T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

SIR PAYLAŞIM SİSTEMLERİ

İBRAHİM ÖZBEK

YÜKSEK LİSANS TEZİ
MATEMATİK ANABİLİM DALI

DANIŞMAN
PROF. DR. İRFAN ŞİAP

İSTANBUL, 2012

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

SIR PAYLAŞIM SİSTEMLERİ

İbrahim ÖZBEK tarafından hazırlanan tez çalışması 27/07/2012 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Prof. Dr. İrfan ŞİAP

Yıldız Teknik Üniversitesi

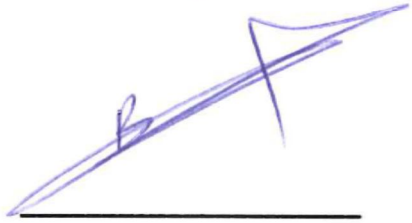
Jüri Üyeleri

Prof. Dr. İrfan ŞİAP

Yıldız Teknik Üniversitesi

Doç. Dr. Bayram Ali ERSOY

Yıldız Teknik Üniversitesi



Yrd. Doç. Dr. Bahattin YILDIZ

Fatih Üniversitesi

ÖNSÖZ

Bu tez şifrelemede önemli bir yere sahip olan anahtar saklama yöntemleri konusunda matematikçilere yardımcı olması amacıyla hazırlanmıştır.

Bu zorlu yolda her zaman yanımda olan ve desteklerini esirgemeyen kıymetli hocam Sayın Prof. Dr. İrfan ŞİAP'a; tez jürimde olup kıymetli yorumlarını ve tavsiyelerini bizimle paylaşan Sayın Doç. Dr. Bayram Ali ERSOY ve Yrd. Doç. Dr. Bahattin YILDIZ hocalarıma; bana her zaman destek veren, her zorlukta yanımda yer alan aileme ve çalışmalarımda bana her zaman destek olan nişanlım Hacer ÖZTÜRK'e en içten şükranlarımı sunarım.

Temmuz, 2012

İbrahim ÖZBEK

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

F_q	$\{0,1,...,q-1\}$ elemanlarından oluşan sonlu cisim
$\mathrm{F}_q{}^n$	Bileşenleri F_q cisminden alınmış n uzunluklu vektörlerin uzayı
$\varnothing$	Boş küme
$boy(V)$	V vektör uzayının boyutu
$S^{\perp}$	S kümesinin dikey tümleyeni, ortogonali
$(n,M)_q-$kod	Kodsözlerinin bileşenleri F_q cisminden alınmış n uzunluklu M tane kodsözden oluşan (lineer olmak zorunda değil) kod
$[n,k]_q-$kod	Kodsözlerinin bileşenleri F_q cisminden alınmış n uzunluklu k boyutlu lineer kod
$[n,k,d]_q-$kod	Kodsözlerinin bileşenleri F_q cisminden alınmış n uzunluklu k boyutlu, d minimum uzaklığa sahip lineer kod
$\lvert C\rvert$	C kodun eleman sayısı
$\langle S\rangle$	S kümesi tarafından üretilen alt uzay
$\langle u,v\rangle$	u ile v vektörünün iç çarpımı
A^T	A matrisinin satırlarını sütun kabul eden matris, transpoze
$d(x,y)$	x ile y vektörleri arasındaki Hamming uzaklık
$w(x)$	x vektörünün Hamming ağırlığı
$w_{\min}$	Kodun minimum ağırlığı
$w_{\max}$	Kodun mksimum ağırlığı
support (v)	v vektörünün sıfırdan farklı bileşenlerinin kümesi
P_i	$i.$ kullanıcı
π	Vektör izomorfizması

$d(C)$	C kodun herhangi iki vektörü arasındaki sıfırdan farklı uzaklıkların en küçüğü
$w(C)$	C kodun sıfırdan farklı kodsözlerinin ağırlıklarının en küçüğü
G	Üreteç matris
H	Kontrol matrisi
I_n	n satır ve n sütundan oluşan birim matris
F_q^*	$\{1,...,q-1\}$ elemanlarından oluşan sonlu cisim
$M^i(x)$	α_i 'ye karşılık gelen minimal polinom
(k,n)	Eşik değer, n parçadan k tanesi
D	Dağıtıcı, sistemi kuran kişi
K	Anahtarlar kümesi
s	Sistemi çözebilen anahtar
$ebob(m_i,m_j)$	Verilen iki sayının en büyük ortak böleni
Γ	Anahtarı oluşturabilecek kullanıcıların oluşturduğu alt kümelerin tümü
$\overline{\Gamma}$	Anahtarı oluşturamayacak kullanıcıların oluşturduğu alt kümelerin tümü
$\Gamma_{\min}$	Γ 'da ki bütün minimal kümeler
$\overline{\Gamma}_{\max}$	Γ 'da ki bütün maksimal kümeler
ρ	Tekrar derecesi
θ	Farklı paket sayısı
$S(t,\alpha,v)$	Steiner Sistem
C_{MBR}	Depolama kapasitesi
$R_C(k)$	FR kod oranı
$R_{n,d}$	n düğümlü $d.$ dereceden düzenli graf

KISALTMA LİSTESİ

RS Kod	Reed Solomon Kod
MDS Kod	Maximum Distance Seperable Kod
FR Kod	Fractional Repetition Kod
DS Sistem	Distributed Storage System

ŞEKİL LİSTESİ

Sayfa

ÖZET

SIR PAYLAŞIM SİSTEMLERİ

İbrahim ÖZBEK

Matematik Anabilim Dalı
Yüksek Lisans Tezi

Tez Danışmanı: Prof. Dr. İrfan ŞİAP

Teknolojinin gelişmesiyle birlikte günlük hayatta şifrelemenin yani güvenliğin önemi artmaktadır. Bu nedenle birçok şifreleme sistemi geliştirilmektedir. Şifreleme sitemlerinin kırılmaya karşı üst düzey şekilde geliştirilmesi anahtar güvenliğinin önemini arttırmaktadır. (Bazı sitemlerin çözülmesi bilgisayar yardımıyla bile yıllar sürebilir)

Anahtar güvenliği, sistemin güvenlik derecesi olduğundan anahtar saklama yöntemleri geliştirilmiştir. İlk olarak akla gelen anahtarın kopyalanmasıdır fakat dezavantajları çoktur. İkinci olarak ise anahtarın parçalanması ve son olarakta sır paylaşım yöntemi geliştirilmiştir.

Sır paylaşım sisteminin temel kurallarını kullanarak geliştirilen yöntemler üzerinde duracağımız bu tez çalışmasında ilk olarak Shamir ve Blakley 'in birbirinden bağımsız olarak bulduğu interpolasyon yönteminden bahsedilecek.

İkinci olarak, ilk yöntemin genellemesi olan Mceliece ve Sarwate tarafından geliştirilen Reed Solomon kodlarla birleştirilen yöntem anlatılacak. Bu yöntemin temel noktası Reed Solomon kodların kodlama şemasıdır. Kodlama teorisine girildiğinden birçok avantajı vardır.

Üçüncü olarak, Çin Kalan Teorimini kullanarak geliştirilen ve özel sırada tam sayı dizilerinin kullanılmasıyla inşa edilen sistemden bahsedilecek.

Dördüncü olarak Massey'in geliştirdiği, lineer kod ve erişim kümesi arasında birebir eşleme yakalanarak anahtarın daha hızlı inşa edilebildiği sistemden bahsedilecek. Bu yöntem sayesinde sır paylaşım sistemi bütün lineer kodlar için uygulanabilir hale gelmiştir.

Son olarakta Fractional Repetition Kod ile ilgili temel tanım ve teoremleri vereceğiz ve Fractional Repetition Kod üzerinde Sır Paylaşım Sistemini tanımlayacağız.

Anahtar Kelimeler: Anahtar Saklama Yöntemleri, Sır Paylaşım Sistemi, Çin Kalan Teoremi, Erişim Kümesi, Minimal Kodsöz, Lineer Kodlar, Reed Solomon Kod, FR Kod

ABSTRACT

SECRET SHARING SCHEMES

İbrahim ÖZBEK

Department of Mathematics

MSc. Thesis

Advisor: Prof. Dr. İrfan ŞİAP

Encryption or security of digital data have become increasingly important with the development of technology in daily life. Therefore, many encryption systems are being enhanced. Key security increases the importance of development of high-level manner against breakage encryption systems (Some systems may take years to resolve, even with the help of a computer).

As key security determines the degree of a security of system, key keeping methods have been improved. The first solution that comes to mind is copying the key, but there are many disadvantages. The second is disintegration of key, and finally secret sharing method is improved.

In this thesis, we will focus on developed methods for secret sharing system using the basic rules. Firstly, we point out that interpolation method is put forward independently by Shamir and Blakley.

Secondly, as a generalization of the first method, we present the method which uses Reed Solomon codes developed by McEliece and Sarwate. The main point of this method is the coding scheme for Reed Solomon codes. It is shown that there are many advantages due to coding theory.

Thirdly, we present the construction systems using Chinese remainder theorem and integer arrays of the specific order.

Fourthly, we present that key systems can be constructed more quickly when a one to one mapping is established between the linear code and access sets developed by Massey. Secret sharing system has become feasible for all linear codes.

Finally, we give some basic definitions and theorems about Fractional Repetition Codes. Next, we introduce a new method for constructing a secret-sharing scheme by making use of Fractional Repetition Codes.

Key words: Key Storage Methods, Secret Sharing Scheme, Access Structure, Minimal Codeword, Linear Codes, Reed Solomon Code, Fractional Repetition Codes

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

Şifreleme yöntemlerinin gelişmesiyle birlikte anahtarın güvenli bir biçimde saklanması problemi ortaya çıkmıştır [4]. Kullanılan farklı anahtar saklam yöntemleri olmasına rağmen güvenlik zafiyetinin çok olması veya yöntemin kullanışsız olması nedeniyle ortaya atılan problem, ilk defa birbirinden bağımsız bir biçimde Shamir ve Blakley tarafından 1979 da çözülmüştür [8,9]. Temel mantığın anahtarı parçalamak ve daha az kullanıcıyla tekrar oluşturmak olan ve (k, n) eşik değer olarak adlandırılan bu sisteme Shamir 'in çözüm yöntemi İnterpolasyon formülü, Blakley 'in ise hiper düzlemlerin kesişimi olmuştur. İkinci olarak 1981' de McElice ve Sarwate tarafından Reed Solomon kodları kullanarak geliştirilen sistemdir [12]. Aslında bu yöntem Reed Solomon kodların kodlama şemasının bir özelliğidir. Kodlama teorisine girilmesiyle daha kullanışlı hale gelen bu yöntem sayesinde hatalı kullanıcılara karşı sistem garanti altına alınmaya çalışılmıştır. Zamanla sisteme farklı çözümler getirilmiştir. Farklı parçaları birleştirerek anahtarı oluşturmaya çalıştığımızdan, Çin Kalan teoremi özel sırada dizilerle bir çözüm olmuştur. Assmuth Bloom ve Magnette iki farklı yöntem geliştirmiştir [14]. Daha sonra Massey tarafından 1993'te geliştirilen yöntem sayesinde sır paylaşım sistemi lineer kodların tamamında uygulanabilir hale gelmiştir [19]. Bu yöntem sayesinde erişim kümeleriyle minimal kodsözler arasında birebir eşleme yakalanmıştır. Son olarak bizim geliştirdiğimiz yöntem olan FR Kod ile Sır Paylaşım Sistemi ile, yeni inşa edilen kod üzerinde yeni bir yöntem tanımlanmıştır. Bu yöntem RS kod yönteminde ki gibi hatalı kullanıcılara karşı dayanıklıdır ve anahtar daha

genel bir haldedir. Anahtar kodlama yapılarak paketlere aktarılır ve düzenli tekrar edecek biçimde sistem kurulur.

1.2 Tezin Amacı

Bu tez, Kodlama Teorisi alanında çalışan veya yeni çalışmaya başlayan herkesin yararlanabilmesi amacıyla hazırlanmıştır. Bu çalışmada öncelikle Kodlama Teorisinin temel kavramları anlaşılır şekilde anlatılmış ve anahtar saklama yöntemlerinden bahsedilmiştir.

Bu ön çalışmalardan sonra asıl konumuz olan Sır Paylaşım Yöntemlerinden dört tanesi açıkça anlatılmış ve özgün örneklerle daha da basit hale getirilmeye çalışılmıştır. Son bölümde ise yeni inşa edilen Fractional Repetition Kod üzerinde Sır Paylaşım Sistemi tanımlanmıştır. Bu yapıyla birlikte yeni bir yöntem geliştirilmeye çalışılmıştır.

1.3 Hipotez

Şifrelemenin amacı sistemin güvenliğini sağlamaktır. Bu yüzden çok üst düzey sistemler kullanılmakta ve yasal olmayan kişiler tarafından anahtarın ele geçirilmemesi için de anahtar saklama yöntemleri geliştirilmektedir. Bu sistemler arasında en kullanışlı ve güvenli olanı Sır Paylaşım Yöntemidir.

Sır Paylaşım Sisteminin iki temel kuralı vardır ve aslında çözülmeyi beklen bir problemdir. Şimdiye kadar yapılan çalışmalarda farklı çözüm yöntemleri geliştirilmiştir. Bundan sonrası adına farklı konularla bağlantısı sağlanabilir ve yeni inşa edilen kodlar üzerine uygulanabilir. Biz tezde yeni inşa edilen Fractional Repetition Kod üzerinde yeni bir yöntem geliştirmeye çalıştık. Ayrıca daha önce yapılmamış olan, halkalar üzerine tanımlanmış kodlar üzerine sistemi inceledik ve kendine dual kodlar üzerinde sistemin daha hızlı işleyebileceği üzerine çalışmalar yaptık.

BÖLÜM 2

LİNEER KODLAR

Bu bölümde Kodlama Teorisiyle alakalı temel tanımlamalar yapılacaktır. Öncelikle sonlu cisimlere giriş yapılacak, daha sonra kod ve lineer kod kavramları anlatılacaktır. Son bölümde lineer kodların özel bir sınıfı olan devirli kodlar kısa bir biçimde anlatılacaktır.

2.1 Sonlu Cisimler Üzerinde Vektör Uzayları

Tanım 2.1 F_q, eleman sayısı q olan bir sonlu cisim olsun ve her $v, w \in \mathrm{F}_q{}^n$ için vektör toplamı ve skaler çarpımı

$$+ : \mathrm{F}_q{}^n \times \mathrm{F}_q{}^n \to \mathrm{F}_q{}^n$$
$$v + w \mapsto (v_1 + w_1, \ldots, v_n + w_n)$$

$$\cdot : \mathrm{F}_q \times \mathrm{F}_q{}^n \to \mathrm{F}_q{}^n$$
$$\lambda v \mapsto (\lambda v_1, \ldots, \lambda v_n)$$

şeklinde tanımlansın. Buna göre boştan farklı bir V kümesi + ve $\cdot$ işlemleri ile aşağıdaki özellikleri sağlıyorsa V ye F_q üzerinde bir vektör uzayı (ya da lineer uzay) denir [1].

Her $u, v, w \in V$ ve her $\lambda, \mu \in \mathrm{F}_q$ için;

i. $u + v \in V$;

ii. $(u + v) + w = u + (v + w)$;

iii. Her $v \in V$ için $0 + v = v + 0 = v$ olacak şekilde bir $0 \in V$ vardır;

iv. Her $u \in V$ için $u + (-u) = 0 = (-u) + u$ olacak şekilde $-u \in V$ vardır;

v. $u+v=v+u$;

vi. $\lambda v \in V$;

vii. $\lambda(u+v)=\lambda u+\lambda v$ ve $(\lambda+\mu)u=\lambda u+\mu u$;

viii. $(\lambda\mu)u=\lambda(\mu u)$;

ix. 1, F_q nin çarmaya göre etkisiz elemanı ise $1u=u$.

Buradaki $\mathrm{F}_q{}^n$ vektör uzayının elemanları $v=\{v_1,v_2,v_3,...v_n\}$ şeklinde olduğundan toplama ve çarpma işlemleri sırasıyla $v,w\in \mathrm{F}_q{}^n$ için

$v+w=(v_1+w_1,...,v_n+w_n)$, $vw=(v_1\cdot w_1,...,v_n\cdot w_n)\in \mathrm{F}_q{}^n$ şeklindedir.

Örnek 2.1

i. $C_1=\{000,101,010,111\}$, F_2 üzerinde bir vektör uzayıdır.

ii. Her q için $C_2=\{(\lambda,\lambda,...,\lambda)\,|\,\lambda\in \mathrm{F}_q\}$ kümesi F_q üzerinde bir vektör uzayıdır.

Tanım 2.2 V vektör uzayının boştan farklı bir C alt kümesi aynı vektör toplamı ve skalerle çarpım altında bir vektör uzayı ise C ye V nin bir alt vektör uzayı denir [1].

Örnek 2.2 Örnek 2.1 deki C_1 ve C_2 alt kümeleri sırasıyla $\mathrm{F}_2{}^n$ nin ve $\mathrm{F}_q{}^n$ nin alt vektör uzaylarıdır.

Önerme 2.1 F_q üzerinde bir V vektör uzayının boştan farklı bir C alt kümesinin bir alt uzay olması için gerek ve yeter koşul $\forall x,y\in C$ ve $\forall\lambda,\mu\in \mathrm{F}_q$ için $\lambda x+\mu y\in C$ olmasıdır [1].

Tanım 2.3 V, F_q üzerinde bir vektör uzayı olsun. $v_1,...,v_r\in V$ vektörlerinin bir lineer kombinasyonu, $\lambda_1,...,\lambda_r$, F_q'nun bazı skaler elemanları olmak üzere $\lambda_1v_1+...+\lambda_rv_r$ şeklinde bir vektördür [1].

Tanım 2.4 V, F_q üzerinde bir vektör uzayı olsun. $\lambda_1v_1+...+\lambda_rv_r=0$ için tek çözüm $\lambda_1=...=\lambda_r=0$ oluyorsa $\{v_1,...,v_r\}$ vektörler kümesi V de lineer bağımsızdır denir.

Lineer bağımsız olmayan kümeye ise lineer bağımlıdır denir.

Örnek 2.3

i. 0 vektörünü içeren her S kümesi lineer bağımlıdır.

ii. Herhangi bir F_q cismi için $\{001, 010, 100\}$ lineer bağımsızdır.

Tanım 2.5 V , F_q üzerinde bir vektör uzayı ve $S = \{v_1, v_2, ..., v_k\}$, V nin boştan farklı bir alt kümesi olsun. S nin (lineer) üreteci $\langle S \rangle = \{\lambda_1 v_1 + ... + \lambda_k v_k \mid \lambda_i \in \mathrm{F}_q\}$ şeklinde tanımlıdır [1].

Eğer $S = \varnothing$ ise $\langle S \rangle = \{0\}$ dir.

Eğer $C = \langle S \rangle$ ise C nin S alt kümesine üreteç küme denir.

Örnek 2.4

i. $q = 3$ ve $S = \{0001, 0010\}$ ise

$\langle S \rangle = \{0000, 0001, 0010, 0002, 0020, 0021, 0011, 0012, 0022\}$ dir.

ii. $q = 5$ ve $S = \{001, 100\}$ ise

$\langle S \rangle = \{000, 001, 100, 002, 200, 003, 300, 004, 400, 101, 201, 301, 401, 102, 202$

$302, 402, 103, 203, 303, 403, 104, 204, 304, 404\}$

Tanım 2.6 V , F_q üzerinde bir vektör uzayı olsun.

i. $V = \langle B \rangle$ ise B lineer bağımsız alt kümesine V için bir taban denir.

