan çubuk formudur.

Birinci form olan sabit (fixed) formda alan, aynı satır sayısına sahip birkaç çubuğa ayrılmaktadır. Karıştırma işi, bu çubukların sınırları içinde gerçekleşmektedir.

İkinci form olan kayan çubuk (sliding bar) formu öncekinden daha güvenlidir. Çubukların herbir alanda sabit konumlarda bulunmasının yerine, bu çubukların konumu alandan alana

değişiklik göstermektedir. Bu durum, alanları örnekleyen ve karşılaştıran korelasyon hack işleminin başarı şansını azaltmaktadır.

Video düzeltici işlemi, çoğu satır karıştırıcı sistemde olduğu gibi ASIC bazlıdır. Bu ASIC, bu zamana kadar kod çözücülerde kullanılmış olan en karmaşık ASIC'lerden biridir. Çünkü bu ASIC henüz ters mühendislik işleminden geçirilememiştir.

Video düzeltici, bir TDA8708 video analog-dijital konverterini ve bir TDA8702 dijital-analog konverterini baz almaktadır. Asıl düzeltme işlemi, bu ASIC tarafından yönetilmektedir.

Havadan gelen olan video sinyali filitrelenmekte ve bu analog-dijital konverteri beslemeden önce kenetlenmektedir (clamp). Daha sonra bu dijital karıştırılmış video ASIC'i beslemektedir ve bu ASIC karıştırılmış dijital videoyu RAM'de depolamaktadır. Daha sonra bu ASIC, RAM'in video çıkışını doğru sırada, analog hale geri çevrildiği ve kod çözücünün SCART soketine gönderilmeden önce filtrelendiği dijital-analog konverter şeridine (strip) clock'lamaktadır.

Syster sistemindeki erişim kontrol sistemi ikili (dual) bir sistemdir. Bu sistem, havadan adreslemeyi akıllı kart veya daha doğrusu akıllı anahtara ilaveten kullanmaktadır. Ayrılabilir güvenli mikrokontrolörün taşıyıcısı bir anahtar biçimindedir. Syster sisteminin tanıtım kitapçığında bu, anahtar olarak isimlendirilmiştir.

Bu anahtar, havadan yeniden programlanabilmekte ve aboneye yetki verildiği zaman başlangıç durumuna gelmektedir. Bütün Syster kod çözücülerine havadan yetki verilmesi gereklidir. Bunun için abonenin, abone yönetim merkezini telefonla arayarak kod çözücüsüne yetki verilmesini istemesi gerekmektedir.

Havadan adresleme, düşey karartma aralığında taşınmaktadır. Bu, 4 MHz bölgesinde hızlı bir veri clock'una sahiptir. Bu clock, sisteme seri bir abone güncelleme hızı vermektedir.

Anahtarın, kod çözücünün içindeyken güncellenmesinin gereki olması kod çözücünün işine abonenin kimlik kodunun yerleştirilmiş olduğunu göstermektedir. Bu kod, anahtar karşılaştırmasını sağlamakta ve telif hakları bölgesi dışına çıkartılmış olan yetki verilmiş herhangi bir kod çözücünün bulunmasını sağlamaktadır.

Nagra anahtarında kullanılmış olan mikrokontrolör ST16F44 serisi bir akıllı kart mikrokontrolörüdür. Bu mikrokontrolör oldukça eskidir ve ters mühendislik işleminden geçirilmeye müsaittir.

Nagra sisteminin kanıtlamış olduğu en önemli şey güvenli bir sistem sağlanması için kod çözücülere erişimin kontrol altında tutulmasının gerekli olduğudur. Kod çözücülerini kontrolsüz olarak pazarlamış olan D2-MAC EuroCrypt ve VideoCrypt sistemlerinde korsanlık, kaçınılmaz son olarak gerçekleşmiştir. Fakat bütün bunlara rağmen Nagra sisteminin hack edilmesi engellenememiştir. Bu hack işlemi direkt olarak video karıştırıcı tekniğinde gerçekleşmiştir. Korsan Nagra SECAM kod çözücü tasarımları ve programları, uydu televizyonu ile ilgili internet sitelerinde ve BBS'lerde mevcuttur.

6.6.1 Nagravision video karıştırıcı metodunun analizi

Kudelski Nagravision isimli ödemeli televizyon kanallarının kullandığı koşullu erişim sistemi, tipik televizyon görüntülerinin istatistiksel özelliklerini baz alan bir alanın satırlarını yeniden düzenleyen görüntü işleme algoritmaları ile uygun şekilde kırılabilmektedir. Karıştırıcı donanımın sınırlamaları hakkında biraz bilgiye sahip olarak abone akıllı kartında depolanmış olan kriptografik sırlar bilinmeksizin karıştırılmış bir televizyon görüntüsünün çözülmesi mümkündür [2].

Ödemeli televizyon kanalları, yaptıkları yayınları sadece abonelik ücretini ödeyen ve bir kod çözücüye sahip olan televizyon izleyicilerinin seyredebilmesini sağlamak için koşullu erişim sistemlerini kullanmaktadır [2]. PAL televizyon standandardı Nagravision koşullu erişim sistemi, İsviçre'de Kudelski SA şirketi tarafından geliştirilmiştir. Nagravision karıştırıcı sistemini Premiere (Almanya), Teleclub (İsviçre), Canal Plus (Fransa, İspanya) ve Cinemania (İspanya) isimli ödemeli televizyon kanalları başta olmak üzere pekçok kanal kullanmaktadır [2].

Nagravision sistemi, EuroCrypt ve VideoCrypt gibi diğer hibrit video karıştırıcı sistemlerde de olduğu gibi analog bir televizyon sinyalinin düzeltilmesini kontrol etmek için kod çözücüye radyo arabirimi üzerinden dijital olarak kodlanmış bir kontrol sözcüğü göndermektedir. Bu kontrol sözcüğünün kodu bir akıllı kartın içinde çözülmekte ve bir rasgele sayı üreteci için çekirdek değerine dönüştürülmektedir. Daha sonra bu rasgele sayı üreteci sonraki birkaç saniye için görüntü düzeltme işlemini kontrol etmektedir. Nagravision sisteminde, bir alan içerisindeki satırların yerleri değiştirilerek video sinyali karıştırılmaktadır. Ayrıca, ses spektrumunu tanınmaması için 12.8 kHz'lik bir sinüs dalgası taşıyıcısı ile karıştırarak tersine çevirmektedir. Bu ses sinyali, herhangi bir kriptografik mekanizmayla korunmadığı için sadece bir saniyelik süredeki spektrumunun tersine çevrilmesiyle düzeltilebilmektedir.

Analog biçimde iletilmekte olan bir video sinyalinin karıştırılmasını dijital olarak kontrol eden bütün hibrit karıştırıcı sistemlerde olduğu gibi bu sistemde de, orijinal bir kod çözücü veya akıllı kart kullanmaksızın video sinyalininin düzeltilmesi için iki farklı teknik mevcuttur. Bu teknikler;

- Akıllı kartın kod çözme algoritmasının ve gizli anahtar verisinin çıkartılması için mikroelektronik test etme teçhizatı kullanılabilmekte ve elde edilen bu bilgilerle uygun korsan akıllı kartlar ve kod çözücüler imal edilebilmektedir.