V nin B tabanının eleman sayısına V nin boyutu denir ve $boy(V)$ ile gösterilir. B sonsuz elemanlı ise $boy(V) = \infty$ ile gösterilir [1].

Tanım 2.7 $v = (v_1, ..., v_n)$ ve $w = (w_1, ..., w_n) \in \mathrm{F}_q{}^n$ olsun.

i. v ile w'nin skaler çarpımı $v \cdot w = v_1 w_1 + ... + v_n w_n \in \mathrm{F}_q$ ya da $\langle v, w \rangle$ şeklinde tanımlanır.

ii. $v \cdot w = 0$ ise v ile w vektörleri diktir denir.

iii. S, $\mathrm{F}_q{}^n$'nin bir alt kümesi olmak üzere S nin dikey tümleyeni (ortogonali) $S^{\perp} = \left\{ v \in \mathrm{F}_q{}^n \mid v \cdot s = 0, \forall s \in S \right\}$ şeklinde tanımlanır [1].

Örnek 2.5

$q = 3$ ve $S = \{0001, 1000\}$ için $S^{\perp}$ kümesini bulalım.

Biliyoruz ki aldığımız her $v = (v_1, v_2, v_3, v_4) \in \mathrm{F}_3^4$ için $S^{\perp}$ kümesinin bütün elemanlarıyla skaler çarpımı sıfır olacaktır.

$v \cdot (0,0,0,1) = 0 \Rightarrow v_4 = 0$

$v \cdot (1,0,0,0) = 0 \Rightarrow v_1 = 0$

Buradan $q = 3$ için v_2, v_3 3 farklı değer alabileceğinden

$S^{\perp} = \{0000, 0100, 0010, 0110, 0200, 0020, 0210, 0120, 0220\}$ olarak bulunur.

Sonuç 2.1 Eğer $S = \varnothing$ ise $S^{\perp} = \mathrm{F}_q{}^n$ dir.

Teorem 2.2 $\mathrm{F}_q{}^n$ nin her S alt kümesi için $boy\left(\langle S \rangle\right) + boy\left(\langle S \rangle^{\perp}\right) = n$ dir [2].

İspat $S = \varnothing$ ise $S^{\perp} = \mathrm{F}_q{}^n$ olduğundan ifade doğru olur.

Şimdi kabul edelim ki $boy\left(\langle S \rangle\right) = k \geq 1$ olsun $boy\left(\langle S \rangle^{\perp}\right) = n - k$ olduğunu göstermeliyiz. $boy\left(\langle S \rangle\right) = k \geq 1$ olduğundan $\langle S \rangle$ nin tabanı olacak şekilde $v = \{v_1, \ldots, v_k\}$ vardır. $x \in S^{\perp}$ için

$v_1 \cdot x = \ldots = v_k \cdot x = 0$ olur.

$$\underbrace{\begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix}_{k \times n}}_{A} \cdot \underbrace{\begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}_{n \times 1}}_{X} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}_{k \times 1}$$

şeklinde yazılabileceğinden ve $rank(A)=k$ olduğundan çözüm uzayının boyutu $n-k$ olup bu da $\langle S\rangle^{\perp}$ in boyutudur. Yani $boy\left(\langle S\rangle^{\perp}\right)=n-k$ dır.

Örnek 2.6 $q=3$, $n=4$ ve $S=\{0001,1000\}$ olsun. S lineer bağımsız olduğundan $boy\left(\langle S\rangle\right)=|S|=2$ dir. $S^{\perp}=\{0000,0100,0010,0110,0200,0020,0210,0120,0220,\}$ olarak bulunur. $S^{\perp}$ için bir taban $\{0100,0010\}$ dir. Bu nedenle $boy\left(S^{\perp}\right)=2$ dir. Böylece $boy\left(\langle S\rangle\right)+boy\left(\langle S\rangle^{\perp}\right)=2+2=4=n$ bulunur.

2.2 Lineer Kodlar

Tanım 2.8 $A=\{a_1,a_2,...,a_q\}$ sonlu bir küme olsun. $\varnothing\neq C\subseteq A^n$ kümesine n uzunluğunda bir kod denir. C nin elemanlarına kodsöz ve A^n nin elemanlarına ise söz denir. C nin eleman sayısı $|C|$, n uzunluğunda $|C|=M$ olan kod $(n,M)-kod$ diye kısaca gösterilir [1].

Tanım 2.9 F_q üzerinde uzunluğu n, boyutu k olan bir C lineer kodu, F_q^n uzayının bir alt uzayıdır. Böyle bir kod $[n,k]_q-$ kod şeklinde gösterilir. Özel olarak, $q=2$ iken F_2 üzerinde bir koda ikili kod; $q=3$ iken F_3 üzerinde bir koda üçlü kod denir [1].

Örnek 2.6

i. $q=2$ için $C=\{00000,10000,01000,11000\}$ kodu $\mathrm{F}_2{}^5$ nin bir alt uzayı olduğundan bir ikili lineer koddur.

ii. $q=3$ için $C=\{000,200,100,012,021,212,112,221,121\}$ kodu $\mathrm{F}_3{}^3$ nin bir alt uzayı olduğundan bir üçlü lineer koddur.

Tanım 2.10 C, F_q üzerinde tanımlı bir lineer kod olsun.

i. C nin dual kodu $C^{\perp}$, $\mathrm{F}_q{}^n$'nin alt uzayı olan C'nin dikey tümleyenidir. $C^{\perp}=\{x\in\mathrm{F}_q^n:\langle x,c\rangle=x_1c_1+...x_nc_n=0,\forall c\in C\}$ şeklinde tanımlanır [2].

ii. C lineer kodunun boyutu, C nin F_q üzerinde vektör uzayı olarak boyutudur, yani tabanının eleman sayısıdır ve $boy(C)$ ile gösterilir [1].

Not 2.3 C kodunun F_q üzerinde tanımlandığı biliniyorsa n uzunluklu, M elemanlı bir kod $(n,M)-$ kod olarak; n uzunluklu, k boyutlu lineer bir kod $[n,k]-$ kod olarak gösterilir.

Teorem 2.3 C , $\mathrm{F}_q^{\,n}$ üzerinde boyutu k olan bir lineer kod olsun.

i. $|C| = q^{boy(C)} \quad \left(M = q^k\right)$, diğer bir ifadeyle $boy(C) = \log_q |C|$ dir.

ii. $C^{\perp}$ bir lineer koddur ve $boy(C) + boy\left(C^{\perp}\right) = n$,

iii. $\left(C^{\perp}\right)^{\perp} = C$ [1] .

İspat:

i. C kodun vektör uzayı olarak bir tabanı $\{c_1, c_2, \ldots, c_k\}$ olsun. O halde, $C = \left\{\lambda_1 c_1 + \lambda_2 c_2 + \ldots + \lambda_k c_k \mid \lambda_1, \lambda_2, \ldots, \lambda_k \in \mathrm{F}_q\right\}$ yazılır. $\left|\mathrm{F}_q\right| = q$ olduğundan her bir λ_i için q seçenek vardır. O halde C nin q^k elemanı vardır.

ii. $C^{\perp} = \left\{x \in \mathrm{F}_q^{\,n} \mid \langle x, c\rangle = 0, \forall c \in C\right\}$ nin lineer kod olduğunu göstermek için $\mathrm{F}_q^{\,n}$ vektör uzayının bir alt uzayı olduğu gösterilmelidir.

- $x, y \in C^{\perp}$ olsun. Yani, $\forall c \in C$ için $\langle x, c\rangle = 0$ ve $\forall c \in C$ için $\langle y, c\rangle = 0$ dir. $\forall c \in C$ için $\langle x + y, c\rangle = \langle x, c\rangle + \langle y, c\rangle = 0 \Rightarrow x + y \in C^{\perp}$ dir.

- $x \in C^{\perp}$ olsun. Yani, $\forall c \in C$ için $\langle x, c\rangle = 0$ dir. $\forall c \in C$ ve $\alpha \in \mathrm{F}_q$ için $\langle \alpha x, c\rangle = \alpha \langle x, c\rangle = 0$ olduğundan $\alpha x \in C^{\perp}$ dir.

O halde $C^{\perp}$, $\mathrm{F}_q^{\,n}$ vektör uzayının bir alt uzayıdır, yani bir lineer koddur.

$C = \{0\}$ ise $\mathrm{F}_q^{\,n}$ deki tüm vektörler C ye diktir. Dolayısıyla $\mathrm{F}_q^{\,n} = C^{\perp}$ elde edilir. Böylece $boy(C) + boy\left(C^{\perp}\right) = 0 + n = n$ elde edilir.

$boy(C)=k\geq 1$ olduğunu ve C nin bir tabanı $\{c_1,c_2,\ldots,c_k\}$ olduğunu kabul edelim. Bu durumda $x\in C^{\perp}$ olması için gerek ve yeter koşul $\langle c_1,x\rangle=\langle c_2,x\rangle=\ldots=\langle c_k,x\rangle=0$ olmasıdır. $\{c_1,c_2,\ldots,c_k\}$ tabanının elemanlarını satır kabul eden matris A olsun. $A=\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix}$ ise $Ax^T=0$ dir. Burada n bilinmeyenli k lineer bağımsız denklem olduğundan bu sistemin $n-k$ tane çözümü vardır. Dolayısıyla $C^{\perp}$ uzayının boyutu $n-k$ dir. Böylece $boy(C)+boy(C^{\perp})=k+(n-k)=n$ elde edilir.

iii. $c\in C$ olsun. Bu durumda $\forall d\in C^{\perp}$ için $\langle c,d\rangle=0$ dir. Buradan $\langle d,c\rangle=0$ yazabiliriz. Bu ise $c\in(C^{\perp})^{\perp}$ demektir.

Öte yandan C bir $[n,k]-$kod olduğundan $C^{\perp}$, $[n,n-k]-$koddur. $|(C^{\perp})^{\perp}|=q^k=|C|$ dir. Buradan, $(C^{\perp})^{\perp}=C$ elde edilir.

Örnek 2.7 $q=3$ için $C=\{000,200,100,012,021,212,112,221,121\}$

$M=9=3^k$ olduğundan $k=2$ olur. $C^{\perp}=\{x\in \mathrm{F}_3^3 \mid \langle x,c\rangle=0,\forall c\in C\}$ dir.

$$\left.\begin{array}{ll} \langle x,000\rangle=0, & \langle x,021\rangle=0 \\ \langle x,200\rangle=0, & \langle x,212\rangle=0 \\ \langle x,100\rangle=0, & \langle x,112\rangle=0 \\ \langle x,012\rangle=0, & \langle x,221\rangle=0 \\ \langle x,121\rangle=0, & \end{array}\right\} \Rightarrow \begin{array}{c} x_1=0 \\ x_2+2x_3=0 \\ 2x_2+x_3=0 \end{array}$$

$C^{\perp}=\{(0,l,l):l\in \mathbf{Z}_3\}=\{l(0,1,1)\mid l\in \mathbf{Z}_3\}$ olduğundan $C^{\perp}=\{000,011,022\}$ dir.

Tanım 2.11 C, F_q üzerinde bir lineer kod olsun. $C\subseteq C^{\perp}$ ise C ye kendine dik (ortogonal) kod; $C=C^{\perp}$ ise C ye kendine dual kod denir [2].

Önerme 2.3 Kendine dual bir kodun uzunluğu çifttir ve boyutu $k=\frac{n}{2}$ dir [1].

İspat: Teorem 2.3 ii' nin bir sonucu olarak ve kendine dual kodun tanımından faydalanarak $C = C^{\perp}$ ise $k = n - k$ olmalıdır. Buradan $2k = n$ ve $k = \frac{n}{2}$ elde edilir.

2.3 Hamming Ağırlık ve Hamming Uzaklık

Tanım 2.12 $x = (x_1, x_2, \ldots, x_n)$ ve $y = (y_1, y_2, \ldots, y_n) \in \mathrm{F}_q^n$ için x ile y arasındaki Hamming uzaklık $d(x, y) = d(x_1, y_1) + d(x_2, y_2) + \ldots + d(x_n, y_n)$ dir. Burada,

$d(x_i, y_i) = \begin{cases} 1, & x_i \neq y_i \\ 0, & x_i = y_i \end{cases}$ şeklinde tanımlanır. Diğer bir ifadeyle, $d(x, y) = \left|\{i : x_i \neq y_i\}\right|$ dir [1].

Örnek 2.9

i. F_2 üzerinde $x = (1011100)$ ve $y = (0111110)$ için $d(x, y) = 3$ dir.

ii. F_3 üzerinde $x = (102220)$ ve $y = (002210)$ için $d(x, y) = 2$ dir.

Tanım 2.13 $\mathrm{F}_q{}^n$ deki bir x sözünün Hamming ağırlığı sıfırdan farklı koordinatlarının (bileşenlerinin) sayısı $w(x) = \left|\{i \mid x_i \neq 0\}\right|$ olarak tanımlanır [1].

Örnek 2.10 F_2 üzerinde $x = (1011100)$ için $w(x) = 4$ iken F_3 üzerinde $x = (1022201)$ için $w(x) = 5$ dir.

Not 2.4 F_q sonlu cismindeki her a elemanı için Hamming ağırlık, $w(a) = d(a, 0) = \begin{cases} 1, & a \neq 0 \\ 0, & a = 0 \end{cases}$ şeklinde tanımlanabilir [1].

Bundan yararlanarak $\mathrm{F}_q{}^n$ deki bir $x = (x_1, x_2, \ldots, x_n)$ sözünün Hamming ağırlığı $w(x) = w(x_1) + \ldots + w(x_n)$ olarak hesaplanabilir.

Teorem 2.5 Her $x, y \in \mathrm{F}_q^n$ için $d(x, y) = w(x - y)$ dir [2].

İspat: $x, y \in \mathrm{F}_q^n$ olsun.

$$
\begin{aligned}
d(x,y) &= d(x_1,y_1)+d(x_2,y_2)+\ldots+d(x_n,y_n)\\
&= d(x_1-y_1,0)+d(x_2-y_2,0)+\ldots+d(x_n-y_n,0)\\
&= w(x_1-y_1)+w(x_2-y_2)+\ldots+w(x_n-y_n)\\
&= w(x-y).
\end{aligned}
$$

Tanım 2.15 C bir kod olsun (lineer olması zorunlu değil). C nin minimum (Hamming) ağırlığı sıfırdan farklı tüm kodsözlerinin ağırlıklarının en küçüğüdür ve $w(C)$ ile gösterilir.

Tanım 2.16 $\mathrm{F}_q^{\,n}$ üzerinde bir C kodun minimum uzaklığı,

$d_{\min}(C) = d(C) = \min\{d(x,y) \mid x \neq y, \forall x, y \in C\}$ şeklinde tanımlanır. Minimum uzaklığı d olan bir $[n,k]_q$ – kod, $[n,k,d]_q$ – kod ile gösterilir [2].

Teorem 2.6 C , F_q üzerinde bir lineer kod ise $d(C) = w(C)$ dir.

İspat: Minimum uzaklık tanımından $d(C) = d(x', y')$ olacak şekilde en az bir $x', y' \in C$ vardır. Buradan $d(C) = d(x', y') = w(x' - y') \geq w(C)$ elde edilir.

Tersine, $w(C) = w(z)$ olacak şekilde $\exists z \in C - \{0\}$ vardır. Buradan $w(C) = w(z) = d(z,0) \geq d(C)$ elde edilir.

2.4 Üreteç Matrisi ve Kontrol Matrisi

Tanım 2.17

i. Bir C lineer kodu, $\mathrm{F}_q^{\,n}$ uzayının bir alt uzayı olduğundan bir bazı vardır. C nin bir $\{c_1, c_2, \ldots, c_k\}$ bazındaki vektörleri satır kabul eden G matrisine, C kodunun üreteç matrisi

denir ve $G = \begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_k \end{bmatrix}_{k \times n}$ ile gösterilir.

Dolayısıyla C deki her kodsöz G' nin satırlarının bir F_q lineer kombinasyonu olarak yazılabilir.

ii. C lineer kodun kontrol matrisi H, $C^{\perp}$ dual kodun üreteç matrisidir. H ile gösterilen bu matris $\forall x \in C$ için $H \cdot x^T = 0$ eşitliğini sağlar [1].

Not 2.6

i. C bir $[n,k]-$ lineer kod ise G üreteç matrisi $k \times n$, H kontrol matrisi $(n-k)\times n$ formundadır.

ii. G ve H nin satırları lineer bağımsızdır.

Örnek 2.12 $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}_{3\times 3}$ matrisinin ürettiği C kodu $q^k = 2^3 = 8$ elemanlıdır. C bir $[3,3]_2 -$ koddur.

$C = \{\alpha c_1 + \beta c_2 + \delta c_3 : \alpha, \beta, \delta \in \mathbf{Z}_2\} = \{000,100,010,001,101,110,011,111\}$ dir.

Tanım 2.18 C üreteç matrisi G olan bir $[n,k]_q -$ kod olsun. Bu durumda;

i. $G = [I_k \mid A]_{k\times n}$ ise G nin standart formda olduğu söylenir. Burada, I_k, $k \times k$ tipinde birim matris; A ise $k \times (n-k)$ tipinde bir matristir [1].

ii. $H = [-A^T \mid I_{n-k}]_{(n-k)\times n}$ ise H standart formdadır [1].

Örnek 2.13 Bir C, $[4,2]_3 -$ kodu $G = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ üreteç matris ile üretilsin.

$G = \begin{bmatrix} 1 & 0 & 2 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$ olduğundan $-A^T = \begin{bmatrix} 1 & 0 \\ 2 & 2 \end{bmatrix}$ olur. Bu durumda C kodun H kontrol matrisi $H = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 1 \end{bmatrix}$ bulunur.

Önerme 2.10 C, G tarafından üretilen $\mathrm{F}_q{}^n$ üzerinde bir $[n,k]-$ lineer kod olsun. Bu durumda her $v \in \mathrm{F}_q{}^n$ için $v \in C^{\perp}$ olması için gerek ve yeter koşul $vG^T = 0$ olmasıdır [2].

Özel olarak verilen bir $(n-k)\times n$ tipinde H matrisinin C kodun kontrol matrisi olması için gerek ve yeter koşul H nin satırlarının lineer bağımsız olması ve $HG^T = 0$ olmasıdır [1].

Örnek 2.14 Bu örnekte kontrol matrisi verilen bir kodun üreteç matrisini bulalım ve kodsözlerini yazalım.

Kontol matrisi

$$H = \begin{bmatrix} 2 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}_{2x4}$$

olsun. Kontol matrisindeki her satır üreteç matrisindeki her bir satıra dik olacağından, $v = \{v_1, v_2, v_3, v_4\} \in C$ için şu şekilde yazılabilir:

$$\left.\begin{array}{l} \langle 2101, v\rangle = 0 \\ \langle 0010, v\rangle = 0 \end{array}\right\} \Rightarrow 2v_1 + v_2 + v_4 = 0,\ v_3 = 0$$

Şimdi ise bir lineer denklem sistemi çözülmelidir. 4 tane bilinmeyen 2 tane denklem olduğundan lineer cebirden biliyoruz ki sistemin çözümü için $4-2=2$ tane keyfi değer verilir. Biz $v_2 = l, v_4 = k$ olarak şeçelim. Buradan $v_1 = l + k$ olarak bulunur. Elde edilenlerle artık üreteç matrisi ve kodsözleri bulabiliriz.

$$C = \{(l+k, l, 0, k) \mid l, k \in \mathrm{F}_3\} = \{l(1,1,0,0) + k(1,0,0,1) \mid l, k \in \mathrm{F}_3\}$$

ve $S = \{(1,1,0,0), (1,0,0,1)\}$ olarak aldığımızda C kodunu ürettiğini ve lineer bağımsız olduğu kolayca görülüyor. Üreteç matris ve kodsözler şu şekilde yazılır:

$$G = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}_{2x4}$$

$$C = \{0000, 1100, 1001, 2200, 2002, 1101, 0201, 0102, 1202\}$$

Teorem 2.8 C bir lineer kod ve H, C nin bir kontrol matrisi olsun.

i. C nin mimimum uzaklığının $\geq d$ olması için gerek ve yeter koşul H nin herhangi $d-1$ sütununun lineer bağımsız olmasıdır [1].

ii. C nin minimum uzaklığının $\leq d$ olması için gerek ve yeter koşul H nin en az bir d sütununun lineer bağımlı olmasıdır [1].