- Televizyon sinyallerinin tipik özellikleri, daha sonra görüntünün tamamını yüksek kalitede düzeltmek için kullanılmakta olan orijinal görüntüyü veya düzelticiyi kontrol eden rasgele sayı çekirdek değerini yeniden kurmak için kullanılabilmektedir. Bu teknik, sistemin dijital kriptografi veya akıllı kart güvenlik yaklaşımlarının kırılmasını gereksiz hale getirmektedir. Ayrıca bu teknik, herhangi bir orijinal kod çözücü donanımı kullanılmaksızın gerçekleştirilebilmektedir.

6.6.1.1 Video karıştırıcının analizi

B, G/PAL televizyon standardı, saniyede 25 resim (frame) göstermektedir [2]. Herbir resim, birbirine geçmeli iki alanın bir dizisi olarak gösterildiği için ekrandaki görüntü saniyede 50 alanlık bir oran ile güncelleştirilmektedir. B, G/PAL standardında, satır başına 64 μs ayrılarak saniyede 15625 satır gösterilmektedir. Bu satır aralığının yaklaşık 52 μs'lik kısmı aktif satır içeriğini kapsamaktadır. Geriye kalan yaklaşık 12 μs'lik süre ise 1.55 μs'lik bir satır önü boşluğu (front porch), 4.7 μs'lik bir senkronizasyon darbesi ve 5.8 μs'lik bir satır arkası boşluğu (back porch) içeren yatay karartma aralığıdır. 1/25 saniyede resim başına iletilmekte olan 15625 / 25 = 625 nominal satır, herbiri bir alanın $288 = 2^9 + 2^6$ görülebilir satırını içeren 23-310 ve 336-623 resim satır sayısı aralığındadır. Bu bölümde, tek bir görülebilir alan içersindeki satırlardan bahsedilmektedir ve bu satırlara karşılık gelen 0 ile 287 arasında değişmekte olan alan satır sayıları kullanılmaktadır. Bir resmin geriye kalan 625 - (2 x 288) = 49 satırı, görülebilir bir görüntü sinyali içermemektedir ve bu 49 satır, düşey karartma aralıklarını oluşturmaktadır. Bunlar, düşey senkronizasyon darbesi ve videotekst ve koşullu erişim sistemleri için kontrol sinyalleri gibi dijital olarak iletilmekte olan veriler için kullanılmaktadır.

Nagravision karıştırıcı sistemi, bir alan içersindeki satırların sırasını değiştirerek görüntüyü karıştırmaktadır. Buna ilaveten alanların arasındaki sınırlar, karıştırılmış ve düzeltilmiş

görüntü arasında 32 satır ile kaydırılmaktadır. Herhangi bir alanın 287'inci satırı, Nagravision karıştırıcı sistemi tarafından kullanılmamaktadır. Karıştırılmış bir alanın son 32 satırı (255-286 arası alan satırları) ve bunun ardından gelen alanın ilk 255 satırı (0-254 arası alan satırları), sırası değiştirilmekte olan 287 satırın bir grubunu oluşturmaktadır ve daha sonra düzeltilmiş sinyaldeki tek bir alanı oluşturmak için birlikte kullanılmaktadır. Kod çözücü, karıştırılmış alanın 33'üncü satırını aldığı zaman düzeltilmiş alanın birinci satırını göndermektedir. Bu, (6.3)'teki satır karıştırma permütasyon fonksiyonu ile tanımlanabilir.

$$p : \{0,..., 286\} \rightarrow \{-32,..., 254\} \tag{6.3}$$

Bu fonksiyonun anlamı, temiz görüntüden gelen i alan satırının karıştırılmış görüntüde $p(i)$ alan satırı olarak görünmekte olduğudur. Negatif bir $p(i)$ alan satır sayısı, önceki alandaki $287 + p(i)$ alan satır sayısına işaret etmektedir. (6.4)'teki satır düzeltme permütasyon fonksiyonu, satır karıştırma permütasyon fonksiyonunun (6.3) sadece ters fonksiyonudur.

$$p^{-1} : \{-32,..., 254\} \rightarrow \{0,..., 286\} \tag{6.4}$$

Bu yüzden, karıştırılmış alandaki $-32 \leq j \leq 254$ satırı düzeltilmiş sinyalde $p^{-1}(j)$ satırı olarak bulunmaktadır. Satır arkası boşluğundaki 4.43 MHz'lik PAL renk patlaması sinyalinin sırası değiştirilmemektedir. Fakat Nagravision sisteminin SECAM (Sequentiel à Memoire) varyantında satır arkası boşluğundaki modüle edilmemiş 4.406 MHz veya 4.250 MHz renk alt taşıyıcısının, satırın geri kalan kısmı ile birlikte sırası değiştirilmektedir.

Nagravision sistemi düzeltilmiş sinyalde bir alan oluşturacak olan 287 satırın sırasını, RAM'in 32 satırını tamponlayarak ve bu tamponun içindeki ve dışındaki satırları yalancı rasgele bir sırada yazarak ve okuyarak değiştirmektedir. Bu 32 tampon satır $B_0,...,B_{31}$ olarak düşünülebilir. Alan satır sayısı i alındığı zaman $B_{v(i)}$ tamponunun içeriği düzeltilmiş sinyal olarak gönderilmekte ve daha sonra, gelen satırın sinyaliyle hemen $B_{v(i)}$ tamponunun üzerine yazılmaktadır. Tampon seçme fonksiyonu v'nin yapısı (6.5) eşitliğinde gösterilmiştir.

$$v(i) = \begin{cases} S(u(i)), & 0 \leq i \leq 254 \quad için \\ i - 255, & 255 \leq i \leq 286 \quad için \end{cases} \tag{6.5}$$

Tampon seçme fonksiyonu (6.5) kullanılarak düzeltici permütasyon fonksiyonu (6.6) eşitliğindeki gibi yazılabilir.

$$p(i) = \max\{j \mid -32 \leq j < i \wedge v(j \bmod 287) = v(i)\} \tag{6.6}$$

(6.6) eşitliğindeki permütasyon fonksiyonunun eşdeğeri (6.7) eşitliğinde verilmiştir.

$$p^{-1}(i) = \min\{ j \mid i < j < 287 \wedge v(j) = v(i \bmod 287) \} \quad (6.7)$$

(6.8)'deki S fonksiyonu, düzelticideki değişken olmayan bellekte depolanmakta olan bir yerine koyma (substitution) tablosudur. Bu, uzun bir süre sabittir. Fakat havadan gönderilen sinyaller ile ara sıra güncelleştirilebilmektedir.

$$S: \{0,..., 255\} \rightarrow \{0,..., 31\} \quad (6.8)$$

(6.9)'daki fonksiyon, $r \in \{0,..., 255\}$ ve $s \in \{0,..., 127\}$ parametrelerine bağlıdır. Bu fonksiyon (6.10) eşitliğindeki biçime sahiptir.

$$u: \{0,..., 255\} \rightarrow \{0,..., 255\} \quad (6.9)$$

$$u(i) = (r + t_i) \bmod 256 \qquad t = 2s + 1 \quad (6.10)$$

15 bitlik çekirdek değeri (r, s) her alan için değişmektedir. Bu değer, akıllı kartın kod çözücüye her iki saniyede bir göndermekte olduğu düzeltilmiş 64 bitlik kontrol sözcüğünden hesaplanmaktadır.

$t = 2s + 1$ parametresi, 256 ile ortak çarpana sahip olmadığı için bütün r ve t kombinasyonları için u fonksiyonu {0,..., 255} aralığında bir permütasyondur. Tek sayılar, modülo 256 tamsayılar kümesinde bir çarpımsal alt grup oluşturur. Yani her $i \in \{1, 3,..., 255\}$ için tam olarak bir ters eleman $i^{-1} \in \{1, 3..., 255\}$ mevcuttur. Bu yüzden $i \,.\, i^{-1} \bmod 256 = 1$ olur. r ve t 'nin $2^{15} = 32768$ olası kombinasyonu olduğu için 32768 farklı u fonksiyonu vardır ve S 'nin yapısına bağlı olarak, sabit bir S yerine koyma tablosu ile v ve p 'nin pekçok farklı fonksiyonu mevcuttur.

Sabit bir S için bütün v fonksiyonlarının V_S kümesinin üyeleri arasındaki ilişki hakkında daha fazla bilgi almak için ilk önce bütün 2^{15} u fonksiyonlarının U kümesinin yapısının incelenmesi gerekmektedir.

$u, u' \in U$ olmak üzere herhangi bir (6.11) ve (6.12) fonksiyon çifti için a ve b gibi sadece bir çift sayı mevcuttur. Bu yüzden bunun sonucu (6.13) eşitliğindeki gibi olmaktadır.

$$u(i) = (r + t_i) \bmod 256 \quad (6.11)$$

$$u'(i) = (r' + t'_i) \bmod 256 \quad (6.12)$$

$$u(a + b_i) = u'(i) \quad (6.13)$$

Çünkü $a = (r' - r)$ ve $b = t' . t^{-1}$ sayıları bütün işi yapmaktadır. Bunun nedeni (6.14) eşitliğinde

verilmiştir.

$u(a + b_i) = (r + t(a + b_i)) \bmod 256 = (r + t((r' - r)t^{-1} + t'.t^{-1}.i)) \bmod 256 = (r + (r' - r) + t'.i) \bmod 256 = (r' + t'.i) \bmod 256 = u'(i)$ (6.14)

v fonksiyonlarının V_S kümesinde eşdeğer dönüşümler mümkündür. Bununla birlikte, a ve b sayı çiftinden birden fazla olabilmektedir. Bu yüzden, verilmiş olan bir v, $v' \in V_S$ fonksiyon çifti için (6.15)'teki gibi olmaktadır. Bu, boş bir S yerine koyma tablosu ile gerçekleştirilebilmektedir.

$v(a + b_i) = v'(i)$ (6.15)

Örneğin, eğer bütün i parametreleri için $S(i) = 0$ ise o zaman herhangi bir (a, b) çifti bütün i parametreleri için (6.15) eşitliğindeki gibi sonuçlanacaktır.

Bu karıştırıcı metodun yapısı, $p(i)<i$ veya eşdeğeri $p^{-1}(i) > i$ koşulu ve $p(0),..., p(286)$ dizisinin tekdüze biçimde artan 32 alt diziye bölünebilmesi koşulu ile p permütasyonunu sınırlamaktadır. Bu alt dizilerin herbiri, 32 tamponun birinde depolanmış olan satırların dizisine karşılık gelmektedir. Herhangi bir $0 \le i \le j \le 286$ ile $v(i) = v(j)$ için $p(i) < p(j)$ elde edilir. Eğer S bilinmiyorsa bu $32^{287-32} = 2^{1275}$ olası p permütasyonu, eğer S biliniyorsa sadece 2^{15} olası p permütasyonu ortaya çıkarmaktadır.

6.6.1.2 Permütasyonun yeniden yapılması

$C_{x,y}$ parlaklık veya önceki alandaki piksellere işaret eden negatif satır numaralarından önce gelen karıştırılmış alandaki (x, y) pikselinin üç boyutlu renk vektörünün tamamı olsun. O zaman, $K \in R^{288x288}$ matrisi bir alan için tanımlanmış korelasyon matrisi (6.16) olacaktır.

$$K_{i,j} = \frac{\sum_k C_{k,i-33} C_{k,j-33}}{\sqrt{\sum_k |C_{k,i-33}|^2 . \sum_k |C_{k,j-33}|^2}} \quad (6.16)$$

$K_{i,j}$ matrisi, i - 33 ve j - 33 satırlarının benzerliği için bir ölçüdür. $K_{i,j} = K_{j,i}$ ve $K_{i,i} = 1$ olduğu anlaşılmaktadır. Bundan dolayı, bütün $1 \le i \le j \le 288$ için sadece $K_{i,j}$ matrisinin belirlenmesi gereklidir. C görüntüsündeki i - 33 ve j - 33 satırlarının değiş tokuş edilmesi, K'daki i ve j satırlarının içerklerinin değiş tokuş edilmesine ve i ve j sütunlarının değiş tokuş edilmesine karşılık gelmektedir. C'nin satırlarının yeniden düzenlenmesindeki amaç, köşegene (diagonal) olabildiğince yakın en büyük değerleri getirmek için K'daki sıra değiştirici satırlara ve sütunlara karşılık gelen orijinal görüntüyü oluşturmaktır. Böylece kazanç fonksiyonunun

değeri (6.17) en yüksek dereceye çıkarılmış olur.

$$G(K) = \sum_{i=1}^{287} K_{i,i+1} \tag{6.17}$$

Bu, $G(PKP^T)$ değerini maksimize eden P permütasyon matrisinin bulunmasına karşılık gelmektedir. P, bütün i parametreleri için $P_{p(i)+33,i} = 1$ ile yeniden yapmak istediğimiz p permütasyonunu kapsamaktadır.

Aynı problemin diğer bir formülleştirilmesinde, karıştırılmış görüntüde herbiri bir i alan satırına karşılık gelen N_i düğümleri ($-32 \leq i \leq 254$) ile gösterilmiş bir G_K grafiğine bakılmaktadır. Bu grafikteki N_i ve N_j kenar bağlantıları, bütün i ve j parametmeleri için $K_{i+33,j+33}$ değerine sahiptir. Daha sonra, p için önceden belirtilmiş olan durumları yerine getiren ve kenar tanımlamalarının toplamı en büyük olan $N_{p(0)},\ldots, N_{p(287)}$ formunun bir Hamiltonian yoluna bakılmaktadır. Böyle bir yolun bulunması, yararlı bir takım tahmin algoritmaları bulunan Traveling Salesman probleminin bir varyantıdır.

6.6.1.3 Yerine koyma tablosunun yeniden yapılması

S tablosunu saptamanın olası bir yolu Nagravision kod çözücüsünü ters mühendislik işleminden geçirmek ve bu kod çözücünün değişken olmayan bellek tablosunun tamamını okumaktır [2]. Bu prosedür, bazı bölgelerde yasal olmadığı için diğer yaklaşımlar da denenebilir. $v \in V_S$ fonksiyonlarının kaydedilmiş büyük bir kolleksiyonu meydana getiren B_i satır tamponlarına erişimlerin dizisini incelemek için bir lojik analizör kullanılabilmektedir.