Tanım 2.19 F_q^n uzayı üzerinde uzunluğu n, boyutu k ve minimum uzaklığı d olan bir lineer kod $[n,k,d]_q$ parametreleriyle gösterilir [1].

Örnek 2.15 F_3 cismi üzerinde tanımlı C kodun kontrol matrisi

$H=\begin{pmatrix}1&0&0&1\\0&1&0&1\\0&2&1&0\end{pmatrix}_{3x4}$ olsun. $2H_1+2H_3+H_4=H_2$, yani $1.,2.,3.$ ve $4.$ sütunlar lineer bağımlıdır. Bu nedenle $d(C)\leq 4$ dir. Her üç sütun lineer bağımsız olduğundan $d(C)\geq 3$ dir. O halde $d(C)=w(C)=4$ bulunur.

Örnek 2.16 Bu örnekte F_3 cismi üzerinde tanımlı standart formda verilmeyen üreteç matrisi için kontol matrisini bulmayı göstereceğiz.

Bir C kodun üreteç matrisi olarak verilen $G=\begin{bmatrix}1&1&1&2&0\\0&0&1&1&1\\2&0&2&0&1\end{bmatrix}$ matrisi

$$G=\begin{bmatrix}1&1&1&2&0\\0&0&1&1&1\\2&0&2&0&1\end{bmatrix}\underset{H_{31}(1)}{\square}\begin{bmatrix}1&1&1&2&0\\0&0&1&1&1\\0&1&0&2&1\end{bmatrix}\underset{H_{13}(2)}{\square}\begin{bmatrix}1&0&1&0&2\\0&0&1&1&1\\0&1&0&2&1\end{bmatrix}\underset{H_{12}(2)}{\square}\begin{bmatrix}1&0&0&2&1\\0&0&1&1&1\\0&1&0&2&1\end{bmatrix}$$

şekline gelir ve son olarak ikinci ve üçüncü satırları yer değiştirirsek standart forma gelir. Buradan $A=\begin{pmatrix}2&1\\2&1\\1&1\end{pmatrix}$ olur. O halde $-A^T=\begin{bmatrix}1&1&2\\2&2&2\end{bmatrix}$ dir. Bu C kodu için bir kontrol matrisi, $H=\begin{bmatrix}1&1&2&1&0\\2&2&2&0&1\end{bmatrix}$ dir.

Not 2.10 $H_{ij}(a)$ ile j. Satırın a ile çarpılıp i. satıra eklenmesi işlemi gösterilmiştir.

Örnek 2.17 $H=\begin{bmatrix}1&0&0&1&1&0&1\\0&1&0&1&0&1&1\\0&0&1&0&1&1&1\end{bmatrix}_{3\times 7}$ kontrol matrisi ile verilen C kodu bir $[7,4]_2-$ koddur. Bu durumda $C=\{x\in \mathrm{F}_2^7 \mid Hx^T=0\}$ dir. Buradan elde edilen denklem sistemi 7 bilinmeyenli 3 denklemden oluştuğundan 4 tane keyfi sabit olacaktır. Bu sabitler k,l,m,n olmak üzere,

$$\begin{matrix}x_1+x_4+x_5+x_7=0\\x_2+x_4+x_6+x_7=0\\x_3+x_5+x_6+x_7=0\end{matrix} \quad \text{için} \quad \begin{matrix}x_4=k & x_1=k+l+n\\x_5=l & x_2=k+m+n\\x_6=m & x_3=l+m+n\\ & x_7=n\end{matrix} \quad \text{dir.}$$

Bu durumda $C=\{(k+l+n,k+m+n,l+m+n,k,l,m,n)\mid k,l,m,n\in \mathrm{F}_2\}$ dir.

Öte yandan, $G=\begin{bmatrix}1&1&0&1&0&0&0\\1&0&1&0&1&0&0\\0&1&1&0&0&1&0\\1&1&1&0&0&0&1\end{bmatrix}$ matrisi C için bir üreteç matrisidir. Bu nedenle C, $[7,4,3]_2$ parametrelerine sahip ikili Hamming koddur.

2.5 Lineer Kodlarda Kodlama

Tanım 2.20 C F_q üzerinde $[n,k,d]$-lineer kod ve $\{a_1,a_2,...,a_k\}$ kodun bazı olsun. Kodun bütün elemanlarını tabandaki elemanların lineer birleşimi şeklinde yazabiliriz, yani her $v\in C$ için $v=u_1a_1+u_2a_2+...u_ka_k$, burada $u_1,u_2,...,u_k\in \mathrm{F}_q^{\,k}$, dır.

Bu ifadeyi üreteç matrisi kullanarakta yazabiliriz. Çünkü üreteç matris, kodu üreten bazın elemanları satır kabul eden matristir.

G üreteç matris, $u=\{u_1,u_2,...,u_k\}$ olmak üzere

$v=uG=u_1a_1+u_2a_2+...u_ka_k$ dır. Böylece $u\in \mathrm{F}_q^{\,k}$ $v=uG$ biçiminde kodlanmış olur [1].

Örnek 2.18 C $[4,2]_2-$ lineer kodun üreteç matrisi $G=\begin{bmatrix}1&1&0&0\\1&0&0&1\end{bmatrix}_{2x4}$

olsun. $u = 11$ mesajını kodlayalım.

$$v = uG = (11)\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix} = (0101)$$

2.6 Devirli Kodlar

Tanım 2.20 $\varnothing \neq S \subseteq \mathrm{F}_q^n$ alt kümesi olmak üzere $(c_1, c_2, ..., c_{n-1}) \in S$ iken $(c_{n-1}, c_1, c_2, ..., c_{n-2}) \in S$ oluyorsa S'ye devirlidir denir. C lineer kodu devirli bir küme ise C'ye devirli kod denir [1].

Örnek 2.19 i) $\{0\}, \{\lambda \cdot 1 : \lambda \in \mathrm{F}_q\}, \mathrm{F}_q^n$ trivial kodları devirlidir.

ii) ikili $[3, 2, 2]$- lineer kodu devirlidir: $\{000, 110, 101, 011\}$

Şimdi devirli kodların yapısına karşılık gelen cebirsel bir dönüşüm yapalım. Çünkü kodları cebirsel olarak incelemek daha kullanışlıdır.

Tanım 2.21 $\pi : \mathrm{F}_q^n \to \mathrm{F}_q[x] \big/ (x^n - 1)$ $(a_0, a_1, ..., a_{n-1}) \to a_0 + a_1 x + ... + a_{n-1} x^{n-1}$ dönüşümü bir F_q vektör izomorfizmasıdır. Burda $R_n = \mathrm{F}_q[x] \big/ (x^n - 1)$ 'nın halka olduğunu biliyoruz($n = 1$ olmadıkça cisim değildir.) [1].

Örnek 2.20 $C = \{000, 110, 101, 011\}$ devirli kodu verilsin.

$\pi(C) = \{0, 1 + x, 1 + x^2, x + x^2\} \subset \mathrm{F}_2[x] \big/ (x^3 - 1)$ olur.

Tanım 2.22 R değişmeli bir halka ve sıfırdan farklı bir alt kümesi I olsun.

i. $\forall a, b \in I$ için $a + b, a - b \in I$

ii. $\forall a \in I$ ve $\forall r \in R$ için $ra \in I$

özellikleri sağlanıyorsa I' ya ideal denir [1].

Teorem 2.9 $\varnothing \neq C \subset \mathrm{F}_q^n$ kodunun devirli bir kod olması için gerek ve yeter şart $\pi(C)$ 'nin $R_n = \mathrm{F}_q[x] \big/ (x^n - 1)$ ' de bir ideal olmasıdır [1].

İspat Kabul edelim ki $\pi(C)$ $R_n = {\mathrm{F}_q[x]}\big/{\left(x^n-1\right)}$ ' de bir ideal olsun. O zaman ideal olmanın $ii.$ şartından $\alpha,\beta \in \mathrm{F}_q \subset \mathrm{F}_q[x]/(x^n-1)$ ve $a,b \in C$ için $\alpha\pi(a), \beta\pi(b) \in \pi(C)$ dir. Buradan $\alpha\pi(a)+\beta\pi(b) \in \pi(C)$ olur ve $\pi(C)$'nin lineer izomorfizm olmasından $\pi(\alpha a+\beta b) \in \pi(C)$ dir. Bu da $\alpha a+\beta b \in C$ olması demektir. Dolayısıyla C lineer koddur.

$c=(c_0,c_1,...,c_{n-1}) \in C$ koduna karşılık gelen polinom

$\pi(c)=c_0+c_1x+...+c_{n-1}x^{n-1} \in \pi(C)$ dir. $\pi(C)$ bir ideal olduğundan,

$x\pi(c)=c_0x+c_1x^2+...+c_{n-1}x^n$

$=c_{n-1}+c_0x+c_1x^2+...+c_{n-2}x^{n-1}$ olur. Çünkü $\mathrm{F}_q[x]/(x^n-1)$ de $x^n-1=0$ dır.

Dolayısıyla $x\pi(c) \in \pi(C)$ olduğundan $\left(c_{n-1},c_1,c_2,...,c_{n-2}\right) \in C$ dır yani C devirli bir koddur.

Diğer taraftan, C bir devirli kod olsun. $\pi(C)$ nin ideal olması için gerekli olan $i.$ şart toplamsal olduğundan sağlanır. Herhangi bir $(f_0,f_1,...,f_{n-1}) \in C$ ye karşılık gelen polinom

$f(x)=f_0+f_1x+...+f_{n-1}x^{n-1}=\pi(f_0,f_1,...,f_{n-1}) \in \pi(C)$ için,

C devirli kod olduğundan $xf(x)=f_{n-1}+f_0x+f_1x^2+...+f_{n-2}x^{n-1} \in \pi(C)$ dir. Böylece $x^2f(x)=x(xf(x))$ $\pi(C)$'nin elemanıdır. Tümevarım yapılarak devam edlirse $i \geq 0$ için $x^if(x)$ $\pi(C)$'nin elemanıdır. C bir lineer kod π bir lineer dönüşüm ve F_q da $\pi(C)$ bir lineer uzaydır. Son olarak $g(x) \in \mathrm{F}_q[x]/(x^n-1)$ polinomu için,

$g(x)f(x)=\sum_{i=0}^{n-1} g_i(x^if(x))$ de $\pi(C)$'nin elemanıdır. Buradan da $\pi(C)$ $\mathrm{F}_q[x]/(x^n-1)$ nin bir idealidir.

Örnek 2.21 $C=\{000,\ 110,\ 101,\ 011\}$ kodu için $\pi(C)=\{0,1+x,1+x^2,x+x^2\}$ olur.

$\pi(C)$ $\mathrm{F}_2[x]/(x^3-1)$ ' nin ideali olduğundan C kodu devirlidir.

Önerme 2.10 $\left(\mathrm{F}_q^* = \mathrm{F}_q - \{0\}, \cdot\right)$ devirli bir gruptur [3].

Tanım 2.23 $\mathrm{F}_q = \left\{0, \alpha, \alpha^2, ..., \alpha^{q-1}\right\}$ olarak yazılabiliyorsa $\alpha \in \mathrm{F}_q$ ya ilkel eleman denir. Yani $\mathrm{F}_q^* = \langle \alpha \rangle$ dır [1].

Tanım 2.24 $\alpha \in \mathrm{F}_{q^m}$ için katsayıları F_q 'dan olan ve α yı kök kabul eden $\mathrm{F}_q[x]$ te ki en küçük dereceli monik polinoma minimal polinom denir [1].

Tanım 2.25 $(n, q) = 1$ olmak üzere $\bmod n$ 'göre $q-$ devirsel kalan sınıfı

$C_i = \left\{\left(i \cdot q^j \pmod n\right) \in Z_n : j = 0, 1, ..., n\right\}$ ' dir [1].

Örnek 2.22 $\bmod 15$ 'göre $2-$ devirsel kalan sınıfları $(15, 2) = 1$ olduğundan şu şekilde bulunur:

$C_0 = \left\{0 \cdot 2^j \bmod 15 \;\; j = 0, 1, ..., n\right\} = \{0\}$, $C_1 = \left\{1 \cdot 2^j \bmod 15 \;\; j = 0, 1, ..., n\right\} = \{2, 4, 8, 1\}$

$C_2 = \left\{2 \cdot 2^j \bmod 15 \;\; j = 0, 1, ..., n\right\} = \{2, 4, 8, 1\}$, $C_3 = \left\{3 \cdot 2^j \bmod 15 \;\; j = 0, 1, ..., n\right\} = \{3, 6, 9, 12\}$

$C_5 = \left\{5 \cdot 2^j \bmod 15 \;\; j = 0, 1, ..., n\right\} = \{5, 10\}$, $C_7 = \left\{7 \cdot 2^j \bmod 15 \;\; j = 0, 1, ..., n\right\} = \{7, 14, 13, 11\}$

Burada bazı kalan sınıfları birbirine denk olduğundan yazılmadı, yani $C_1 = C_2 = C_4 = C_8,\; C_3 = C_6 = C_9 = C_{12}$ '*dir*.

Teorem 2.10 $\alpha \in \mathrm{F}_{q^m}$ nin ilkel elemanı olsun. α^i ye karşılık gelen minimal polinom $M^i(x) = \prod_{j \in C_i} (x - \alpha^j)$ dir. Burda ki C_i ler i yi içeren $q-$ devirsel sınıfıdır [1].

Tanım 2.26 $\alpha \in \mathrm{F}_{q^m}$ nin ilkel elemanı olsun. α^i ye karşılık gelen minimal polinomu $M^i(x)$ ile gösterelim. $g(x) = ekok\left\{M^a(x), M^{a+1}(x), ..., M^{a+\delta-2}(x)\right\}$ üreteç polinomuna sahip bir devirli koda $n = q^m - 1$ uzunluğunda δ tasarlanmış minumum uzaklığa sahip $q-$ lu bir ilkel BCH kod denir. Eğer $a = 1$ alınırsa dar anlamda bir BCH kod denir [1].

Tanım 2.27 $g(x) = ekok\left\{M^a(x), M^{a+1}(x), ..., M^{a+\delta-2}(x)\right\}$ tarafıdan üretilen $n = q^m - 1$ uzunluğunda $q-$ lu BCH kodunu ele alalım. Burada, $\alpha \in \mathrm{F}_{q^m}$ nin ilkel eleman ve $M^i(x)$ ler α^i nin minimal polinomlarıdır.

Eğer $m=1$ alınırsa $n=q-1$ uzunluğunda BCH kod elde ederiz. Elde edilen bu koda Reed Solomon kod denir.

O zaman $\alpha \in \mathrm{F}_{q^m}$ ilkel elemanı için α^i nin F_q daki minimal polinomları $x-\alpha^i$ ler olur.

$\delta \le q-1$ için üreteç polinom

$g(x)=ekok\left\{x-\alpha^a, x-\alpha^{a+1}, ..., x-\alpha^{a+\delta-2}\right\}$ olur. Burada minimal polinomlar arasında asal olduğundan

$g(x)=\left(x-\alpha^a\right)\cdot\left(x-\alpha^{a+1}\right)\cdot ...\cdot\left(x-\alpha^{a+\delta-2}\right)$ şeklinde olur [1].

RS kod iyi parametrelere sahip olduğundan kullanışlı bir koddur. Ayrıca RS kodlar MDS kodların en iyi bilinen sınıfıdır.

Bu kodun faklı kodlama ve dekodlama algoritmaları vardır. Biz konumuzla alakalı olan kodlama şemasını Bölüm 5 te vereceğiz.

BÖLÜM 3

ANAHTAR SAKLAMA YÖNTEMLERİ

Kriptoloji anahtara sahip olmayan kişilerin dosyalara erişimini engelleyen sistem olarak tanımlanabilir. Teknolojinin her geçen gün daha da ilerlemesi anahtar güvenliğinin önemini arttırmaktadır. Sistemi çok iyi ve güvenli bir biçimde kurabilirsiniz fakat anahtarı iyi saklayamadığınızda ya da çaldırdığınızda veya kaybettiğinizde sistem çözülecektir. Bu nedenle akla gelen anahtarın çoğaltılması ve iyi bir şekilde saklanmasıdır.

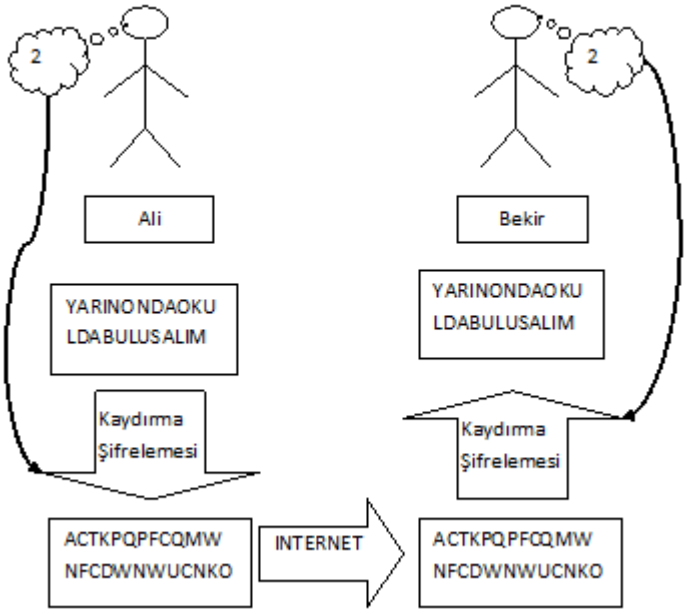
Anahtar saklama ile ilgili ilk olarak akla gelen yöntem anahtarın aynen kopyalanması olmuştur, çünkü anahtarın sadece bir kişide ya da bir yerde olması tehlike oluşturmaktadır. Bu nedenle anahtarlar kopyalanmış ve safe box adı verilen depolarda saklanmıştır [4]. Fakat bu depolar saldırılara karşı çok zayıf kaldığından anahtarın güvenli bir biçimde saklanması problemi ortaya çıkmıştır. Anahtarın güvenli saklanmasının önemli olduğu kadar, sistemin kullanışlı ve ucuz olması da önemlidir. Biz de bu bölümde öncelikle kriptolojide ki anahtar kavramından bahsedip, anahtar saklama yöntemlerini anlatacağız.

3.1 Kriptoloji'de Anahtar Kavramı

Basitçe matematiksel yöntemler kullanılarak verinin anlaşılmaz hale gelmesi ve ancak doğru kişiler tarafından açılması olarak tanımlanabilir. Amaç mesaj gizliliğidir ve rakibin eline geçse bile (zorla ele geçirmesi, mesajın bir kopyasına ulaşması ya da mesajın gönderildiği kanalın dinlenilmesi) rakip tarafından kolayca anlaşılmayacak veya çözülemeyecek bir şekle dönüştürülmesi işlemidir.