Eğer bir kod çözücünün içinin açılmasının yasal sebeplerden dolayı uygun olmadığı düşünülürse, karar verilen bir şifreli görüntü saldırısını gerçekleştirmek için bir bilgisayar video adaptörü kullanılabilir. Bu saldırıda, düşey karartma aralığındaki kodlanmış gerçek kontrol sözcüğü bilgisini içeren bir test görüntüsü kod çözücüye gönderilir ve bu, her satırı kendi alan satır sayısı ile işaretlemek için bir artık (redundant) binary kod kullanmaktadır. Daha sonra düzeltilmiş test görüntüsü kaydedilir ve buradaki satır sayısı işaretleyicilerin dizisi okunarak p permütasyonu elde edilir. Eğer bir Nagravision kod çözücüye ulaşılması mümkün değilse, bir önceki bölümde bahsedilmiş olan karıştırılmış televizyon görüntülerinin korelasyon matrisinden p permütasyon örneklerinin saptanması için kullanılan Traveling Salesman tahmin algoritmalarından biri denenebilir.

Her iki durumda da S'yi elde etmeden önce, gözlenmiş olan p permütasyonlarının v tampon erişim fonksiyonlarına dönüştürülmesi gerekmektedir. Bu, verilmiş olan p permütasyonlarının

hatasız olmasını sağlayan aşağıdaki basit algoritma ile başarılabilmektedir. Bütün $0 \leq i \leq 31$ parametreleri için $b_i := i - 32$ gerçekleştirilir. Daha sonra kod çözücü çıkışları olan herbir $0 \leq j \leq 254$ satırı için $b_i = p(j)$ olduğu i parametresi bulunur ve $v(j) := i$ ve $b_i := j$ 'nin her ikisi de gerçekleştirilir. Son bir kontrol olarak, bu 255 adımdan sonra bütün $0 \leq i \leq 31$ için (6.18) eşitliğindeki değere sahip olunduğunun doğrulanır.

$$b_i = p(255 + i) \tag{6.18}$$

Bu yolla V_S'nin birkaç üyesi toplanmış olur. Bu $0 \leq i \leq 254$ için yeniden yapılmış (6.19)'daki fonksiyonlarının herhangi biri, S 'nin biri hariç bütün değerlerini bilinmeyen r ve t parametreleri ile sırası değiştirilmiş olarak gösterir.

$$v(i) = S((r + t_i) \bmod 256) \tag{6.19}$$

Sadece bir v değeri seçip alınır ve bütün $0 \leq i \leq 254$ değerleri için $S''(i) := v(i)$ olacak şekilde yeniden yapılmış olan S'' tablosu seçilir. Daha sonra, başka bir v' tampon erişim fonksiyonu yeniden yapılır ve bütün $0 \leq i \leq 254$ için (6.20) eşitliği gerçekleşecek şekilde a ve b parametreleri aranır ve bunlar bulunduğu zaman ayrıca S'' nin (6.21) eşitliği ile kalan değeri de bulunmuş olur.

$$S''(i) = v'((a + b_i) \bmod 256) \tag{6.20}$$

$$S''(255) = v'((a + b.255) \bmod 256) \tag{6.21}$$

Bulunan S'' parametresinin S 'nin sadece sırası değiştirilmiş bir versiyonu olduğu geçeği bizi ilgilendirmemektedir. Çünkü, eğer bazı (a, b) parametreleri için S'' parametmesi (6.22)'deki gibi ise o zaman bunun anlamı, bunu takip eden doğru (r, t) parametreleri için korelasyon aramasında S'' nin bu permütasyonunu tamamen karşılayacak sadece (r'', t'') parametreleri bulunmuş ve doğru S tablosu ve (r, t) parametreleri ile elde edilmiş olan aynı v 'de sonuçlanmıştır.

$$S''(i) = S((a + b_i) \bmod 256) \tag{6.22}$$

6.6.1.4 Bilinen bir yerine koyma tablosu bazlı gerçek zamanlı permütasyon saptama

S parametresini ya bir Nagravision kod çözücüsünden elde ettikten ya da bir önceki bölümde ana hatları verilen şekilde belirlendikten sonra karıştırıcının oldukça etkili bir şekilde tesine çevrilmesi mümkündür. Bunun için basit bir yaklaşım, bütün 2^{15} olası (r, t) çifti üzerinde bir kaba kuvvet (brute force) araması yapmaktır. Her olası (r, t) çifti için bir penaltı

fonksiyonunun değeri, karıştırılmış görüntüdeki rasgele seçilmiş piksel çiftlerinin küçük bir sayısı arasındaki $|C_{x,p(y)} - C_{x,p(y+1)}|$ farkının ölçülmesiyle tahmin edilebilmektedir. Permütasyonun sadece birkaç test pikseli için uygulanması gerektiği ve görüntünün tamamı için uygulanması gerekmediği için bu durum çok etkili bir şekilde gerçekleştirilebilmektedir. Penaltı fonksiyonunun (6.23) en küçük olacağı (r, t) çiftinin aranması gereklidir.

$$H = \sum_{i=1}^{n} |C_{x_i,p(y_i)} - C_{x_i,p(y_i+1)}| \tag{6.23}$$

$(p(y_i), p(y_i+1))$ çifti, bütün 2^{15} (r, t) çifti için yüksek verim için ön işlemden geçirilmektedir. Bu (r, t) çifti tespit edildiği zaman, bütün satırları gerçek zamanlı olarak yeniden düzenlemek için benzer bir permütasyon fonksiyonu kullanılmaktadır.

Nagravision sisteminde karıştırılmış SECAM sinyalleri için, piksel parlaklık korelasyonuna bakılması gibi basit bir alternatif mevcuttur. SECAM standardında renk, R-Y (kırmızı - parlaklık) ve B-Y (mavi - parlaklık) olan iki fark sinyali biçiminde bir frekans modülasyonlu taşıyıcı üzerinde kodlanmaktadır. Bu modülasyonlu R-Y ve B-Y sinyalleri birbirini izleyen satırlara eklenmektedir. Televizyon alıcısının kendi renk kod çözücüsünü senkronize etmesini sağlamak için R-Y, 282 x 15.625 kHz = 4.406 MHz'lik bir taşıyıcı ve B-Y ise 272 x 15.625 kHz = 4.250 MHz 'lik bir taşıyıcı kullanır. Modüle edilmemiş olan renk taşıyıcı sinyali, yatay karartma aralığındaki satır önü ve satır sonu boşluklarında mevcuttur ve bu, aktif satır ile birlikte sırası değiştirildiği için düzeltilmiş alandaki karıştırılmış bir satırın tek veya çift numaralı satır olup olmadığının görülmesi kolaydır. Karıştırılmış SECAM sinyalinin satır arkası boşluğundaki 4.406 MHz ve 4.250 MHz'lik renk taşıyıcı frekansları nın dizisi, bu alanı karıştırmak için kullanılmış olan (r, t) çifti için karakteristiktir. Bir korsan kod çözücü, sadece 255-286 arası satırların satır arkası boşluğunda bulunan taşıyıcı frekansın dizisini temsil eden 1 bitlik bir dizi oluşturmalıdır ve bu bit dizisini bir karma tablo taramasındaki anahtar olarak, değişen taşıyıcı frekanslardan biri ile bu diziyi doğru şekilde düzelten (r, t) çiftine ulaşmak için kullanmalıdır. Daha sonra bu (r, t) çifti, geriye kalan alanı doğru bir şekilde düzeltmek için kullanılmaktadır.

Bu saldırının ticari amaçlı bir donanım uygulaması 1995 yılında Fransa'da mevcuttu. Canal Plus, buna bir karşı tedbir olarak kod çözücülerine yeni bir S yerine koyma tablosu yükledi. Bu tablo, renk taşıyıcı frekanslarının dizisini devamlı değiştirmekte ve bu nedenle (r, t) çifti hakkında bilgi sızdırmamaktaydı. Bu saldırının gelişmiş bir versiyonu hem frekansa hem de satır arkası boşluğundaki renk taşıyıcısının fazına bakmaktadır. SECAM renk taşıyıcısı,

taşıyıcı sinyalin neden olduğu görülebilir nokta örneklerini bastırmak için herbir üçüncü satır için 180 derece ile faz kaydırılmıştır. İlk 32 satırların hangilerinin bu bu faz kaydırmasını gösterdiğini belirten bir bit dizisi, uygun (r, t) çiftini hızlı bir şekilde bulmak için bir karma tablo tarama anahtarı gibi davranır. PAL renk patlamasının sırası değiştirilmediği için bu SECAM renk taşıyıcı saldırı tekniği, direkt olarak PAL için Nagravision düzelticisine dönüştürülemez.

6.6.1.4.1 Yerine koyma tablosunun özellikleri

Premiere, Teleclub ve günümüze kadar diğer pekçok ödemeli televizyon kanalının kullanmakta olduğu S yerine koyma tablosu aşağıdaki biçimdedir:

```
10, 11, 12, 13, 16, 17, 18, 19, 13, 14, 15, 16,  0,  1,  2,  3,
21, 22, 23, 24, 18, 19, 20, 21, 23, 24, 25, 26, 26, 27, 28, 29,
19, 20, 21, 22, 11, 12, 13, 14, 28, 29, 30, 31,  4,  5,  6,  7,
22, 23, 24, 25,  5,  6,  7,  8, 31,  0,  1,  2, 27, 28, 29, 30,
 3,  4,  5,  6,  8,  9, 10, 11, 14, 15, 16, 17, 25, 26, 27, 28,
15, 16, 17, 18,  7,  8,  9, 10, 17, 18, 19, 20, 29, 30, 31,  0,
24, 25, 26, 27, 20, 21, 22, 23,  1,  2,  3,  4,  6,  7,  8,  9,
12, 13, 14, 15,  9, 10, 11, 12,  2,  3,  4,  5, 30, 31,  0,  1,
24, 25, 26, 27,  2,  3,  4,  5, 31,  0,  1,  2,  7,  8,  9, 10,
13, 14, 15, 16, 26, 27, 28, 29, 14, 15, 16, 17, 18, 19, 20, 21,
22, 23, 24, 25,  5,  6,  7,  8, 19, 20, 21, 22, 12, 13, 14, 15,
17, 18, 19, 20, 27, 28, 29, 30, 10, 11, 12, 13, 11, 12, 13, 14,
 6,  7,  8,  9,  1,  2,  3,  4,  0,  1,  2,  3,  4,  5,  6,  7,
 3,  4,  5,  6,  8,  9, 10, 11, 15, 16, 17, 18, 23, 24, 25, 26,
29, 30, 31,  0, 25, 26, 27, 28,  9, 10, 11, 12, 21, 22, 23, 24,
20, 21, 22, 23, 30, 31,  0,  1, 16, 17, 18, 19, 28, 29, 30, 31
```

Bu özel tablo (6.24)'te görülen özelliğe sahiptir. Fakat bunun nedeni tam olarak bilinmemektedir.

$$S(i) = (S(i - i \bmod 4) + i \bmod 4) \bmod 32 \qquad (6.24)$$

Canal Plus, yukarıdaki tabloyu 1997 yılı Eylül ayında aşağıdaki tablo ile değiştirmiştir. Bu yeni tablo (r, t) çiftini karıştırılmış görüntüdeki renk taşıyıcı frekansının dizisinden yeniden yapan korsan SECAM Nagravision kod çözücülerin piyasada mevcut olmasına bir yanıt olarak yaratılmıştı.

Bu yeni tablo $S(i) \equiv i \pmod 2$ özelliğine sahiptir. Bu yolla, ortaya çıkan permütasyon devamlı tek ve çift numaralı satırlar arasında değişmekte ve karıştırılmış bir SECAM görüntüsündeki renk alt taşıyıcı frekanslarının dizisi r ve t değerlerinin tamamını değil sadece r mod 2 değerini gösterebilmektedir.

$$i \neq j \pmod 6 \quad \Rightarrow \quad S(i) = S(j) \tag{6.25}$$

Eğer S tablosu (6.25)'teki gibi seçilmişse, temiz sinyalde her altı satırda tekrarlanmakta olan renk taşıyıcı fazı ve frekansının kombinasyonu sadece r mod 6 ve t mod 3 değerlerini gösterebilmektedir.

```
 0,  1,  2,  3,  4,  5,  6,  7,  2,  5,  4,  7,  8,  9, 10, 11,
14, 17, 16, 19, 22, 25, 24, 27, 26, 31, 30,  1, 24, 27, 26, 29,
 8, 11, 10, 13, 20, 23, 22, 25, 20, 21, 22, 23, 30, 31,  0,  1,
16, 17, 18, 19, 28, 29, 30, 31, 10, 11, 12, 13, 16, 17, 18, 19,
12, 15, 14, 17,  0,  1,  2,  3, 20, 23, 22, 25, 18, 19, 20, 21,
22, 25, 24, 27, 26, 27, 28, 29, 18, 21, 20, 23, 10, 13, 12, 15,
28, 29, 30, 31,  4,  5,  6,  7, 22, 23, 24, 25,  4,  7,  6,  9,
30,  1,  0,  3, 26, 29, 28, 31,  2,  5,  4,  7,  8,  9, 10, 11,
14, 15, 16, 17, 24, 27, 26, 29, 14, 17, 16, 19,  6,  9,  8, 11,
16, 19, 18, 21, 28, 31, 30,  1, 24, 25, 26, 27, 20, 21, 22, 23,
 0,  3,  2,  5,  6,  7,  8,  9, 12, 13, 14, 15,  8, 11, 10, 13,
 2,  3,  4,  5, 30, 31,  0,  1, 24, 25, 26, 27,  2,  3,  4,  5,
30,  1,  0,  3,  6,  9,  8, 11, 12, 15, 14, 17, 26, 27, 28, 29,
14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25,  4,  7,  6,  9,
18, 21, 20, 23, 12, 13, 14, 15, 16, 19, 18, 21, 20, 29, 28, 31,
10, 11, 12, 13, 10, 13, 12, 15,  6,  7,  8,  9,  0,  3,  2,  5
```

6.7 DirecTv Sistemi

DirecTv sisteminin patentine (U.S. Patent No: 4,748,668) göre akıllı kartın üzerinde bir Fiat-Shamir Sıfır Bilgi Testi algoritması mevcuttu. Bu algoritma, kod çözücüye yerleştirilmiş olan akıllı kartın gerçek bir akıllı kart olup olmadığını görmek için kod çözücünün çalıştırdığı bir doğruluk ispatlama algoritmasıdır. Aynı algoritma, Avrupa'da kullanılmış olan VideoCrypt sisteminde de kullanılmıştı ve korsanlar tarafından yenilgiye uğratılmıştı. Bu, yeni bir sistem için tam anlamıyla en iyi başlangıç değildi.