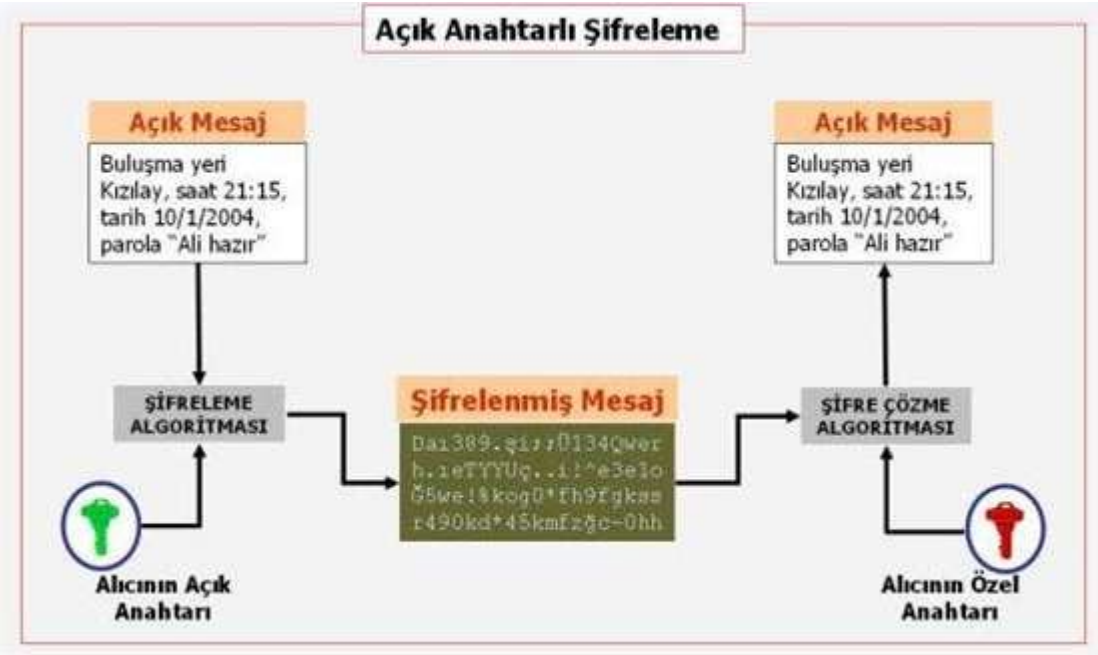
Kullanılan iki türlü şifreleme vardır. Bunlar Simetrik Şifreleme ve Asimetrik Şifreleme'dir.(public key cryptography) Bu iki şifreleme siteminde farklı anahtar yönetim şeması vardır.

Simetrik şifreleme de şifreleme işlemini yapan kişiyle, şifreli metni çözecek olan kişide ki anahtar aynıdır. Yani bu sistemde tek anahtar vardır. Aşağıdaki şekilde bu şifrele sistemi gösterilmektedir, bu örnekte şifrelemeyi yapan ve çözen anahtar 2'dir.



Şekil 3.1 Simetrik Şifreleme [5]

Asimetrik şifreleme de şifreleme işlemini yapan anahtar ile şifreli metni çözen anahtar birbirinden farklıdır. Yani bu sistemde iki farklı anahtar vardır. Şifrele işlemini yapan anahtar açık anahtar olarak adlandırılır ve herkes tarafından bilinmektedir, şifreyi çözen anahtar ise özel anahtar olarak adlandırılır ve sadece şifreyi çözebilecek kişide vardır. Aşağıdaki şekilde bu şifrele sistemi gösterilmektedir:



Şekil 3.2 Asimetrik Şifreleme [6]

Kripto sistemlerinin kalbi anahtarlardır, daha teknik bir ifade ile "bir kripto sisteminin güvenliği anahtarların gizliliğine dayanmalıdır". Bu ilke 19. Yüzyılda yaşamış Fransız dilbilimci Auguste Kerckhoff tarafından ortaya atılmıştır [7]. Sisteminiz, şifreleme algoritmanız ve yaptığınız her türlü matematiksel işlem ve fonksiyonlar bir şekilde düşmanın eline geçebilir. Bu durumda dahi sisteminiz güvenli olmalı. Güvenliğinizi algoritmanın ya da haberleşme protokolünün gizli olmasına, açık metinlerin tahmin edilemez ve karmaşık olmasına dayandırırsanız ciddi bir risk altındasınız demektir.

Algoritmanız öyle tasarlanmış olmalı ki, biri nasıl çalıştığını bilse bile anahtarı bulmadan ondan yararlanamamalı. Hatta saldırganın elinde "bol miktarda" algoritma girdisi ve çıktısı bulunsa dahi anahtar hakkında bilgi edinememeli. Bu nedenle sistemi kurarken, sistemin güvenliğinin anahtarın güvenliğine indirgendiğini bilerek anahtarı iyi bir biçimde saklamalısınız.

Aşağıda anahtar saklama yöntemlerinden bahsedilmektedir.

3.2 Anahtarın Kopyalanması

Akla gelen ilk yöntem anahtarın koyalanmasıdır ve en basit yöntemdir. Bu sitemde anahtar aynen kopyalanır. Yani s anahtar ve v_i ler birer parça olmak üzere $v_1 = v_2 = v_3 = ... = v_n = s$. Dolayısıyla her bir parça bir anahtardır [4].

Bu yöntemde $n-1$ parça kaybolsa veya zarar görse bile sistem çalışmaya devam edecektir. Fakat anahtarların kopyalanması hem çok masraflı hem de güvenli değildir. Çünkü anahtarların bulunduğu yer ele geçirilirse sistem çok kolay bir şekilde çözülecektir. Güvenlik zafiyeti çok olduğundan bu yöntem çok tercih edilmemektedir.

3.3 Anahtarın Parçalanması

Bu yöntem önceki yöntemin geliştirilmesidir fakat yeterli değil aynı zamanda risklidir. Çünkü bu yöntemde s anahtar ve v_i ler birer parça olmak üzere $v_1 + v_2 + v_3 ... + v_n = s$ şeklinde parçalandığından herhangi bir parçanın kaybolması, bozulması veya çalınması durumunda anahtar tekrar oluşturulamaz [4]. Dolayısıyla anahtarın inşası için bütün parçalara ihtiyaç vardır. Bu toplantının yapılabilmesi için bütün üyelerin eksiksiz olması anlamına gelmektedir. Bu nedenle çok kullanışlı değildir. Ama anahtar saklama problemi bir adım daha ileriye götürüldüğünden önemlidir.

3.4 Sır Paylaşım Sistemi

Bu yöntem Shamir ve Blakley tarafından birbirinden bağımsız olarak bulunmuştur [8,9]. Sistemin yaklaşımı anahtarın parçalanması ve bu parçaların kullanıcılara dağıtılması fakat tekrar inşasında bütün kullanıcılara ihtiyaç olmadan belirli kullanıcıların anahtarı oluşturabilmesidir. Bu yöntemin temel özellikleri şunlardır:

Anahtar n parçaya bölünsün ve bu parçalar $v_1, v_2, v_3, ..., v_n$ olsun,

$i)$ Parçalardan herhangi k tanesi anahtarı tekrar oluşturabilir.

$ii)$ $k-1$ parça anahtar hakkında bir bilgiye sahip değildir.

$iii)$ Herhangi bir parça anahtardan uzun olamaz [4].

n parçadan k tanesi anahtarı tekrar oluşturabildiğinden (k,n) eşik değer olarak adlandıracağımız sistem, güvenliği tek bir yerde toplanmayıp risk azaltılmakta ve bozulmalara karşı da sistem garanti altına alınmaya çalışılmaktadır. Geliştirilen saklama yöntemleri arasında en iyisi bu sistemdir ve biz de bu sistem üzerine geliştirilen çeşitli yöntemleri daha sonraki bölümlerde açıklayacağız.

Son olarak $ii)$ şartını sağlayan sistem mükemmel sistem olarak adlandırılırken, $iii)$ şartındaki eşitlik durumunuda sistem ideal olarak adlandırılmaktadır [10,11].

BÖLÜM 4

SHAMİR'İN İNTERPOLASYON YÖNTEMİ

Bu bölümde eşik değer ve interpolasyon yöntemi tanıtılmış, bunlar üzerine inşa edilen sır paylaşım sistemi gösterilmiştir. Bölüm sonunda örneklere yer verilmiştir.

4.1 Genel Bilgiler

(k,n) eşik değer yöntemi Shamir ve Blakley tarafından birbirinden bağımsız olarak 1979 yılında geliştirilmiştir.[8,9]

Yöntemlerin hepsinde ortak olarak sitemi kuran bir dağıtıcı D, anahtar kümesi K ve parçalar kümesi $P=\{P_1,P_2,P_3,...,P_n\}$ vardır. D tarafından $s\in K$ oluşturularak $P=\{P_1,P_2,P_3,...,P_n,\}$ parçalar kümesindeki elemanlara $i.$ parça P_i.kullanıcıya olacak şekilde dağıtılır. Parçalar gizli bir şekilde dağıtılır, hiçbir kullanıcı bilgisini diğer kullanıcılarla paylaşmaz [10]. $B\subset P$ alt kümesinin tekrar anahtarı oluşturabilmesi için k bir pozitif tamsayı olmak üzere $|B|\geq k$ olmalıdır. Eğer $|B|<k$ ise $s\in K$ tekrar oluşturulamaz. Aşağıda yukarıda anlatılanlar tanımlanacaktır.

Tanım 4.1 K (anahtar kümesi) sonlu bir küme ve $s\in K$ bir anahtar ve $C=\{c_1,c_2,c_3,...,c_n\}$ kümesi P parçalar kümesinin elemanlarından oluşmak üzere (k,n) eşik değer yöntemi;

$T1)$ Herhangi k eleman anahtar $s\in K$ yı tekrar oluşturabilir.

$T2)$ Herhangi $k-1$ eleman anahtar $s\in K$ hakkında hiçbir bilgiye sahip değildir [4].

Burada $T2)$ koşulu sistemin mükemmel olması olarak adlandırılır. Dolayısıyla her sistem mükemmel olmayabilir.

Shamir bu sistemi Lagrange interpolasyon formülü kullanarak çözmüştür, kurduğu bu sistem hem mükemmel hemde idealdir [10].

4.2 Sistemin Çalışma Şeması

$q > n$ ve $q = p^s, p$ asal sayı ve $K = S = \mathrm{F}_q$ olsun. Kabul edelim ki

$s \in K$ anahtarın bilgileri $P_1, P_2, P_3, ..., P_n$ parçalarına dağıtılmış olsun. Dağıtıcı gizli biçimde rastgele ve bağımsız olarak, $k-1$ adet $a_1, a_2, ..., a_{k-1}$ elemanlarını F_q cisminden seçer, burda $a_{k-1} \neq 0$ dır. Seçilen katsayılara karşılık gelen polinom

$f(x) = a_0 + a_1 x + a_2 x^2 + ... + a_{k-1} x^{k-1}$ dır.

Bu polinomdaki sabit değer olan $a_0 = s$ dır. Daha sonra D farklı $x_i \in \mathrm{F}_q$ için $y_i = f(x_i)$ değerini hesaplar ve $c_i = (x_i, y_i)$, $i = 1, 2, ..., n$ olacak şekilde dağıtır yani $C = \{c_i \,|\, i = 1, 2, ..., n\}$ [8].

Şunu söyleyebiliriz ki $x_i \in \mathrm{F}_q$ değerlerinin saklanmasına ihtiyaç yoktur ve herkes tarafından bilinebilir, sadece y_i değerinin gizli bir biçimde dağıtılması gerekir [10].

Teorem 3.1 Yukarıda tanımlanan sistem mükemmel bir (k, n) eşik değer yöntemdir [10].

İspat

Kabul edelim ki (x_{i_j}, y_{i_j}), $j = 1, 2, ..., k$ olacak şekilde k tane parça biliniyor olsun. $f(x)$ polinomu lagrange interpolasyon formülünden

$$f(x) = \sum_{j=1}^{k} y_{i_j} \prod_{l \neq j} \frac{x - x_{i_l}}{x_{i_j} - x_{i_l}}$$

elde edilebilir. Daha sonra $K = a_0 = f(0)$ yani $T1)$ elde edilir.

Şimdi kabul edelim ki (x_{i_j}, y_{i_j}), $j = 1,2,...,l$ olacak şekilde $l < k$ tane parça biliniyor olsun. Her $a \in \mathrm{F}_q$ için tam q^{k-l-1} tane $y_{i_j} = f(x_{i_j}), j = 1,2,...,l, f(0) = a$ sağlayan $f(x)$ polinomu vardır. Bu nedenle tüm ihtimaller a için benzer görünür ve $l < k$ tane kullaınıcı kendi bilgileriyle sistemi tekrar oluşturamazlar. Böylece $T2)$ koşulu sağlanır yani sistem mükemmeldir.

Örnek 4.1 P_1, P_2, P_3, P_4 olmak üzere 4 tane kullanıcı olsun ve anahatar 7 seçilsin. Şimdi $a_0 = 7$ olacak şekilde bir polinoma ihtiyaç var, rastgele değerlerle bir polinomu seçilebilir. Polinom $x^2 + 2x + 7$ seçilsin ve kullanıcılara parçalar dağıtılsın.

$P_1 = (1,10)$, $P_2 = (2,15)$, $P_3 = (3,22)$, $P_4 = (4,31)$ olsun.

2.dereceden bir polinom seçildiğinden herhangi 3 kullanıcı tekrar anahtarı oluşturabilir. Biz birkaç faklı durumu inceleyelim.

P_1, P_3, P_4 kullanıcılarıyla sistemi tekrar oluşturalım ve anahtarı bulalım:

İnterpolsayon formülü uygulandığında

$10\frac{(x-3)(x-4)}{(1-3)(1-4)} + 22\frac{(x-1)(x-4)}{(3-1)(3-4)} + 31\frac{(x-1)(x-3)}{(4-1)(4-3)}$ elde edilir ve bu da aradığımız $x^2 + 2x + 7$ polinomudur. $a_0 = 7$ olduğundan anahtar tekrar oluşturulabilir.

P_1, P_2, P_4 kullanıcılarıyla sistemi tekrar oluşturalım ve anahtarı bulalım:

İnterpolsayon formülü uygulandığında

$10\frac{(x-2)(x-4)}{(1-2)(1-4)} + 15\frac{(x-1)(x-4)}{(2-1)(2-4)} + 31\frac{(x-1)(x-2)}{(4-1)(4-2)}$ elde edilir ve bu da aradığımız $x^2 + 2x + 7$ polinomudur. $a_0 = 7$ olduğundan anahtar tekrar oluşturulabilir.

Son olarak 3 ten daha az kullanıcıyla tekrar oluşturulamayacağını görelim.

P_2, P_3 kullanıcılarını şeçelim ve tekrar anahtarı oluşturmayı deneyelim.

interpolsayon formülü uygulandığında

$15\frac{(x-3)}{(2-3)} + 22\frac{(x-2)}{(3-2)} = 7x + 1$ elde edilir ve bu polinomla anahtar tekrar oluşturulamaz.

Örnek 4.2 Yukarıdaki örneği F_{11} cismi üzerinde düşünelim. Polinomumuz x^2+2x+7 $\mathrm{F}_{11}[x]$ olur. Dolayısıyla anahtar $a_0=7$ ve dağıtılacak parçalar $P_1=(1,10)$, $P_2=(2,4)$, $P_3=(3,0)$, $P_4=(4,9)$ olur. 2. dereceden bir polinom seçildiğinden herhangi 3 kullanıcı tekrar anahtarı oluşturabilir. Biz birkaç faklı durumu inceleyelim.

P_1, P_3, P_4 kullanıcılarıyla sistemi tekrar oluşturalım ve anahtarı bulalım:

İnterpolsayon formülü uygulandığında

$10\dfrac{(x-3)(x-4)}{(1-3)(1-4)}+0\dfrac{(x-1)(x-4)}{(3-1)(3-4)}+9\dfrac{(x-1)(x-3)}{(4-1)(4-3)} \bmod 11$ elde edilir ve bu da aradığımız x^2+2x+7 polinomudur. $a_0=7$ olduğundan anahtar tekrar oluşturulabilir.

Farklı parçalar için örnek tekrar kullanılabilir ve sonuç yine aynı sonuç çıkacaktır.

BÖLÜM 5

REED SOLOMON KOD VE SIR PAYLAŞIM SİSTEMİ

Bu yöntem McEliece ve Sarwete tarafından geliştirilmiş bir yöntem olup Bölüm 4' de anlatılan Shamir'in Sır Paylaşım sisteminin genelleştirilmesidir [12]. Diğer sisteme ek olarak, anahtar genel bir hale getirilip yanlış veya sahte kullanıcı kavramı incelenmiştir.

5.1 Reed Solomon Kodlarda Kodlama

Bölüm 2 de devirli kodlar kısmında RS kodlardan genel olarak bahsedilmişti, şimdi ise bu kodların kodlama şemasını ve genel özellikleri verilip, sistem kurulacaktır.

Tanım 5.1 p asal sayı ve $k \le n \le p$ olsun. $a_1, a_2, ..., a_n$ F_p de farklı elemanlar olsun. Her $f(x) \in \mathrm{F}_p[x]$ polinomu için

$u(f) = \left(f(a_1), f(a_2), ..., f(a_n)\right)$ şeklinde tanımlansın.

RS kodun kodsözleri

$\left\{u(f) : f \in \mathrm{F}_p[x], \deg f \le k-1\right\}$ biçiminde olur [13].

Tanım 5.2 $[n,k]_q$ parametreli RS kodun q^k elemanlı olduğunu biliyoruz. Dolayısıyla q^k tane bilgi mesajı vardır. $\left(b_0, b_1, ..., b_{k-1}\right) \in \mathrm{F}_q^k$ bilgi mesajına karşılık gelen polinom

$f(x) = b_0 + b_1 x + ... + b_{k-1} x^{k-1}$ olmak üzere

kodlanmış mesaj $u(f) = \left(f(a_1), f(a_2), ..., f(a_n)\right) \in \mathrm{F}_q^n$ şeklinde bulunur [13].

Örnek 5.1 $q=5, k=2, n=4$ ve $a_1=0, a_2=1, a_3=2, a_4=3$ olsun. $(4,2)\in \mathrm{F}_5^2$ sözünü kodlayalım.

$f(x)=4+2x$ olduğundan $f(0)=4, f(1)=1, f(2)=3, f(3)=0$ olur.

Kodsöz $(4,1,3,0)$ olarak bulunur.

RS kodların kodlama şeması polinomlarla olduğundan rahat bir biçimde lagrange interpolasyon formülünden

$$f(x)=\sum_{j=1}^{k} y_{i_j} \prod_{l\neq j} \frac{x-x_{i_l}}{x_{i_j}-x_{i_l}},$$

anahtar elde edilebilir. Bu yüzden Shamir'in sistemiyle denk bir yöntemdir [12].

5.2 Sistemin Çalışma Şeması

$(\alpha_1, \alpha_2, ..., \alpha_{q-1})$ F_q'da sıfırdan farklı elemanlar olsun. RS kodun kodlama algoritması, bilgi mesajı $a=(a_0, a_1, ..., a_{k-1})\in \mathrm{F}_q^k$, $a_i \in \mathrm{F}_q$, için kodsöz $D_i=\sum_{j=0}^{k-1} a_j \alpha_i^j$ şeklinde olmak üzere $D=(D_1, D_2, ..., D_{q-1})$ olsun. Parçaların D_i 'ler olduğu bu sistemde anahtar $s=a_0=-\sum_{i=1}^{q-1} D_i$ olarak bulunur [4].