Doğruluk ispatlama algoritması, güvenli kalması amaçlanmmış olan veri güvenli kalmadığı için tehlikeye düşmüştür. Bununla birlikte, bu algoritmanın nasıl çalıştığını anlayan bir korsan, kolay bir şekilde doğru yanıtların taklitlerini yapabilmektedir. Avrupa'daki korsanlar bu beceriyi, Fiat-Shamir Sıfır Bilgi Testinin VideoCrypt-I sisteminden daha fazla önemli olduğu VideoCrypt-II sisteminde kazanmışlardı. Çünkü Fiat-Shamir Sıfır Bilgi Testi VideoCrypt-I sisteminde sadece kartın doğruluğu ispatlamak için kullanılmıştır. VideoCrypt-II sisteminde ise Fiat-Shamir Sıfır Bilgi Testinin sonuçları, doğru çekirdek sonuçlarını vermek için karma fonksiyonun sonuçları ile EXOR'lanmıştır.

Avrupa'da News Datacom'un 09 serisi için kullanmış olduğu akıllı kart, DSS kartının ilk serisiyle ve VideoCrypt-II kartıyla aynıydı. DirecTv sistemindeki hack işleminin kökeni Sky

07 ve 09 kartlarının hack edilmesine dayanmaktadır. Bu hack işlemlerinden elde edilmiş olan bilgiler, DirecTv kartının hack edilmesi için çok yardımcı olmuştur.

Avrupa'da 07 serisi kartı kullanmış olan VideoCrypt sistemi hack edilmişti ve bu kartın kaynak kodunun tamamı ilgili internet siteleri ve BBS'ler üzerinde ücretsiz olarak dağıtılmıştı. Digital Satellite System (DSS), Amerika'da kullanılmak üzere hazırlanmaktaydı. News Datacom için Sky 09 kartını yeni DSS kartı için uyarlamak çok kolaydı. ROM rutinlerinin büyük bir kısmı, bu yeni sisteme çok kolay adapte edilebilmekteydi. En önemli değişiklikler EEPROM'da gerçekleştirilecekti. Akıllı kartın EEPROM'u en önemli kriptografik rutinleri içeren bölgedir.

Avrupa'da 09 serisi Sky kartının içeriğinin okunması sadece birkaç ay sürmüştür. Bu işlem, akıllı kartın tamamen ters mühendislik işleminden geçirilmesini kapsamaktadır. 09 serisi Sky kartının ön deneme (preliminary) kodunun bir bölümü Londra'da bir açık arttırmada satılmıştı. Bu sadece bir başlangıçtı. Fakat bundan dört ay sonra bu sistem artık tamamen tehlike altındaydı. Bu işlemin en önemli kısmı akıllı kartın kodunda bir arka kapı (back door) olduğunun farkına varılmasıydı.

DirecTv kartının genel teorisi büyük ölçüde 07 serisi Sky kartına ve VideoCrypt-II kartına dayanmaktaydı. VideoCrypt-II kartındaki algoritmada kullanılmış olan Sıfır Bilgi Testi doğruluk ispatlaması ile çekirdek üretiminin entegre edilmesi gibi düzenlerin bu sistemde yeniden başarılı olabileceği düşünülemezdi. Ayrıca DirecTv kartının veri hızı, VideoCrypt-II kartının daha hızlı veri hızının (38.4 kbaud) burada kullanılabileceğini göstermektedir.

6.7.1 VideoGuard kart protokolü

1) 58h paketi (23 Bayt)

58h paketi, sigorta (fuse) bilgisini içermektedir ve ayrıca, elektronik kimlik numarasının ilk dört baytında neyin bulunması gerektiğini göstermektedir. Sigorta bilgisi bayt 00 ve bayt 12'dir. Görünüşe göre bu sigorta bilgisi, kartın durumunu tanımaktadır. 05h veya 25h değerleri aktif bir kartı gösterirken bir 04h değeri kapatılmış bir kartı göstermektedir.

01 ile 04 arasındaki baytlar kartın elektronik kimlik numarasının en soldaki dört baytını içermektedir. Bu numara, kart seri numarasından farklıdır. Çünkü bu numara karta yetki verilirken veya kartın yetkisi alınırken bu kartı adreslemek için kullanılmaktadır.

58h paket yapısı:

Bayt 00 : Sigorta verisi 00

01 ile 04 arasındaki baytlar : Kart kimlik numarasının en soldaki 4 baytı

Bayt 05 : Kart dağıtım numarası (01)

06 ile 11 arasındaki baytlar : Bilinmiyor

Bayt 12 : Sigorta verisi 01

13 ile 23 arasındaki baytar : Bilinmiyor

2) 2Ah paketi (119 Bayt)

Bu paket, karttan kod çözücüye giden kritik bilgilerin büyük bir kısmını taşımaktadır. Bu paket aşağıda incelenmiştir. Bu paketin sonuçlarının modifiye edilmesiyle bu kartın başka IRD'lerde kullanılmasını sağlamak mümkündür.

24h paket yapısı:

Bayt 00 : Sigorta verisi 00

01 ile 03 arasındaki baytlar : Kartın dağıtım numarası (ATR'den gelen 21h B0h 11h)

04 ile 11 arasındaki baytlar : Kartın seri numarası

12 ile 26 arasındaki baytlar : Elektronik kimlik numarası

27 ile 54 arasındaki baytlar : IRD'nin kimliği

55 ile 118 arasındaki baytlar : Kanalın abone detayları

Kartın elektronik kimlik numarası 5 bayt uzunluğundadır. Bu numara, DSS kanalı tarafından kartları adreslemek için kullanılmıştır.

IRD'nin kimliği, kartın kullanıldığı IRD'nin ayrıntılarını içermektedir. DirecTv sistemindeki kartlar, özel IRD'lerle birleştirilmektedir. Elektronik kimlik numarasının ilk 4 baytı ile IRD'nin kimliği EXOR'lanarak doğru kod çözücü kutu numarası elde edilmektedir. Ayrıca bu, elektronik kimlik numarasının ilk 4 baytı ile 58h paketinin 01 ile 04 arasındaki baytlarının EXOR'lanmış olduğu anlamına da gelmektedir. Bir kartın birden fazla IRD'de kullanılabilmesini sağlayacak basit bir hack işlemi gerçekleştirilebilmektedir.

3) 4Ch paketi (9 Bayt)

Amerika'daki bazı korsanlara göre bu paket kartın seri numarasıdır. Fakat kartın seri numarasının 2Ah paketinde mevcut olduğu gerçeği bu paketin kimliğin başka bir biçimi olduğunu göstermektedir.

4) 40h paketi (25Bayt)

Bu paket çekirdeğin hesaplanması için gerekli olan veri paketidir. Bu paket kanaldan kanala değişmektedir. Fakat herzaman 09h ile başlamaktadır. Bu paket, çekirdek verisi veya yetki verme paketlarindeki gibi kritik bilgi içeren bir paket için bir bayraktır (flag).

Herbir paket 09h ile başladığı için bu paket yapısı standarttır. Diğer elemanlar ise kanal kimliği, televizyon programı kimliği ve bir clock'tur. Son 5 bayt ise karma imzanın birkaç formudur.

5) 54h paketi (13 Bayt)

Bu çekirdek paketidir. Bu, VideoCrypt sisteminde kullanılmış olandan daha büyük bir çekirdektir. İkinci en son konumdaki 01h baytı, çekirdeğin geçerli veya geçersiz olduğunu göstermektedir. Bu paket, sonraki çekirdeğin üretiminde bu çekirdeğin buna nasıl katılacağını göstermektedir.

6) 4Ah paketi (1 Bayt)

Bu paket, kayıtta (log) 01h olarak gönmekte olan tek bir bayttır. Bu sistemde kullanılmakta olan Fiat-Shamir Sıfır Bilgi Testine göre bu paket, işlemdeki Q baytıdır.

7) 5Ah paketi (8 Bayt, 64 Bayt)

Bu paketlerin uzunlukları bunların Fiat-Shamir Sıfır Bilgi Testi işleminin bir parçası olabileceğini göstermektedir. Normalde Fiat-Shamir Sıfır Bilgi Testi, kart tarafından kendisinin doğruluğunu kod çözücüye ispatlamak için kullanılmaktadır. Eğer bu ispatlama başarısız olursa, o zaman kod çözücü kapanacaktır ve çalışmayacaktır. Fakat bundan daha mantıklı olan Fiat-Shamir Sıfır Bilgi Testinin kartın içinde dahili olarak çekirdek üretimi için kullanılmış olduğudur. Fiat-Shamir Sıfır Bilgi Testinin sonucu, karma fonksiyondan gelen çekirdek çıkışına doğru EXOR'lanmıştır.

8) 52h paketi (4 Bayt)

Kayıtta bu paketin içerikleri, sıfırlardan oluşmuş olan bir dizidir. Bu baytların görevi henüz

bilinmemektedir.

9) 5Eh paketi (75 Bayt)

Bu paket çoğunlukla boş olmasına rağmen sıralama yapısının birkaç formu gibi görünmektedir

10) 5Ch paketi (4 Bayt)

Kayıtta bu paketin içerikleri, sıfırlardan oluşmuş olan bir dizidir. Bu baytların görevi henüz bilinmemektedir.

10) 42h paketi (31 Bayt, 44 Bayt, 18 Bayt)

Sistemin yetki verme işleminde kullanılan paketi 42h paketidir. Bu paket, kartları adreslemede ve bu kartlara bir kanal veya kanal dizileri için yetki verme veya yetki alma işi için kullanılmaktadır. Bu paket, uygulamadan uygulamaya değişen bir uzunluğa sahiptir.

Bu sistemdeki kart kimlik yapısı üç diziden oluşmuştur. Burada bir elektronik seri numarası (kart kimliği), bir kart seri numarası ve bir içine yerleştirilmiş kart numarası mevcuttur. İçine yerleştirilmiş olan kart numarası bir U (55h) ile başlar ve bunu bir takım basamaklar takip eder. Bu numara, kartlara ayrı ayrı yetki vermek için kullanılmaktadır. Böyle bir yetki verme paketi kart kimliğinden (en soldaki 4 bayt), kart seri numarasından ve U numarasından gelen verileri içermektedir.

6.7.2 DirecTv sisteminde gerçekleştirilen hack işlemleri

Bu sistemde Battery kart ve Phoenix'lenmiş kart olmak üzere iki tip hack işlemi mevcuttur. Birkaç Battery kartı varyantı bulunmaktadır. Orijinal varyantlardan biri Dallas 5002FP mikrokontrolörünü baz almıştır. Daha sonraki versiyonlar ise Dallas 5002FP'nin piyasadan temin edilmesi zor olduğu için Dallas 5001 ve Dallas 5000 mikroçiplerini kullanmıştır. Bu Dallas 5001 varyantı için devre diyagramı Bölüm 4'te verilmiştir.

Bu kartların yeniden programlanması gerekmekteydi. Amerikan versiyonu Battery kartlarda tuş takımı yoktu. Tuş takımının yerine, kartın özel bir programlama ünitesi ile yeniden programlanmasını sağlamak için bir sıra pad'e sahipti. Battery kartlarına bütün güncellemeler yeni dosya formatındadır. Bu dosyalar MAIN* ile tanımlanmaktadır. Buradaki * sembolü, güncelleme versiyonunu gösteren iki basamaktır. Bu dosyalar belirli bir karta göre kodlanmıştır. Bu yüzden internet ve BBS'ler üzerinden güvenli bir şekilde dağıtılabilmektedir.

Phoenix'lenmiş kartlar daha yeni bir gelişmedir. Bunlar, bir Phoenix kartı kullanılarak aktif hale getirilmiş olan orijinal DSS akıllı kartlarıdır. Bununla birlikte bu yeniden programlanabilen kartlar, DirecTv sistemi için çok büyük bir tehlikeydi. Çünkü bu kart, abone yönetim sistemine direkt bir saldırı oluşturmaktaydı.

Burada bir SEASON hack işlemi ve bir Blocker hack işlemi olmak üzere olası iki tip hack işlemi mevcuttur. SEASON hack işlemi, DSS 01 kart serisine çok uygundur. Bu tür bir hack işlemi bilgisayarlarda (PC ve Apple MAC) çalışmaktadır ve Avrupa'daki Sky ve D2-MAC SEASON hack işlemleri ile aynı formattadır. Özelikle haberleşme rutinleri olmak üzere benzer kaynak kodlarının bazıları yeniden kullanılabilmektedir.

Blocker hack işlemi kanallar için, Phoenix'lenmiş kartlar ile benzer bir tehlike düzeyine sahiptir. Bu hack işlemi, orijinal bir kartın ömrünün arttırmak için veya bu kartın DSS abone yönetim sistemi tarafından kapatılmasını engellemek için kullanılmaktadır. Bu hack işleminin detayları bu bölümün VideoCrypt kısmında verilmiştir.

09 serisi Sky kartı bloke edicileri için PIC16C84 kaynak kodu ilgili internet sitelerinde veya BBS'lerde mevcuttur. Fakat bu kodun, farklı paketleri okuması ve daha yüksek baud hızında çalışması için modifiye edilmesi gerekmektedir.

6.7.3 DIREC programı

Bu bölümde kartın incelenmesi için verilmiş olan bu program DSS kartları ile test edilmiştir ve uygun şekilde çalışmıştır. DIREC isimli bu program, Bölüm 4'te verilmiş olan Phoenix arabirimleri ile çalışmaktadır.

DIRECT isimli bu program Markus Kuhn tarafından VideoCrypt kod çözücülerinin çalışma şeklini emüle etmek (emulate) için geliştirilmiş olan DECOEM.C isimli programı baz almıştır. Burada verilmiş olan DIRECT isimli program, bir bilgisayarın bir DSS kod çözücüsünü emüle etmesini ve orijinal bir DSS kartı veya korsan bir DSS kartı ile haberleşmesini sağlamaktadır.

DSS kartı 9600 Baud'luk bir baud hızında başlatılmaktadır. Başlatıldıktan sonra, veri transferinin daha hızlı yapılabilmesi için 38400 Baud'luk bir hıza geçmektedir. Bunun anlamı, bu DSS kartının orijinal 07 veya 09 serisi Sky kartlarından daha hızlı veri gönderebildiği ve alabildiğidir.

Bu durduğu zaman bu program karttan üç paket okumaktadır. Bu paketler; ATR, 58h paketi

ve 2Ah paketidir. Bu paketler kartı, IRD'yi ve kanalın abone detaylarını saptadığı için sistemdeki en önemli paketlerden bazılarıdır.