Bu yöntemin işlemesindeki en temel nokta RS kodların aynı zamanda bütün MDS kodların da bir özelliği olan herhangi k bileşenin yani üreteç matriste ki k sütunun lineer bağımsız olmasıdır. Dolayısıyla her kodsözün k bileşeni birbirinden farklıdır. Bu da her kodsözü k bileşene kısıtlayıp oradan tanıyabileceğimizi bize söylüyor. Böylece bize verilen k parçayla sistemi tekrar oluşturabiliriz. $l<k$ parça ile ise sistem tekrar oluşturulamaz. Çünkü $\alpha \in \mathrm{F}_q$ ilk bileşen olacak şekilde l parça ile q^{k-l-1} tane kodsöz bulunur [10].

Teorem 5.1 McEliece ve Sarwete tarafından geliştirilen bu yöntem mükemmel bir $(k,n)-$eşik değer yöntemidir [10].

Shamir ile McEliece ve Sarwete tarafından geliştirilen yöntemler birbirine denktir. Fakat bu yöntemde kodlama teorisine girildiğinden sağladığı avantajlar vardır. Bu yöntem sayesinde sahte veya yanlış kullanıcılar olsa bile sistem tekrar kurulabilmektedir.

Teorem 5.2 $[n,k]_q$ parametreli RS kod için t kullanıcı hatalı olsun. s kullanıcının anahtarı tekrar oluşturabilmesi için $s \geq k+2t$ olmalıdır [12].

İspat RS kodların dekodlama algoritmasında, t hata ve r silinmenin düzeltilmesi için $2t+r \leq d-1 = n-k$ olmalıdır $[12]$. Biz de bilinmeyen $n-s$ kordinatı silinmiş gibi hatalı t kullanıcıyı da t hata olarak düşünebiliriz. Buradan da $(c_1, c_2, ..., c_n)$ kodu, dekodlama algoritmasından eğer $2t+(n-s) \leq n-k,$ yani $s \geq k+2t$ olursa tekrar oluşturulur. $(c_1, c_2, ..., c_n)$ kodu bulunduktan sonra da anahtara kolay bir şekilde ulaşılır.

Görülüyor ki Shamir'in sistemi bu yöntemin özel bir halidir. O sistemde $t=0, \alpha_i = i, p$ asal sayıydı [12].

Örnek 5.2 Öncelikle k bileşenin farklı olmasını örnek üzerinde görüp k kullanıcı bilindiğinde kodun nasıl inşa edilebildiğini küçük bir örnek üzerinde görmüş olalım.

$GF(4) = \{0, 1, \alpha, \beta = \alpha^2\}$,burada $\alpha^2 + \alpha + 1 = 0$, cismi üzerinde $n=3, \delta = 2, a = 2$ ve üreteç polinomu $g(x) = x - \beta$ olan RS kodunun yazalım [9].

000	$1\alpha 0$	$\beta 0 \alpha$	$\beta \alpha 1$
01α	$\alpha\beta 0$	10β	111
$0\alpha\beta$	$\beta 10$	$1\beta\alpha$	$\alpha\alpha\alpha$
$0\beta 1$	$\alpha 01$	$\alpha 1\beta$	$\beta\beta\beta$

$k=2$ olduğundan 2 bileşenin aynı yerde bulunduğu bir kodsöz yoktur.

Örneğin α'nın 1.bileşende ve β 'nın üçüncü bileşende olduğu kodsözleri bulalım.

Bakıldığında sadece $\alpha 1 \beta$ kodsözü vardır.

Dolayısıyla anahtarı bulmak için $s = a_0 = -\sum_{i=1}^{q-1} D_i$ olduğundan, alınan kodsözlerin herhangi 2 bileşeni söylendiğinde anahtar bulunabilir.

Örneğin, $\beta 10$ kodsöz olarak seçilsin. Buradan anahtar $s = a_0 = -\sum_{i=1}^{q-1} D_i$ olduğundan anahtar α olur. ($\alpha^2 + 1 = -\alpha$ olduğundan) Parçalar da sırasıyla $P_1 = \beta, P_2 = 1, P_3 = 0$ olur.

Şimdi iki parça verilsin ve anahtarı oluşturmaya çalışalım.

$P_1 = \beta, P_2 = 1$ verilsin. Yani ilk bileşeni β ikinci bileşeni 1 olan kodsözlere bakıldığında:

Görülüyor ki sadece $\beta 10$ kodsözü var.

Eğer $P_1 = \beta, P_3 = 0$ verilirse yine görülüyor ki sadece $\beta 10$ kodsözü vardır. Kodsöz bulunduktan sonra ise anahtar $s = a_0 = -\sum_{i=1}^{q-1} D_i$ den kolayca bulunur.

Örnek 5.3 Şimdi hatalı kullanıcı verilmesi durumuyla alakalı bir örnek yapalım.

Örnek 4.1 de verilen kodu alalım. Yani $q = 5,\ k = 2,\ n = 4$ ve $a_1 = 0, a_2 = 1,\ a_3 = 2,\ a_4 = 3$ olsun. $(4,2) \in \mathrm{F}_5^2$ sözü kodlansın.

$f(x) = 4 + 2x$ olduğundan $f(0) = 4,\ f(1) = 1,\ f(2) = 3,\ f(3) = 0$ olur.

Kodsöz $(4,1,3,0)$ olarak bulunur. Dolayısıyla anahtar $s = 2$ olur.

Kabul edelim ki kodsöz $(4,0,3,0)$ biçiminde hatalı olarak alınsın. Dolayısıyla dağıtıcı hatalı parçalar gönderecektir. $P_1 = (0,4),\ P_2 = (1,0),\ P_3 = (2,3),\ P_4 = (3,0)$

Kodun minimum ağırlığı $n - k + 1 = 3$ olduğundan 1 hata düzeltilebilir.

Şimdi durumlar aşağıda ki gibi incelenirse:

Durum 1) $P_1 = (0,4), P_3 = (2,3)$ kullanıcıları verilirse lagrange interpolasyon formülünden

$f(x) = 4\frac{(x-2)}{(0-2)} + 3\frac{(x-0)}{(2-0)} \bmod 5 = 2x + 4$ olduğudan kodsöz tekrar bulunur. Daha sonra kolay bir biçimde anahtar bulunabilir.

Durum 2) $P_1 = (0,4), P_2 = (1,0)$ kullanıcıları verilirse Lagrange İnterpolasyon formülünden

$f(x) = 4\frac{(x-1)}{(0-1)} + 0\frac{(x-0)}{(1-0)} \bmod 5 = x + 4$ olduğundan kodsöz $(4,0,1,2)$ olur.

Durum 3) Geriye kalan bütün durumları da benzer şekilde bulunabileceğinden, bütün durumlar aşağıda verilmiştir:

Alınan Kullanıcılar	Elde Edilen Polinom	Bulunan Kodsöz
$(1,0),(2,3)$	$f(x) = 2 + 3x$	$(2,0,3,1)$
$(0,4),(3,0)$	$f(x) = 4 + 2x$	$(4,1,3,0)$
$(1,0),(3,0)$	$f(x) = 0$	$(0,0,0,0)$
$(2,3),(3,0)$	$f(x) = 4 + 2x$	$(4,1,3,0)$

Elde edilen kodsözlere bakıldığında $(4,0,3,0)$ kodsözüne uzaklığı en yakın kodsöz $(4,1,3,0)$'tür. En yakına dekodlama gereği kodsöz $(4,1,3,0)$ olacaktır. Kodsöz tekrar doğru olarak bulunduğundan anahtar inşa edilebilecektir.

BÖLÜM 6

ÇİN KALAN TEOREMİNİ KULLANARAK SIR PAYLAŞIM SİSTEMİ

Bu bölümde Asmuth ve Bloom tarafından geliştirilen, Çin Kalan Teorimini kullanarak inşa edilen ve mükemmel olmayan Sır Paylaşım sisteminden bahsedeceğiz [14]. Bu şemalarda Çin Kalan Teoremi boyunca özel bir sırada tam sayı dizileri kullanılır.

6.1 Çin Kalan Teoremi

Tanım 6.1 Bir m pozitif tamsayısı verilmiş olsun. $a,b \in \mathbf{Z}$ için $m \mid (a-b)$ ise a ve b m modülüne göre denktirler denir ve $a \equiv b (\mathrm{mod}\, m)$ yazılır. Böylece ortaya çıkan bağıntıya m modülüne göre kongrüans bağıntısı denir. Kongrüans bağıntısı bir denklik bağıntısıdır.

Teorem 6.1 $m_1, m_2, ..., m_r$ pozitif tamsayılar ve her $i \neq j$ için $ebob(m_i, m_j) = 1$ olsun. $a_1, a_2, ..., a_r$ tamsayıları verildiğinde

$$x \equiv a_1 \bmod m_i$$
$$x \equiv a_2 \bmod m_2$$

...

$$x \equiv a_r \bmod m_r$$

kongrüans sisteminin $\mathbf{Z}$ de bir x çözümü vardır ve bu çözüm M modunda tektir. Kongrüans kümelerinin çözümü ise şu şekilde hesaplanır:

$M = m_1 \cdot m_2 \cdot ... \cdot m_r$ modülüne göre

$$x \equiv a_1 b_1 \frac{M}{m_1} + \ldots + a_r b_r \frac{M}{m_r} (\mathrm{mod}\, M)$$

ve

$b_i \frac{M}{m_i} \equiv 1 (\mathrm{mod}\, m_i)$' dir [15].

6.2 Sistemin Çalışma Şeması

1) Parçaların Dağıtılması

$m_1, m_2, \ldots, m_r$ pozitif tamsayılar ve her $i \neq j$ için $ebob(m_i, m_j) = 1$ olsun. $m_0 > K$ bir asal sayı olmak şartı ile $m_0 < m_1 < m_2 \ldots\ldots < m_n$ olarak seçilsin. Bunun sonucunda aşağıdaki eşitsizlik sağlanmaktadır:

$\prod_{i=1}^{t} m_i > m_0 \prod_{i=1}^{t-1} m_{n-i+1}$.(Bu çarpımın sağlanması dizinin özel seçilmesine bağlıdır)

M , $\prod_{i=1}^{t} m_i$ 'yi göstersin. Daha sonra dağıtıcı $0 \leq y < M$ koşulunu sağlayan a sayısı için $y = K + am_0$ değerini hesaplar.

$i.$ kullanıcının paylaşımları $1 \leq i \leq n$ aralığında $y_i \equiv y \bmod m_i$ denklemindeki değerdir.

2) Anahtarın Tekrar Oluşturulması

Kullanıcıların anahtarı tekrar oluşturmak için bir araya geldiği kümeyi S ile gösterelim. Yani $S = \{y_1, y_2, .., y_t\}$ dir. M_S ile $\prod_{i \in S} m_i$ gösterelim.

Çin kalan teoremini kullanarak y yi aşağıdaki denklem sistemini çözerek elde edebiliriz:

$y \equiv y_i (\mathrm{mod}\, m_i)$

Anahtarı ise

$K \equiv y (\mathrm{mod}\, m_0)$ ile bulunur. Çin kalan teoremine göre de çözüm $\mathbf{Z}_{M_s}$ ve $y < M \leq M_s$ olduğundan $\mathbf{Z}_M$ ye göre tektir [14].

Not 6.1 Asmuth-Bloom gizlilik paylaşım şeması mükemmel olmayan bir sistemdir yani $k-1$ parça hiçbir bilgiye sahip değildir denilemez ve her kullanıcı gizliliğe ulaşabilecek eşit güce sahip değildir [15].

Örneğe geçmeden önce tekrar yöntemi kısaca maddeler halinde özetlemek istiyoruz.

Öncelikle bilinmelidir ki eşik şema için özel tamsayılar seçilmektedir ve bu sayılar birbirlerine göre ikişerli olarak asaldır. Paylaşımlar K anahtar değeriyle ilişkili sayılardır. Şimdi maddeler halinde yazarsak;

1) m_0 asal sayısı $m_0 > K$ ve $m_1, m_2, ..m_n$ sayıları $m_0 < m_1 < m_2 < ... < m_n$ olacak şekilde seçilir.

2) $ebob(m_0, m_i) = 1, \forall i$ ve $i \neq j$ için $ebob(m_i, m_j) = 1$.

3) $m_0 m_{n-t+2} ... m_n < m_1 ... m_t$ olmalıdır.

Örnek 6.1 $2 \leq t \leq n$ şartını sağlayan $(t, n) = (3, 4)$ gizlilik paylaşım şemasını kuralım.

Öncelikle $K = 4$ olarak şeçilir.

$m_0 < m_1 < m_2 < m_3 < m_4$ sayılarınıda

$5 < 17 < 18 < 19 < 23$ olarak özel bir sırada şeçilir.

$M = m_1.m_2.m_3 = 17.18.19 = 5814$ sayısı alınır ve $\left[0, (M/m_0) - 1\right]$ oranında rastgele bir a sayısı seçilir. Biz $a = 7$ alalım.

$K' = K + am_0$ formulü ile yeni anahtar elde edilir.

$K' = 4 + 7.5 = 39$

4 kişi arasında paylaşım şu şekilde yapılır:

$K_1 = K' \bmod m_1 = 39 \bmod 17 = 5$
$K_2 = K' \bmod m_2 = 39 \bmod 18 = 3$
$K_3 = K' \bmod m_3 = 39 \bmod 19 = 1$
$K_4 = K' \bmod m_4 = 39 \bmod 23 = 16$

$P_1 = (K_1, m_1) = (5,17)$
$P_2 = (K_2, m_2) = (3,18)$
$P_3 = (K_3, m_3) = (1,19)$
$P_4 = (K_4, m_4) = (16,23)$

Kullanıcılar P_1, P_2, P_3, P_4 ' dır.

Dağıtım işlemi gerçekleşti. Şimdi de anahtarı herhangi 3 kullanıcıyla tekrar oluşturalım.

P_1, P_2, P_3 kullanıcıları anahtarı elde etmek istesinler.

$x \equiv 5 \bmod 17$
$x \equiv 3 \bmod 18$
$x \equiv 1 \bmod 19$

Şimdi ise Çin Kalan teoremi uygulanarak $K^{'}$ elde edilecektir.

$b_i \dfrac{M}{m_i} \equiv 1 (\bmod m_i)$ olduğundan

$b_1 . 5814/17 \equiv 1 \bmod 17 \Rightarrow b_1 = 9$
$b_2 . 5814/18 \equiv 1 \bmod 17 \Rightarrow b_2 = 17$
$b_3 . 5814/19 \equiv 1 \bmod 19 \Rightarrow b_3 = 10$

olarak hesaplanır. Çözüm ise $x \equiv a_1 b_1 \dfrac{M}{m_1} + \ldots + a_r b_r \dfrac{M}{m_r} (\bmod M)$ formülüyle

bulunur.(Çin Kalan Teoreminden)

$K^{'} = 5.9.5814/17 + 3.17.5814/18 + 1.10.5814/19 \bmod 5814 = 39$

$K^{'} = K + am_0$ eşitliğinden

$K = K^{'} - am_0 = 39 - 7.5 = 4$ olarak anahtar bulunur.

BÖLÜM 7

LİNEER KODLAR VE SIR PAYLAŞIM SİSTEMİ

Bu bölümde lineer kodlar kullanılarak inşa edilen sır paylaşım sistemi anlatılacak. Massey tarafından geliştirilen bu yöntemde, minimal kodsöz ile minimal erişim kümeleri arasındaki birebir eşleme yakalanmış ve bu sayede anahtar daha kolay bir şekilde tekrar oluşturulmuştur. Bu yöntem kullanılarak yüksek boyutlarda ve özel sınıftaki kodlar için sistem uygulanabilir hale getirilmiştir [16,17].

7.1 Sır Paylaşım Sisteminde Minimal Erişim Kümeler Kavramı

Daha önceki bölümlerde kullanıcılar kümesi $P=\{P_1,P_2,P_3,...,P_n\}$ den bahsedilmişti. Anahtarın tekrar oluşturulması bu kümeden alınan belirli elemanlarla olmaktaydı. Bu bölümde ise bu ifadenin genellemesi yapılarak, P 'nin alt kümelerinden oluşan küme Γ ya , $\Gamma \in 2^P$, erişim yapısı diyeceğiz.

Şunu da söylemeliyiz ki her kullanıcı grubu anahtarı tekrar oluşturamaz yani P 'nin bütün alt kümeleri erişim kümesi değildir. P 'nin bu alt kümelerini de $\overline{\Gamma}=2^P/\Gamma$ ile göstereceğiz.

Tanım 7.1 $B\in\Gamma$ ve $B\subset B'\subset P$ iken $B'\in\Gamma$ oluyorsa Γ'ya monoton erişim yapısı denir [10].

Tanım 7.2 $B\in\Gamma$ erişim kümesi olmak üzere, $B\subset B'\subset P$ iken $B'\in\Gamma$ oluyorsa B'ye minimal küme denir. Γ ' da ki bütün minimal kümeleri $\Gamma_{\min}$ ile gösterilir [10].

Tanım 7.3 $B \in \overline{\Gamma}$ için $B \subset B' \subset P$ iken $B' \in \Gamma$ oluyorsa B'ye maximal küme denir. $\overline{\Gamma}$ ' da ki bütün maximal kümeleri $\overline{\Gamma}_{\max}$ ile gösterilir [10].

7.2 Massey'in Sır Paylaşım Sistemi

Bu alt bölümde Massey 'in sisteminin genel şemasını anlatıp, temel tanımlamalara yer vereceğiz.

C F_q sonlu cisminde tanımlı $[n,k,d]$ lineer kod ve bu kodun üreteç matrisi $G=[g_0,g_1,...,g_{n-1}]$ olsun. Kabul edelim ki G'nin hiçbir sütunu sıfır olmasın. Bu yöntemde de $s \in \mathrm{F}_q$ anahtar, $n-1$ tane kullanıcı ve dağıtıcı bulunmaktadır.

Parçaların belirlenmesi için dağıtıcı kodsözün ilk bileşeni $t_0 = s$ olacak şekilde $t \in C$ kodsözünü seçer. $t=(t_0,t_1,...,t_{n-1})$ kodsözü üreteç matris kullanılarak üretildiği için bir $u=(u_0,u_1,...,u_{k-1}) \in \mathrm{F}_q^k$ bilgi mesajı vardır ki $s = ug_0$ ve $t = uG$ dır. Tabiki $s = ug_0$ özelliğini sağlayan q^{k-1} tane farklı u bilgi mesajı vardır, bu da $t \in C$ kodsözünün tek olmadığını göstermektedir. Son olarak dağıtıcı kodsözü seçtikten sonra ilk bileşeni kendisine saklayıp geriye kalan $\{t_1,t_2,...,t_{n-1}\}$ bileşenlerini kullanıcılara dağıtır [18].

Not 7.1 **i)** G üreteç matrisi kullanıcılar tafanından bilinmektedir.

ii) G'nin herhangi bir sütununun sıfır olması demek o sütuna karşılık gelen kullanıcının her zaman sıfır olması demektir yani bu kullanıcının sisteme hiçbir etkisi olmayacaktır. Bu yüzden herhangi bir sütunun sıfır olmaması gerekmektedir [10].