Bu program C programlama dilinde yazılmıştır ve Borland C programında derlenmiştir. Prosedür; DIREC.PRJ isimli dosyayı yaratmak, buna DIREC.C isimli dosyayı eklemek ve daha sonra da ASYNC.OBJ isimli dosyayı eklemekten ibarettir. Daha sonra bu programın derlenmesi basit bir iştir. OBJ dosyasını ve programın derlenmiş versiyonunu içeren dosya, ilgili internet sitelerinden ve BBS'lerden temin edilebilmektedir.

Bu programın çatısı kullanılarak, kartları farklı paketler ile test etmede kullanılabilecek bir programın yaratılması mümkündür. Fakat Phoenix tipi bir program yaratmak için çalışan bir karma fonksiyon gerekmektedir. Ayrıca, kartın adresleme sistemi neredeyse tamamen anlaşılır olduğu için kartın ilgili adresleme verisi için 42h paketlerinin herbirini inceleyecek Blocker tipi bir programın da yaratılması mümkündür.

DSS kartı, 07 serisi Sky kartı ile aynı dönemde çıkmış olduğu için böyle bir hack işleminin gerçekleşmesi mümkündür. 07 serisi Sky kartı, havadan gönderilen yetki verme ve yetki alma verisini, komutları ve kart numaralarını kodlamamıştır. Bu durum, 09 serisi Sky kartı ve ayrıca VideoCrypt-II kartının bir özelliğiydi. Eğer 42h paketi gerçekten asıl işi yapan paket ise, o zaman bu paket uygun kart açma veya kapatma sinyalleri ve kart kimlik verisi için incelenebilecektir. Bundan sonra bir Blocker yapmak mümkün olur. VideoCrypt sisteminde kullanılmış olan Genesis/Blockers'ı baz almış olan bu Blocker aygıtı, 58h ve 2Ah paketlerinden kart kimlik verisini okumakta ve bu kart kimlik verisi ile 42h paket verisiyle karşılaştırmaktadır. Daha sonra, eğer kart bilgisi 42h paketinde tutulmakta ise bu paketin karta ulaşması engellenir. Aksi taktirde kod çözme işlemi gerçekleşmez.

Bu oldukça basit bir hack işlemidir. Fakat News Datacom 42h paketlerini zincirlediği (chained) için bu hack işlemi artık çalışmayabilir. Zincirlemenin anlamı, ilgili 42h paketi ve ilgili çekirdek üretim veri paketinin (muhtemelen 40h paketi) herikisinin de çekirdek üretimi için gerekli olmasıdır.

ATR, IRD'ye akıllı kartı nasıl idare edeceğini bildirmektedir. Örneğin, hangi clock frekansını kullanacağını ve hangi programlama gerilimlerinin ve akımlarının gereki olduğunu IRD'ye bildirir (Bu detaylı bir biçimde Bölüm 4'te incelenmiştir). Ayrıca reset cevabının önemli bir yaklaşımı 2Ah paketinde gösterilmektedir. 21 b0 11 baytları kartın kimliğini saptamak için kullanılmıştır.

ATR: 3f 76 13 25 04 21 b0 11 4a 50 03

7. SONUÇLAR ve ÖNERİLER

Bu çalışmada anlatılan tüm bilgilerin ışığında hiçbir karıştırıcı sistemin güvenliğini tam olarak sağlayamadığı anlaşılmaktadır. Bir üreticinin karıştırıcı sisteminde kullanmış olduğu karıştırıcı teknik hack edilirse, aynı tekniği kullanan başka bir üreticiye ait başka bir sisteme de bu hack işlemi uygulanabilmektedir. Genellikle bir karıştırıcı sistemin zayıf noktası, erişim kontrol sistemidir. Bu erişim kontrol sistemi planının tamamı sadece akıllı kartları baz almaktadır. VideoCrypt, EuroCrypt ve DirecTv akıllı kart bazlı sistemlerde hack işlemi gerçekleştikten sonra akıllı kartların korsanlığı önleyeceği düşüncesinin ne kadar yanlış olduğu anlaşılmıştır.

Son yıllarda gerçekleştirilmiş olan akıllı kart bazlı hack işlemlerinin tamamı, orijinal akıllı karttaki algoritmaların ve anahtarların çıkarılması ve bunların korsan akıllı kartlarda emüle edilmesi prensibine dayanmaktadır. Çünkü akıllı kart teknolojisi bir takım kusurlara sahiptir.

Piyasadaki sonuca ulaşan yeni sistemlerin çoğunluğu, dijital video tekniklerinin birini veya birkaçını kullanmaktadır. En yaygın kullanılan dijital karıştırıcı tekniği satır karıştırmadır (line shuffle). Kayan çubuk karıştırması (sliding bar shuffle) kullanmak daha ucuz bir seçenek olduğunda, tam alan karıştırmasına (full field shuffle) dayanan daha güvenli diğer versiyonları da ortaya çıkmıştır. Tam alan karıştırma, bellek gerektiren bir seçenektir ve bu durum kod çözücü birim maliyetine yansımaktadır. Kod çözücünün yüksek maliyetinden dolayı, sıradan primli televizyon programları yayınlayan ödemeli televizyon kanallarından ziyade son derece değerli programlar yayınlayan kanallar hedeflenmektedir.

Kablolu bazlı karıştırıcı sistemler geliştirilmediği için kablolu sistemlerin güvenliği tehlike altındadır. Çünkü kablolu televizyon sistemlerinde kullanılmış olan teknoloji değişmeden kalırken korsanların teknolojisi hızla ilerlemektedir. Kablolu televizyon kanalları bu konudaki yasalara güvenmek zorunda kalmışlardır. Çünkü kablolu televizyon korsanlığı oldukça ciddi bir suçtur ve bir orijinal kod çözücüyü modifiye eden bir kişi yakalanırsa çok büyük para cezalarına çarptırılmaktadır.

Günümüzde donanım bazlı hack işlemlerinin yerini yazılım bazlı hack işlemleri almıştır. Sadece standart bir bilgisayar ve bu bilgisayara takılacak olan bir televizyon kartı ile ücretli televizyon kanallarının yayınları izlenebilmektedir. Bu durumda televizyon kanalının bu duruma karşı alacağı tedbir de çok sınırlı olmaktadır. Çünkü herhangi bir korsan kod çözücü kullanılmaksızın televizyon yayınları izlenebilmektedir. Yani, ne tür bir karşı tedbir alınırsa alınsın uygun bir yazılımla bu durumun da üstesinden gelinmesi kaçınılmazdır.

KAYNAKLAR

[1] McCormac, J., (1996), European Scrambling Systems 5, Waterford University Press MC^2 Publications Division, Ireland.

[2] Kuhn, M., (1998), "Analysis of the Nagravision Video Scrambling Method", University of Cambridge Computer Laboratory, mgk25:1-13.

ÖZGEÇMİŞ

Doğum tarihi	21.08.1975	
Doğum yeri	İstanbul	
Lise	1990-1993	Özel Şener Lisesi
Lisans	1993-1997	Yıldız Teknik Üniversitesi Mühendislik Fakültesi Elektrik Mühendisliği Bölümü
Yüksek Lisans	1997-2000	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektrik Mühendisliği Anabilim Dalı
Çalıştığı kurum		
	1997-1999	Aykor Denizcilik Mühendislik San. ve Tic. A.Ş.