Anahtarın tekrar oluşturulması için üreteç matrisin sütunlarından yararlanacağız. Yani $g_0, g_{i_1}, ..., g_{i_m}$ sütunları lineer bağımlı olmak üzere anahtarın tekrar inşası için ilk olarak

$$g_0 = \sum_{j=1}^{m} x_j g_{i_j}$$

lineer eşitliğinin çözülmesi gerekmektedir. Buradan bulunan x_j katsayılarını kullanarak anahtar şu şekilde hesaplanır:

$t_0 = ug_0 = \sum_{j=1}^{m} x_j ug_{i_j} = \sum_{j=1}^{m} x_j t_{i_j}$ [18].

Şimdi sistemi kurmadan önce bilinmesi gereken temel tanımları yapılacak ve sistemin kurulması için gerekli olan özellikler verilecektir.

Tanım 7.4 Kodsözün sıfırdan faklı bileşenlerinin yerini gösteren kümeye kodsözün support'u denir. Yani $v \in \mathrm{F}_q^n$ olmak üzere

support $(v) = \{0 \le i \le n-1 : v_i \neq 0\}$ dir [18].

Örnek 7.1 $v = 100255 \in \mathrm{F}_7^6$ kodsözü verilmiş olsun support $(v) = \{1,4,5,6\}$ dır.

Tanım 7.5 v_1 kodsözünün support'u v_2 kodsözünün support'unu içeriyorsa v_1 kodsözü v_2 kodsözünü örtüyor denir [18].

Örnek 7.2 $v_1 = 022501$, $v_2 = 001203 \in \mathrm{F}_7^6$ kodsözleri verilmiş olsun.

support $(v_1) = \{2,3,4,6\}$, support $(v_2) = \{3,4,6\}$ olduğundan v_1 kodsözü v_2'yi örter.

Tanım 7.6 $v \neq 0$ vektörünü örten yalnız kendi katı olan bir vektör ise bu vektöre minimal vektör denir [18].

Örnek 7.3 $v_1 = 100255, v_2 = 200433 \in \mathrm{F}_7^6$ vektörleri verilmiş olsun.

support $(v_1) = \{1,4,5,6\}$, support $(v_2) = \{1,4,5,6\}$ ve $v_2 = 2v_1$ olduğundan v_1 ve v_2 minimal vektördür.

Tanım 7.7 İlk bileşeni 1 olan minimal vektöre minimal kodsöz denir [18].

Örnek 7.4 $v_1 = 100255 \in \mathrm{F}_7^6$ kodsözü verilen özelliklere göre bir minimal kodsözdür.

Neden minimal kodsözlere ihtiyaç olduğu şu şekilde özetlenebilir:

$v=(1,v_1,v_2,...,v_{n-1})\in C^{\perp}$, $\exists v_j\neq 0$, kodsözü için $vt=t_0+v_1t_1+...+v_{n-1}t_{n-1}=0$ dır. ($t\in C$) Bu eşitlikten $t_0=-(v_1t_1+...+v_{n-1}t_{n-1})$ elde edilir. Görülüyor ki anahtarı bulma işlemini $v\in C^{\perp}$ kodsözündeki bileşenlere kısıtlandı. Yani anahtarı elde etmek için hangi kullanıcıların gerektiğini elimizdeki kodsöze göre belirlenebilecek hale geldi. Dahasi eğer elimizde $w=(1,0,0,...,w_{l_1},0,....,w_{l_m},0,...0)\in C^{\perp}$ şeklinde , $\exists w_{l_j}\neq 0$ olmak üzere, kodsöz varsa

$wt=t_0+w_{l_1}t_{l_1}+...+w_{l_m}t_{l_m}=0$ olacak ve anahtar tekrar oluşturulabilecektir.

Bu ifadeler bize minimal erişim kümelerinin, dual koddaki ilk bileşeni 1 olan minimum ağırlıklı kodsözlerle belirlenebileceği, yani minimal kodsözlerle bulunabileceği noktasında yol göstermektedir. Buradan erişim yapılarının minimal kosözlerle tamamen belirlenebileceği sonucu çıkartılabilir.

Şimdi $C^{\perp}$ deki kodsözlerle G üreteç matrisinin lineer bağımlı sütünları arasında birebir eşleme olduğunu gösteren ifaye vereceğiz.

Önerme 7.1 G'nin $g_{i_1},g_{i_2},...,g_{i_m}$ sütunlarının lineer bağımlı olması için gerek ve yeter şart $C^{\perp}$ 'de $c=(0,0,0,...,c_{i_1},0,....,c_{i_m},0,...0)\neq 0$ kodsözünün olmasıdır [18].

İspat $g_{i_{r_s}}$ ile g_{i_r} sütununun $s.$ bileşenini gösterelim. Eğer $g_{i_1},g_{i_2},...,g_{i_m}$ sütunları lineer bağımlıysa $c_{i_1}g_{i_1}+c_{i_2}g_{i_2}+...+c_{i_m}g_{i_m}=0$ olacak şekilde en az bir $c_{i_j}\neq 0$ için eşitlik sağlanır. Açıktır ki $\forall s=0,1,...,m-1$ için $c_{i_1}g_{i_{1s}}+c_{i_2}g_{i_{2s}}+...+c_{i_m}g_{i_m{}^s}=0$ dır.

Herhangi bir $v\in C$ alalım. v G üreteç matrisinin satır vektörlerinin lineer birleşimi olarak yazılabildiğinden, $v=\sum_{j=0}^{m-1}a_j(g_{1j},...,g_{(m-1)j})$ şeklindedir.

$c=(0,0,0,...,c_{i_1},0,....,c_{i_m},0,...0)$ için

$$vc=\sum_{j=0}^{m-1}a_j(g_{1j},...,g_{(m-1)j})(0,0,0,...,c_{i_1},0,....,c_{i_m},0,...0)$$

$$=\sum_{j=0}^{m-1}a_j(c_{i_1}g_{i_{1j}},...,c_{i_m}g_{i_{(m-1)j}})=\sum_{j=0}^{m-1}a_j0=0$$

olduğundan $c \in C^{\perp}$ bulunur.

Tersine $0 \neq c \in C^{\perp}$ ve her $v \in C$ için $vc = 0$ olduğundan yukardaki benzer ifadeleri kullanarak $g_{i_1}, g_{i_2}, ..., g_{i_m}$ sütunları lineer bağımlı olduğu gösterilebilir.

Önerme 7.2 c_1 ve c_2 C kodunda faklı iki minimal kodsöz olsun. c_1 ve c_2 ' nin aynı bileşenleri sıfır olamaz [18].

İspat Aksini kabul edelim. Farklı bileşenleri aynı olmayan iki farklı minimal kodsöz alalım. $c_1 = (1,...,a,...), c_2 = (1,...,b,...)$ kodsözlerini alalım, burada $j.$ bileşenleri a, b olmak üzere $a \neq b$ ve $a \neq 0, b \neq 0$ dır. Bu durumda C kodunda $c_3 = c_2 - a^{-1}bc_1$ olacak biçimde kodsöz vardır. Görülmektedir ki c_1 ve c_2 kodları c_3 kodunu örter ve c_3 kodunun ilk bileşeni sıfırdan farklıdır. Böylece ilk bileşeni 1 olan $c_4 = (1 - a^{-1}b)c_3$ kodu vardır ve bu kod c_1 ve c_2 kodlarının bir katı değildir fakat c_1 ve c_2 c_4 kodunu örtmektedir. Bu da c_1 ve c_2 kodlarının minimal kodsöz olmasıyla çelişmektedir.

Anahtarı yasal olarak oluşturabilecek olan grubun kullanıcılardan oluşan bir küme olduğu açıktır. Bizde kullanıcılardan oluşan öyle bir küme arıyoruz ki kendisi anahtarı oluşturabilsin fakat herhangi bir alt kümesi bu işlemi yapamasın.

Tanım 7.8 $B \in \Gamma$ erişim kümesi anahtarı tekrar oluşturabilirken B kümesinin herhangi bir öz alt kümesi anahtarı oluşturamıyorsa B 'ye minimal erişim kümesi denir [18].

Tanım 7.9 Bütün minimal erişim kümelerinde bulunan kullanıcılara diktatör kullanıcılar denir [18].

Tanım 7.10 Bütün kullanıcılar minimal erişim kümelerinde t defa bulunuyorsa sır paylaşım sisteminin demokratiklik derecesi t ' dir denir.

Minimal kodsöz ve minimal erişim kümeleri arasındaki eşleşmeyi kurmadan önce, bilinen bir önermeyi vermek istiyoruz [18].

Önerme 7.3 Eğer $\left\{P_{i_1}, P_{i_2}, ..., P_{i_m}\right\}$ minimal erişim kümesi ise ona karşılık gelen $g_{i_1}, g_{i_2}, ..., g_{i_m}$ sütunları lineer bağımsızdır [18].

İspat Aksini kabul edelim. Yani $\left\{P_{i_1}, P_{i_2}, ..., P_{i_m}\right\}$ minimal erişim kümesi fakat $g_{i_1}, g_{i_2}, ..., g_{i_m}$ sütunları lineer bağımlı olsun. Bu durumda $\lambda_1 g_{i_1} + \lambda_2 g_{i_2} + ... + \lambda_m g_{i_m} = 0$ olacak şekilde $\exists \lambda_j \neq 0$ vardır.

Kabul edilsin ki $\lambda_1 \neq 0$ olsun, o zaman P_{i_1} kullanıcısı diğer kullanıcıların lineer birleşimi şeklinde yazılabileceğinden $\left\{P_{i_2}, ..., P_{i_m}\right\}$ kullanıcıları anahtarı tekrar oluşturabilecektir. Bu da en başta aldığımız $\left\{P_{i_1}, P_{i_2}, ..., P_{i_m}\right\}$ kümesinin minimal olmasıyla çelişir.

Şimdi minimal kodsözlerle minimal erişim kümeleri arasındaki eşleşmeyi göstereceğiz.

Önerme 7.4 Minimal kodsöz ile minimal erişim kümesi arasında $1-1$ eşleşme vardır öyle ki her minimal kodsöze karşı minimak erişim kümesi karşılık gelir [19].

$\left\{P_{i_1}, P_{i_2}, ..., P_{i_m}\right\}$ minimal erişim kümesine karşılık gelen minimal kodsöz

$c = (1, 0, ..., c_{l_1}, 0, ..., c_{l_m}, 0, ...0) \in C^{\perp}, c_{i_j} \neq 0 \quad j = 1, 2, ..., m$, şeklindedir.

İspat $\left\{P_{i_1}, P_{i_2}, ..., P_{i_m}\right\}$ minimal erişim kümesi olduğundan $g_0, g_{i_1}, g_{i_2}, ..., g_{i_m}$ sütunları lineer bağımlıdır. Önerme 6.1 'e göre $a = (a_0, 0, 0, ..., a_{i_1}, 0, ..., a_{i_m}, 0, ...0) \in C^{\perp}$ vardır.

$c = a_0^{-1} a = (1, 0, 0, ..., c_{i_1}, ..., c_{i_m}, ..., 0)$ olsun. Eğer $j \in \{1, 2, ..., m\}$ için $c_{i_j} = 0$ olsaydı Önerme 6.1 den $\left\{P_{i_1}, ..., P_{i_{j-1}}, P_{i_{j+1}} ..., P_{i_m}\right\}$ kümesi anahtarı tekrar oluşturabileceğinden, minimal olmayla çelişir.

Eğer c minimal kodsöz değilse c'nin örttüğü $\overline{c} \neq 0$ için $c \neq \lambda \overline{c}$ şeklindedir. Önerme 6.3 'den $\overline{c}_0 \neq 0$ dır. $\overline{\overline{c}} = \overline{c} c_0 - \overline{c} \neq 0$ kodsözü için c $\overline{\overline{c}}$'yi örter ve $\overline{\overline{c}} = 0$ dır. Bu yüzden $\overline{\overline{c}} = (0, 0, ..., \overline{\overline{c}}_{i_1}, ..., \overline{\overline{c}}_{i_m}, 0, ..., 0) \in C^{\perp}$ formundadır. Bu ise Önerme 6.1 ve Önerme 6.3 ile

çelişmektedir ve böylece c minimal kodsöz olur. c 'nin tekliğide Önerme 6.2 'den gelmektedir.

İspatın ikinci kısmına gelirsek, eğer $c=(1,0,...,c_{l_1},0,....,c_{l_m},0,...0)$ minimal kodsöz olduğundan Önerme 6.1 'den $g_0,g_{i_1},g_{i_2},...,g_{i_m}$ sütunları lineer bağımlıdır. Bu yüzden $\left\{P_{i_1},P_{i_2},...,P_{i_m}\right\}$ kümesi anahtarı oluşturabilir. Eğer herhangi bir öz alt kümesi $\left\{P_{i_1},...,P_{i_{j-1}},P_{i_{j+1}}...,P_{i_m}\right\}$ gibi anahtarı oluşturabilseydi, buna karşılık gelen başka bir kodsöz olurdu. Dolayısıyla bu kodsöz c tarafından örtülüyor olurdu. Bu da c 'nin minimal olmasıyla çeliştiğinden $\left\{P_{i_1},P_{i_2},...,P_{i_m}\right\}$ kümesi minimal erişim kümesidir.

Minimal kodsözleri bulmak her kod için kolay bir işlem değildir. Bunu ilk bakışta görmek ve büyük örnekler için sistemi kurmak oldukça zordur.

Minimal kodsözlerin bulunmasıyla alakalı birçok çalışma yapılmıştır. Biz bu son kısımda yapılan çalışmalarla alakalı bazı bölümleri anlatıp örneklerle konuyu bitireceğiz.

Önerme 7.5 C bir $\left[n,k,d\right]_q$ kod olsun. Kodun minimum ağırlığını $w_{\min}$ ve maksimum ağırlığını $w_{\max}$ ile gösterelim. Eğer

$\frac{w_{\min}}{w_{\max}}>\frac{q-1}{q}$ ise C deki sıfırdan farklı her kodsöz minimaldir [20,21]**.**

İspat Kabul edelim ki $c_1=(u_0,u_1,...,u_{n-1})$ kodu $c_2=(v_0,v_1,...,v_{n-1})$ kodunu örtsün fakat c_1 c_2 'nin bir katı olmasın. Şu eşitlik vardır:

$w_{\min}\le w(c_1)\le w(c_2)\le w_{\max}$.

Herhangi bir $t\in \mathrm{F}_q^*$ için, $m_t=\left|\left\{i:v_i\neq 0,u_i=tv_i\right\}\right|$ olsun. Tanımdan

$\sum_{t\in \mathrm{F}_q^*} m_t=w(c_2)$ olur. Böylece $m_t\ge w(c_2)/q-1$ olacak şekilde $\exists t\in \mathrm{F}_q^*$ vardır. c_1-tc_2 kodu için,

$$w(c_1 - tc_2) \le w(c_1) - \frac{w(c_2)}{q-1} \le w_{\max} - \frac{w_{\min}}{q-1} < \frac{q}{q-1} w_{\min} - \frac{w_{\min}}{q-1} = w_{\min}$$ dir.

Bu da sıfırdan farklı $c_1 - tc_2$ kodsözü için $w(c_1 - tc_2)$'nin $w_{\min}$ den küçük olması demektir, bu da çelişkidir.

Önerme 7.6 C bir $[n,k,d]_q$ kod ve $G = [g_0, g_1, ..., g_{n-1}]$ üreteç matrisi olsun. Eğer C 'nin sıfırdan farklı her kodsözü minimal vektör ise, sır paylaşım sisteminin temeli $C^{\perp}$ kodudur ve q^{k-1} tane minimal erişim kümesi vardır. Buna ek olarak;

$1.\ 1 \le i \le n-1$ için g_i sütunu g_0'ın bir katıysa, P_i kullanıcısı bütün minimal erişim kümelerinde vardır. Yani P_i kullanıcısı diktatör kullanıcıdır.

$2.\ 1 \le i \le n-1$ için g_i sütunu g_0'ın bir katı değilse, P_i kullanıcısı q^{k-1} tane minimal erişim kümesinden $(q-1)q^{k-2}$ tanesinde olmak zorundadır [22].

Verilen bir C lineer kodu için bütün minimal erişim kümelerini bulmak oldukça ilginç ve zor bir problemdir. Bu problem Covering Problem olarak adlandırılır [23].

Örnek 7.5 Öncelikle küçük bir örnekle başlayalım.

F_2 cismi üzerinde 4 kullanıcının olduğu bir sistem kuralım.

$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$ üreteç matrisi verilsin.

$t = 11010$ olarak şeçelim. Dolayısıyla $s = 1$, kullanıcılarda sırasıyla $P_1 = 1, P_2 = 0, P_3 = 1, P_4 = 0$ olur.

Dağıtım işlemini yaptıktan sonra kontrol matrisini bulup minimal kodsözleri tespit etmeliyiz.

$H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{pmatrix}$ olduğundan $C^{\perp} = \{00000, 01110, 11101, 10011\}$ olur.

Kod elimizde olduğundan minimal kodsözleri daha önceden belirtilen özellikleri kullanarak kolayca tespit edebiliriz. Bunlar $\{11101, 10011\}$ dır.

İlk kodsöz bize P_1, P_2, P_4 kullanıcılarıyla, ikinci kodsöz de P_3, P_4 ile sistemi tekrar oluşturabileceğimizi söylemektedir. Bu da ilk kodsöz için g_0, g_1, g_2, g_4 ve ikinci kodsöz için de g_0, g_3, g_4 lineer bağımlı olduğunu göstermektedir. Ayrıca burada P_4 kulanıcısı her iki kümede de yer aldığından diktatör kullanıcıdır.

Şimdi anahtarı bu bilgilere göre tekrar oluşturalım.

Birinci minimal kodsözü kullanarak inşaya başlayalım:

$g_0 = ag_1 + bg_2 + cg_4$ ve $s = aP_1 + bP_2 + cP_4$ olduğundan öncelikle $a, b, c \in \mathrm{F}_2$ değerlerini bulmalıyız.

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = a\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} + b\begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} + c\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \Rightarrow a = 1, b = 1, c = 1$$

$s = 1.1 + 1.0 + 1.0 = 1$ olarak anahtar tekrar bulunur.

Şimdi diğer minimal kodsözü kullanarak işlemi tekrarlarsak:

$g_0 = ag_3 + bg_4$ ve $s = aP_3 + bP_4$ olduğundan öncelikle $a, b, c \in \mathrm{F}_2$ değerlerini bulmalıyız.

$$\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = a\begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix} + b\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \Rightarrow a = 1, b = 1$$

$s = 1 \cdot 1 + 1 \cdot 0 (\mathrm{mod}\, 2) = 1$ olarak anahtar tekrar bulunur.

Örnek 6.6 F_3 cismi üzerinde 5 kullanıcın olduğu bir sistem kuralım.

$G = \begin{pmatrix} 1 & 0 & 0 & 2 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 2 & 2 & 1 & 2 & 1 \end{pmatrix}$ üreteç matrisi verilsin.

$t = 121200$ olarak şeçelim. Dolayısıyla $s = 1$, kullanıcılarda sırasıyla $P_1 = 2, P_2 = 1, P_3 = 2, P_4 = 0, P_5 = 0$ olur.

Dağıtım işlemini yaptıktan sonra kontrol matrisini bulup minimal kodsözleri tespit etmeliyiz.

$$H=\begin{pmatrix}1&2&2&1&0&0\\2&2&0&0&1&0\\0&2&2&0&0&1\end{pmatrix}$$

olduğundan

$$C^{\perp}=\left\{\begin{array}{l}000000,122100,220010,022001,211200,110020,011002,012110,111101,212011,\\001111,002222,101210,200201,102021,201012,202120,100102,120211,020112,\\222121,0212201,222202,121022,010221,210122,112212\end{array}\right\}$$

olur.

Kod elimizde olduğundan minimal kodsözleri daha önceden belirtilen özellikleri kullanarak kolayca tespit edebiliriz. Bunlar $\{111101,101210,120211,121022\}$ dır.

İlk kodsöz bize P_1,P_2,P_3,P_5, ikinci kodsöz P_2,P_3,P_4, üçüncü kodsöz P_1,P_3,P_4,P_5 ve dördüncü kodsöz ise P_1,P_2,P_4,P_5 kullanıcılarıyla sistemi tekrar oluşturabileceğimizi söylemektedir.

Şimdi anahtarı bu bilgilere göre tekrar oluşturalım.

Birinci minimal kodsözü kullanarak inşaya başlayalım:

$g_0=ag_1+bg_2+cg_3+dg_5$ ve $s=aP_1+bP_2+cP_3+dP_5$ olduğundan; öncelikle $a,b,c,d\in \mathrm{F}_3$ değerlerini bulmalıyız.

$$\begin{pmatrix}1\\0\\0\end{pmatrix}=a\begin{pmatrix}0\\1\\2\end{pmatrix}+b\begin{pmatrix}0\\0\\2\end{pmatrix}+c\begin{pmatrix}2\\1\\1\end{pmatrix}+d\begin{pmatrix}0\\1\\1\end{pmatrix}\Rightarrow a=2,b=2,c=2,d=2$$

$s=2\cdot 2+2\cdot 1+2\cdot 2+2\cdot 0(\mathrm{mod}\,3)=1$ olarak anahtar tekrar bulunur.

Biz son olarak ikinci minimal kodsöz için inşayı yapalım diğerleri de benzer biçimde yapılabilir.

$g_0=ag_2+bg_3+cg_4$ ve $s=aP_2+bP_3+cP_4$ olduğundan öncelikle $a,b,c\in \mathrm{F}_3$ değerlerini bulmalıyız.

$$\begin{pmatrix}1\\0\\0\end{pmatrix} = a\begin{pmatrix}0\\0\\2\end{pmatrix} + b\begin{pmatrix}2\\1\\1\end{pmatrix} + c\begin{pmatrix}1\\1\\2\end{pmatrix} \Rightarrow a = 2, b = 1, c = 2$$

$s = 2.1 + 1.2 + 2.0 (\mathrm{mod}\, 3) = 1$ olarak anahtar tekrar bulunur.

Bu örnekte her kullanıcı eşit sayıda minimal erişim kümelerinde bulunduğundan demokratiklik derecesi 3'tür.

Tabi ki bu örnekler küçük boyut ve uzunluklarda yapıldı, daha büyük örnekler için minimal kodsözleri bulmak oldukça zor bir işlemdir. Şu an bununla ilgili yapılan çalışmalarda belirli kod ve sınıflar için minimal kodsözler belirlenmiştir. Yani araştırmacılar için değişik sınıflarda bu problemi çözmek açık bir problemdir.

BÖLÜM 8

KESİRLİ TEKRARLI KOD (FRACTIONAL REPETITION CODE) İLE SIR PAYLAŞIM SİSTEMİ

Bu bölümde 2010 yılında Salim El Rouayheb ve Kannan Ramchandran tarafından inşa edilen Kesirli Tekrarlı Kod (Fractional Repetition Kod (FR Kod)) anlatılacak ve Sır Paylaşım sistemi üzerine uygulanmaya çalışılacaktır [24]. Bizim tanımladığımız bu yöntemde anahtar genel bir haldedir ve hatalı kullanıcılara karşı çalışabilen bir sistemdir. Bu kısımda ilk olarak FR Kod tanıtılacak ve bu kod üzerinde nasıl bir yöntem inşa ettiğimiz gösterilecektir.

8.1 Paylaşmalı Depolama Sistemi (Distributed Storage Systems (DS Sistem))

Günlük yaşamda kullandığımız bilgisayarlar da ya da cep telefonlarında çok farkında olamasak da veri transferleri sırasında donanımdan veya ağ transferinden kaynaklı olarak veriler kaybolabilir ya da zarar görebilir. DS sistem sayesinde veriler daha uzun süre ve daha güvenli bir biçimde saklanabilir [24]. Bu sistemde alınan dosya “node” adı verilen parçalara bölünür ve depolama işlemi “node” lar ile yapılır.

Not 8.1: Node, graflar da ki düğüm kavramına karşılık gelir. Verilerin depolanmasında yer alan sıralı n-li ler olarak adlandırılabilir. Tezde de node yerine düğüm kavramı kullanılacaktır.

Tanım 8.1 Bir (n,k,d) parametreli DS sistem de;

i. n ile dosyanın bölündüğü düğüm sayısı,

ii. $k < n$ ile dosyanın tekrar oluşturulabilmesi için gerekli olan düğüm sayısı,

iii. d ile bozulan ya da kaybolan düğümün tamiri için gerekli olan düğüm sayısı

ifade edilir [24]. Burada her zaman $k \geq d\,'dir.$

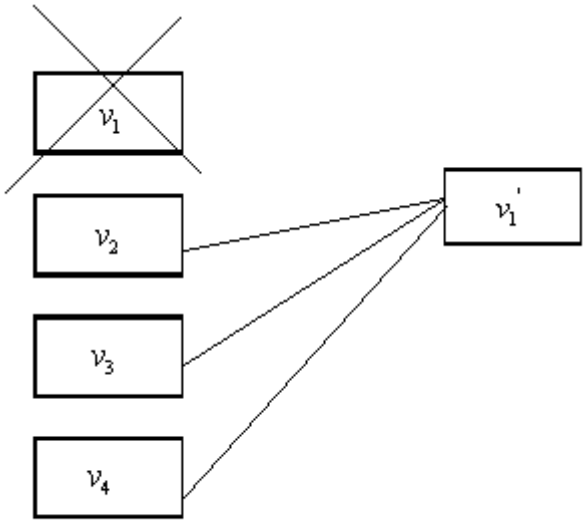
Tanımda ki ii özelliğine MDS özelliği denilmektedir. Bölüm 5'te de anlatıldığı gibi herhangi k tanesi ile bütüne ulaşıldığından bu isim verilmiştir.

d ifadesine de tamir derecesi denilirken, kullanılan d düğüme de kurtarıcı düğüm denilmektedir [24].

DS sistem dosyayı parçalara bölerek, hatada ya da kaybolma da tüm dosyayı taramaktansa lokal olarak tarama yapmaktadır. Böylece kısa zamanda ve daha ucuz olarak tamir sürecini tamamlamaktadır.

Hata ya da kaybolma olduğunda sistem tarafından bir boş düğüm oluşturulur. Bu boş düğümler "blank node" olarak adlandırılır. Oluşturulan boş düğümlerle, d tane düğüm bağlantı kurarak düğümde olan bilgi tekrar bulunur ve kaybolan düğüm aynen oluşturulmuş olur. Aşağıdaki örnekte DS sistemin işleyişi şekil üzerinde gösterilmiştir.

Örnek 8.1 $(4,2,3)$ DS sistem örneği



Şekil 8.1 $(4,2,3)$ DS sistem

Yukarıdaki örnekte dosya 4 düğüme bölünmüştür, yani depolama işlemi 4 düğümde yapılmıştır. v_1 düğümün de hata veya kaybolma olması durumunda, şeklin ikinci

tarafında gösterildiği gibi yeni bir $v_1^{'}$ düğümü oluşturulur. $(4,2,3)$ sistem olduğundan 3 düğümle de tamir süreci gerçekleştirilir ve v_1 düğümünün bilgileri $v_1^{'}$ düğümüne aktarılır.

Tanım 8.2 Bir (n,k,d) parametreli DS sistem de depolama kapasitesi

$C_{MBR}(n,k,d) = kd - \binom{k}{2}$ ile ifade edilir [24].

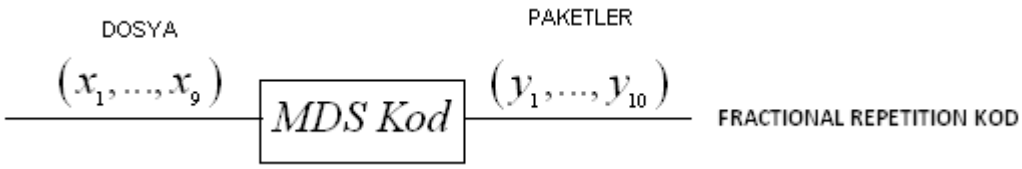
Depolama kapasitesi, sistemin k düğümle elde edilecek maximum bilginin değerini ifade eder. Yani k düğüm bilindiğinde depolanan dosyanın ne kadarına ulaşılabildiğini gösterir [24].

Not 8.2: Burada MBR ile ifade edilen Minumum Bandwidth Regenerating koddur [24]. Tezde anlatılacak olan FR kod bu kodun genel hali olduğundan o kısma girilmemiştir.

Örnek 8.2 $(5,3,4)$ DS sistem için $C_{MBR}(5,3,4) = 3\cdot 4 - \binom{3}{2} = 12-3 = 9'dur.$

8.2 FR Kodun İnşası

DS sistem için geliştirilen kodlar vardır. Bu kodlardan bir taneside FR koddur. FR kodda, MDS özelliğinin sağlanması için kod önce MDS kod özelliği sağlanacak şekilde paketlere aktarılır ve bu paketlerde belirli bir zaman içerisinde düzenli tekrar ederek hatalara karşı sistemi garanti altına alır. FR kodun yapısı aşağıda şematize edilmiştir.



ŞekiL 8.2 FR Kod Yapısı

FR kodun diğer kodlara göre avantajları vardır. Bu kodun tamir süreci çok hızlıdır ve dışarıdan yardım almadan gerçekleştirilir [24]. Ayrıca çoklu hatalara karşıda sistem çalışabilmektedir.

Tanım 8.3 (n,k,d) DS sistem için tekrar derecesi ρ olan C FR kodu şu şekilde tanımlanır;

$\Omega = \{1,2,...,\theta\}$ farklı paketlerin sayısı ve $V_1, V_2, ...V_n$ 'de düğümleri göstermek üzere, FR kod

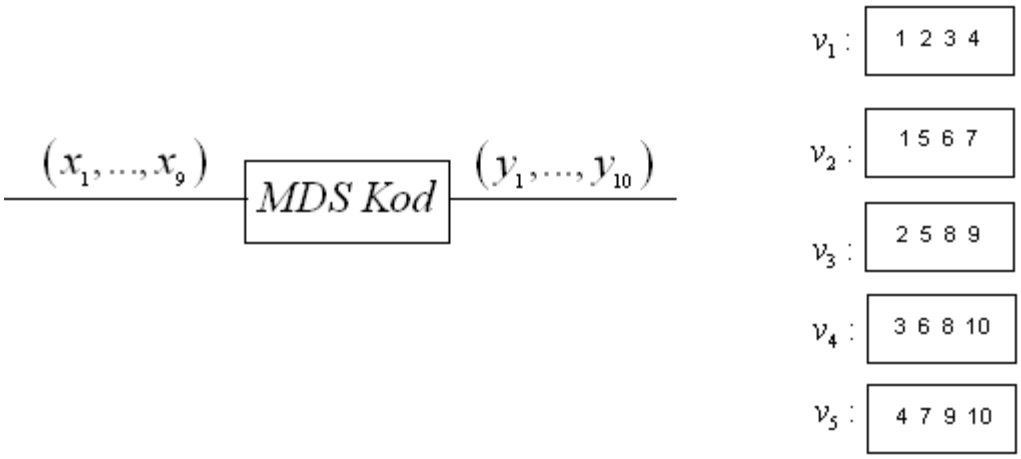
$C = \{V_1, V_2, ...V_7\}$' dir [24].

Not 8.3: i) ρ tekrar derecesiyle paketlerin belirli bir zaman içerisinde aynı sayıda tekrar etmesi anlatılmaktadır.

ii) Sistemdeki d sayısı aynı zamanda düğümlerin uzunluğunu da belirtir [24].

Örnek 8.3 $X = (x_1,...,x_9) \in \mathrm{F}_q^{\,9}$ dosyasını $(5,3,4)$ DS sistemi kullanarak, $\rho = 2$ tekrarlı FR kodu ile kodlanması;

Bu depolama DS sistem üzerinde FR kod kullanarak şu şekilde yapılabilir.



Şekil 8.3 $\rho = 2$ Tekrarlı FR kod

Bu örnek için $C_{MBR}(5,3,4) = 3\cdot 4 - \binom{3}{2} = 12 - 3 = 9$' dur, yani herhangi 3 düğümle en fazla 9 pakete ulaşılabilir.

Sisteme bir tane kontrol hanesi (parity check) eklendiğinden $(10,9)$ MDS kod elde edilmiştir. Böylece alınan $X = (x_1,...,x_9)$ dosyasına karşılık, $Y = (y_1,...,y_{10})$ elde edilmiştir.

Burada kodlama şu şekilde yapılmıştır;

$y_i = x_i, i = 1,...,9$ *ve* kontrol hanesi $y_{10} = \sum_{i=1}^{9} x_i$ 'dir.

Kodlanmış paketler, $\rho = 2$ olduğundan 2 tekrarlı olarak düğümlere yerleştirilmiştir. Ayrıca herhangi iki düğüm sadece 1 pakette olacak şekilde özel bir tasarım yapılmıştır. Bu tasarım sayesinde tamir işlemi gerçekleştirilebilmektedir.

$(5,3,4)$ DS sistem olduğundan 3 tane düğüm ile $X = (x_1,...,x_9)$ dosyasına ulaşılabilir. Örneğin, v_1, v_4 *ve* v_5 düğümlerini kullanarak $\{1,2,3,4,6,7,8,9,10\}$ paketlerine ulaşılır, buradan da kontrol hanesi kullanılarak $X = (x_1,...,x_9)$ dosyası tekrar elde edilir.

Eğer herhangi bir düğüm de bozulma ya da kaybolma gerçekleşirse bu örnek için 4 düğümle tamir gerçekleştirilebilir. Örneğin v_2 düğümü bozulursa diğer düğümler kullanılarak özel bir tasarım olduğundan kolay biçimde bulunabilir. (Her paket iki defa kullanılacağından, diğer 4 düğüme bakıldığında 2'şer defa kullanılmayan 1, 5, 6 ve 7 paketleri vardır ve v_2 düğümüne ulaşılır.)

Son olarakta burada kullandığımız düğümler FR kodun kodsözleridir. Yani C FR kodu;

$C = \{v_1, v_2, v_3, v_4, v_5\}$, *burada* $v_1 = \{1,2,3,4\}, ...,\ v_5 = \{4,7,9,10\}$ biçimindedir.

Tanım 8.4 (n,k,d) DS sistem ve $C = \{V_1,...,V_n\}$ FR kodu için FR kod oranı;

$R_C(k) := \min_{\substack{I \subset [n] \\ |I|=k}} \left| \cup_{i \in I} V_i \right|$ biçiminde tanımlıdır [24]. $\left(\ [n] = \{1,2,...,n\} \ \right)$

Tanım 8.5 $R_C(k) \geq C_{MBR}(n,k,d)$ ise FR koda evrensel iyi kod(universally good code) denir [24].

Önerme 8.1 (n,k,d) DS sistem için ρ tekrar derecesi ve θ farklı paket sayısını göstermek üzere

$$nd = \theta\rho \text{ '} \text{ dir [24].}$$

8.2.1 $\rho = 2$ Tekrarlı Durum için FR Kodun İnşası

$\rho = 2$ durumu için düzenli graflar üzerinde geliştirilen algoritma şu şekildedir:

1) Genel olarak d. dereceden $u_1, \ldots, u_n$ şeklindeki n düğümlü düzenli graf $R_{n,d}$ ile gösterilir.

2) $R_{n,d}$ nin kenarları, 1' den $\frac{nd}{2}$ olacak şekilde numaralandırılır.

3) Depolanan v_i düğümünün paketleri, sırasıyla u_i düğümünün komşularıdır.

Not 8.4: i)Düzenli graflar, her düğümden aynı sayıda kenarın çıktığı graflardır.

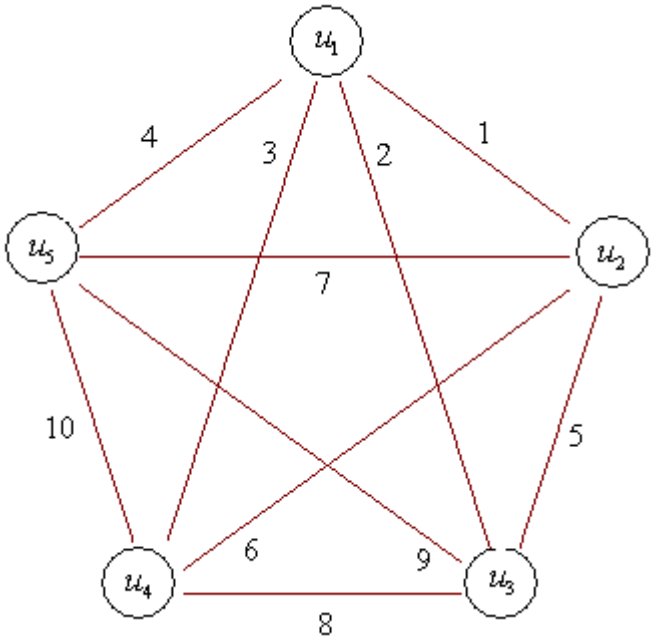
ii) $\rho = 2$ için FR kod tek hata düzeltir [24].

Örnek 8.4 Örnek 8.3 düzenli graf üzerinde şu şekilde inşa edilir:

1) $(5,3,4)$ DS sistem olduğundan $R_{5,4}$ düzenli graf çizilir.

2) Kenarlar 1'den $\frac{nd}{2} = \frac{5 \cdot 4}{2} = 10$ 'a kadar numaralandırılır.

3) Komşuluklar düğümler için yazıldığında (aşağıdaki şekilden) Örnek 8.3' teki FR kod elde edilir.



Şekil 8.4 $R_{5,4}$ Graf

Örneğin u_1'in komşulukları $1, 2, 3, 4$ kenarlarıdır, bunlar da v_1 düğümünün paketlerine karşılık gelir.

Lemma 8.1: $\rho = 2$ için inşa edilen yukarıdaki FR kod, universally good koddur [24].

8.2.2 $\rho > 2$ Tekrarlı Durum için FR Kodun İnşası

$\rho > 2$ durumu için iki farklı inşa vardır. Steiner Sistem'e dayalı olan bu iki inşa verilmeden önce kısaca Steiner Sistem anlatılacaktır.

Tanım 8.6 $S(t, \alpha, v)$ Steiner Sistem, bloklar ve noktalar kümesinden oluşur öyle ki; bloklar kümesi $B = \{B_1, ..., B_b\}$ ve noktalar kümesi $V = \{v_1, ..., v_v\}$ olmak üzere t nokta birlikte yalnızca bir blokta bulunabilir. Burada ki α değeri blokların eleman sayısını ifade eder [24].

Not 8.4: i) FR kodda her zaman $t = 2$'dir. Yani iki düğüm en fazla 1 pakette kesişebilir.

ii) $\rho > 2$ için FR kod $\rho - 1$ hata düzeltir [24].

Önerme 8.2 $S(2, \alpha, v)$ Steiner Sistem için;

$$b\alpha = vr,$$
$$v - 1 = r(\alpha - 1)'dir.$$

Burada b ile blok sayısı, r ile de noktaların tekrar sayısı gösterilmektedir [24].

Önerme 8.2' de ki eşitlikle Önerme 8.1' de ki eşitlik birbirine denktir. Yani $v = \theta,\ r = \rho,\ \alpha = d\ ve\ b = n$ olarak düşünülebilir [24]. Dolayısıyla Steiner Sistem üzerine FR kod inşa edilebilir.

Teorem 8.1 α pozitif bir sayı olmak üzere, yeterince büyük v sayısına karşılık gelen $S(2, \alpha, v)$ Steiner Sistem olması için $vr \equiv 0 \bmod \alpha$ ve $v - 1 \equiv 0 \bmod \alpha - 1$ olmalıdır [24].

8.2.2.1 Kod İnşaları

Kod İnşası 1: $S(2, \alpha, v)$ Steiner Sistem'i $B = \{B_1, ..., B_b\} \subset V = [v]$ blokları ile verildiğinde, C FR kodu $C = \{B_1, ..., B_b\}$ olur. Burada parametreler

$$\rho = \frac{v-1}{\alpha - 1},\ \theta = v,\ n = \frac{v(v-1)}{\alpha(\alpha - 1)}\ ve\ d = \alpha'dır\ [24].$$

Lemma 8.2: $\rho > 2$ için inşa edilen yukarıdaki FR kod, universally good koddur [24].

Örnek 8.5 $S(2,3,9)$ Steiner Sistem 'e karşılık gelen FR kod aşağıdaki gibidir.

$$1)\ \rho = \frac{v-1}{\alpha-1} = \frac{9-1}{3-1} = 4$$
$$2)\ \theta = v = 9$$
$$3)\ n = \frac{v(v-1)}{\alpha(\alpha-1)} = \frac{9\cdot(9-1)}{3\cdot(3-1)} = 12 \ ve\ d = \alpha = 3$$

Parametrelerine sahip olan FR kod;

$v_1 : 1\ 2\ 3$ $\quad$ $v_7 : 2\ 6\ 7$
$v_2 : 1\ 4\ 7$ $\quad$ $v_8 : 3\ 4\ 8$
$v_3 : 1\ 5\ 9$ $\quad$ $v_9 : 3\ 5\ 7$
$v_4 : 1\ 6\ 8$ $\quad$ $v_{10} : 3\ 6\ 9$
$v_5 : 2\ 4\ 9$ $\quad$ $v_{11} : 4\ 5\ 6$
$v_6 : 2\ 5\ 8$ $\quad$ $v_{12} : 7\ 8\ 9$

olur.

Bu inşada n ve ρ parametreleri açıkça görülememektedir, bu yüzden ikinci bir inşa kodun duali alınarak bulunmuştur [24].

Kod İnşası 2: $S(2,\alpha,v)$ Steiner Sistem'i $B = \{B_1,\ldots,\ B_b\} \subset V = [v]$ blokları ile verildiğinde, C FR kodu $C = \{V_1,\ldots,V_n\}$ olur. Burada $V_i = \left\{ j \,\middle|\, i \in B_j, i = 1,\ldots,n \right\}' dir.$

Parametreler:

$\rho = \alpha,\ \theta = \frac{n(n-1)}{\rho(\rho-1)},\ n = v\ ve\ d = \frac{n-1}{\rho-1}$' dır [24].

Yukarıda ki inşadan farklı olarak burada noktalar ve bloklar kümesi yer değiştirmiştir. Yani bu inşa da bloklar paketlere, noktalar düğümlere karşılık gelir.

Örnek 8.6 Örnek 8.5 bu yöntemle inşa edilirse;

$$1)\ \rho = \alpha = 3$$
$$2)\ \theta = \frac{n(n-1)}{\rho(\rho-1)} = 12$$
$$3)\ n = v = 9\ ve\ d = \frac{n-1}{\rho-1} = 4$$

Parametrelerine sahip olan FR kod;

v_1 : 1 2 3 4 v_7 : 2 7 9 12
v_2 : 1 5 6 7 v_8 : 4 6 8 12
v_3 : 1 8 9 10 v_9 : 3 5 10 12
v_4 : 2 5 8 11
v_5 : 3 6 9 11
v_6 : 4 7 10 11

olur.

Bu iki kod birbirine denktir. Yani bir düzleme aktarıldığında ikisi de aynı sonucu verecektir.

8.3 FR Kod ile Sır Paylaşım Sistemi

Bu bölümde FR kod üzerinde Sır Paylaşım Sistemini tanımlayacağız. Bizim geliştirdiğimiz bu yöntem de, sistemimiz hatalı kullanıcılara karşı dayanıklıdır ve anahtar genel bir haldedir. Bu özellikleriyle RS kodlara benzemektedir.

8.3.1 Sistemin Çalışma Şeması

Bu yöntemde dağıtıcı $s = (s_1, s_2, ..., s_t) \in \mathrm{F}_q^n$ olacak biçimde genel bir halde anahtarı seçer. Sistemde kaç tane kullanıcı olacağına ve kaç tanesiyle sistemin tekrar oluşturulabileceğine karar verir. Burada alacağı değerler, FR kod üzerinde sistem kurulacağından

$nd = \theta\rho$ eşitliğini sağlayacak şekilde olmalıdır. Çünkü sistemde kullanıcılar kümesi düğümler kümesine karşılık gelecektir. Yani P kullanıcılar kümesini göstermek üzere, $P = \{V_1, V_2, ..., V_n\}$'dir.

Sistemi kuracak değerler belirlendikten sonra FR kod inşa edilip, düğümler kullanıcılara dağıtılacaktır.

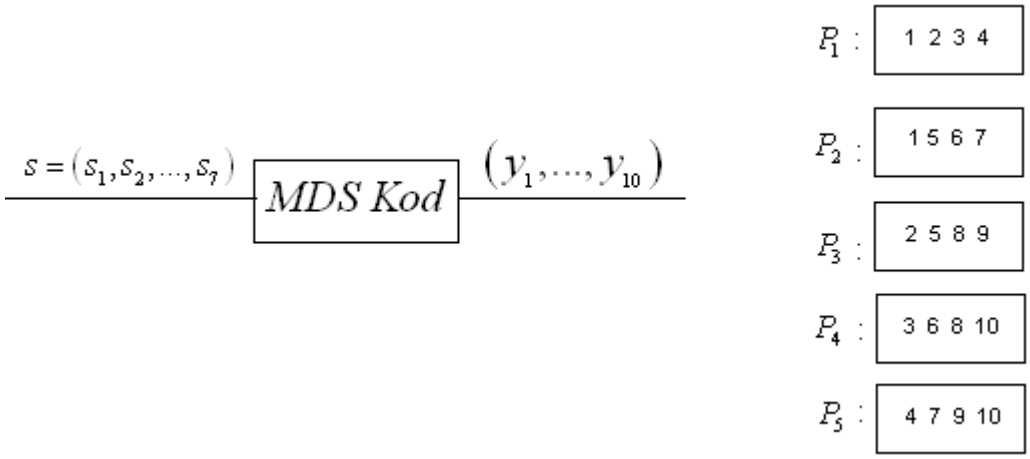
Dağıtım işlemi gerçekleştikten sonra, herhangi alt kümelerin tekrar anahtara ulaşabilmesi için kontrol hanelerinin sisteme uygun olarak seçilmesi gerekir.

Anahtarın tekrar inşa edilmesi için, herhangi k tane kullanıcının bilgileri birleştirilir ve kontrol haneleri kullanılarak inşa süreci tamamlanır.

Not 8.5: Kod tamamen tasarım olduğundan, hatalı kullanıcılara karşı da sistem çalışmaktadır ve sistem $\rho - 1$ hataya karşı çalışır.

Örnek 8.7 $s = (s_1, s_2, ..., s_7) \in \mathrm{F}_q^7$ anahtarlı ve $(2,5)$ sistem kurulmak istenirse;

$nd = \theta\rho$ eşitliğini sağlayacak şekilde bir FR kod kullanılmalıdır. Örnek 8.3' de kullanılan kod uygulanırsa sistem şu şekilde elde edilir:



Şekil 8.5 FR Kod ile Sır Paylaşım Sistemi

Kodlama;

$$y_i = s_i, i = 1, ..., 7 \quad ve \quad \begin{matrix} y_8 = s_3 + s_4 + s_5 + s_6 \\ y_9 = s_1 + s_3 + s_5 + s_7 \\ y_{10} = s_2 + s_6 + s_7 \end{matrix}$$ biçiminde yapılsın.

$k = 2$ olduğundan herhangi 2 kullanıcıyla sistem tekrar oluşturulabilmelidir.

$\binom{5}{2} = 10$ farklı biçimde kullanıcılar seçilebilir. Tüm kullanıcılar için sonuç aşağıdaki tabloda verilmiştir:

Alınan Kullanıcılar	Elde Edilen Bilgiler	Eksik Bilgi
P_1, P_2	$(1,2,3,4,5,6,7)$	Yok
P_1, P_3	$(1,2,3,4,5,8,9)$	$(6,7)$
P_1, P_4	$(1,2,3,4,6,8,10)$	$(5,7)$
P_1, P_5	$(1,2,3,4,7,9,10)$	$(5,6)$
P_2, P_3	$(1,2,5,6,7,8,9)$	$(3,4)$
P_2, P_4	$(1,3,5,6,7,8,10)$	$(2,4)$
P_2, P_5	$(1,4,5,6,7,9,10)$	$(2,3)$
P_3, P_4	$(2,3,5,6,8,9,10)$	$(1,4,7)$
P_3, P_5	$(2,4,5,7,8,9,10)$	$(1,3,6)$
P_4, P_5	$(3,4,6,7,8,9,10)$	$(1,2,5)$

Tablo incelendiğinde görülecektir ki kullanıcılarda bulunan kontrol haneleriyle eksik bilgiler bulunabilir ve bu bilgiler kullanılarak anahtara tekrar ulaşılabilir. Örneğin P_1, P_4 kullanıcıları için durum incelenirse, eksik olan $(5,7)$ bilgileri $y_8 \ ve \ y_{10}$ kontrol haneleri kullanılarak çözülebilir.

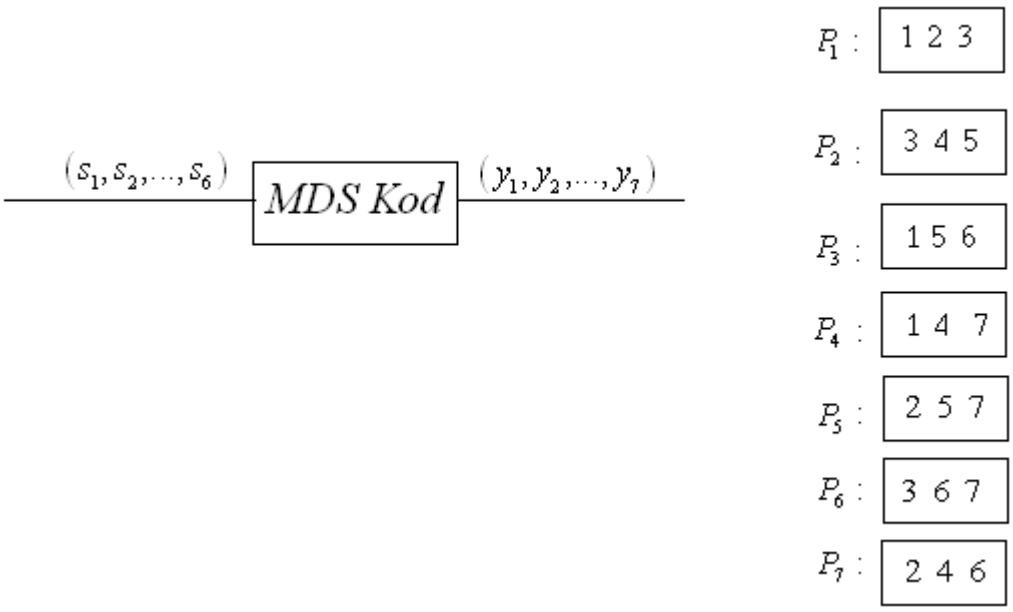
Sistemin hatalı kullanıcılara karşı da çalışabildiği söylenmişti. Bu örnek 2 tekrarlı olduğundan 1 hatalı kullanıcıya karşı koyulabilir. Örneğin sistem de $(1,4,6,7)$ şeklinde bir hatalı kullanıcı kullanılmaya çalışıldığında, FR kod tanımı gereği P_2 kullanıcısında da $(6,7)$ değerleri olduğundan hatalı olduğu anlaşılacaktır.

Örnek 8.8 $s=(s_1,s_2,...,s_6)\in \mathrm{F}_q^6$ anahtarlı ve $(3,7)$ sistem kurulmak istenirse;

$nd=\theta\rho$ eşitliğini sağlayacak şekilde bir FR kod kullanılmalıdır. Bu örnek 2 hataya karşı çalışabilir olsun, o halde 3 tekrarlı kod inşa edilmelidir. Bu inşa $S(2,3,7)$ Steiner Sistem kullanılarak yapılabilir. İnşa ile elde edilen kod:

v_1 : 1 2 3
v_2 : 3 4 5
v_3 : 1 5 6
v_4 : 1 4 7
v_5 : 2 5 7
v_6 : 3 6 7
v_7 : 2 4 6 '*dır*.

Bu kod üzerinde inşa şu şekilde yapılır:



Şekil 8.6 FR Kod ile 2 Hatalı Sır Paylaşım Sistemi

Kodlama;

$y_i = s_i, i = 1,...,6 \;\; ve \;\; y_7 = \sum_{i=1}^{6} s_i$ biçiminde yapılsın.

$k = 3$ olduğundan herhangi 3 kullanıcıyla sistem tekrar oluşturulabilmelidir.

$\binom{7}{3} = 35$ farklı biçimde kullanıcılar seçilebilir. Tüm kullanıcılar için sonuç aşağıdaki tabloda verilmiştir:

Alınan Kullanıcılar	Elde Edilen Bilgiler	Eksik Bilgi
P_1, P_2, P_3	$(1,2,3,4,5,6)$	Yok
P_1, P_2, P_4	$(1,2,3,4,5,7)$	(6)
P_1, P_2, P_5	$(1,2,3,4,5,7)$	(6)
P_1, P_2, P_6	$(1,2,3,4,5,6,7)$	Yok
P_1, P_2, P_7	$(1,2,3,4,5,6)$	Yok
P_1, P_3, P_4	$(1,2,3,4,5,6,7)$	Yok
P_1, P_3, P_5	$(1,2,3,5,6,7)$	(4)
P_1, P_3, P_6	$(1,2,3,5,6,7)$	(4)
P_1, P_3, P_7	$(1,2,3,4,5,6)$	Yok
P_1, P_4, P_5	$(1,2,3,4,5,7)$	(6)
P_1, P_4, P_6	$(1,2,3,4,6,7)$	(5)
P_1, P_4, P_7	$(1,2,3,4,6,7)$	(5)
P_1, P_5, P_6	$(1,2,3,5,6,7)$	(4)
P_1, P_5, P_7	$(1,2,3,4,5,6,7)$	Yok

P_1, P_6, P_7	$(1,2,3,4,6,7)$	(5)
P_2, P_3, P_4	$(1,3,4,5,6,7)$	(2)
P_2, P_3, P_5	$(1,2,3,4,5,6,7)$	Yok
P_2, P_3, P_6	$(1,3,4,5,6,7)$	(2)
P_2, P_3, P_7	$(1,2,3,4,5,6)$	Yok
P_2, P_4, P_5	$(1,2,3,4,5,7)$	(6)
P_2, P_4, P_6	$(1,3,4,5,6,7)$	(2)
P_2, P_4, P_7	$(1,2,3,4,5,6,7)$	Yok
P_2, P_5, P_6	$(2,3,4,5,6,7)$	(1)
P_2, P_5, P_7	$(2,3,4,5,6,7)$	(1)
P_2, P_6, P_7	$(2,3,4,5,6,7)$	(1)
P_3, P_4, P_5	$(1,2,4,5,6,7)$	(3)
P_3, P_4, P_6	$(1,3,4,5,6,7)$	(2)
P_3, P_4, P_7	$(1,2,4,5,6,7)$	(3)
P_3, P_5, P_6	$(1,2,3,5,6,7)$	(4)
P_3, P_5, P_7	$(1,2,4,5,6,7)$	(3)
P_3, P_6, P_7	$(1,2,3,4,5,6,7)$	Yok
P_4, P_5, P_6	$(1,2,3,4,5,6,7)$	Yok
P_4, P_5, P_7	$(1,2,4,5,6,7)$	(3)
P_4, P_6, P_7	$(1,2,3,4,6,7)$	(5)
P_5, P_6, P_7	$(2,3,4,5,6,7)$	(1)

Tablo incelendiğinde görülecektir ki diğer örnekte olduğu gibi kullanıcılarda bulunan kontrol hanesiyle eksik bilgi bulunabilir ve bu bilgiler kullanılarak anahtara tekrar ulaşılabilir. Örneğin P_1, P_4, P_6 kullanıcıları için durum incelenirse, eksik olan (5) bilgisi y_7 kontrol hanesi kullanılarak çözülebilir.

Bu örnek 3 tekrarlı olduğundan 2 hatalı kullanıcıya karşı koyulabilir. Örneğin sistem de $(1,4,5)$ ve $(2,6,7)$ şeklinde iki hatalı kullanıcı kullanılmaya çalışıldığında, FR kod tanımı gereği P_2 kullanıcısında da $(4,5)$ ve P_6 $(6,7)$ değerleri olduğundan kullanıcıların hatalı olduğu anlaşılacaktır.

BÖLÜM 9

SONUÇ VE ÖNERİLER

Bu tezde anahahtar saklama yöntemi olan, sır paylaşım sitemi ve çözüm yöntemleri anlatılmıştır. Bütün lineer kodlara uygulanabilen bu sistemde asıl önemli olan minimal erişim kümelerine ulaşabilmektir, çünkü büyük örnekler ve farklı sınıflardaki kodlar için bunu yapmak kolay değildir. Dolayısıyla farklı sınıflardaki kodlara ve yeni inşa edilen kodlara sistem uygulanabilir.

Ayrıca son bölümde anlatılan ve üzerine uygulaması yapılan FR kod içinde sistem geliştirilebilir ve yeni önermeler elde edilip, sınırlar verilebilir. Her konuyla bağlantısı sağlanabilecek bir konu olduğundan farklı yöntemler geliştirilebilir.

KAYNAKLAR

[1] Ling S. and Xing C, (2004), Coding Theory A First Course, National University of Singapore, Cambridge University Press.

[2] Huffman W. C. and Pless V., (2003), Fundamentals of Error-Correcting Codes, Cambridge University Press.

[3] MacWilliams F. J. and Sloane N. J., (1977), The Theory of Error-Correcting Codes Amsterdam, The Netherlands: North- Holland.

[4] Karnin, D.E., Greene, J.W. ve Hellman, M.E., (1983). ” On Secret Sharing Systems”, IEEE Transaction on Information Theory, 29: 35–41.

[5] http://www.bilgisayarkavramlari.com/2009/06/16/simetrik-sifreleme-symmetric- encryption/, 25 Nisan 2012

[6] http://www.bidb.itu.edu.tr/?d=1002, 25 Nisan 2012

[7] Tuncal, T., (2008). Bilgisayar Güvenliği Üzerine Bir Araştırma ve Şifreleme Deşifreleme Üzerine Uygulama, Yüksek Lisans Tezi, Maltepe Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

[8] Shamir, A., (1979). ” How to Share a Secret ”, Communications of the ACM, 22: 612-61

[9] Blakley, G.R., (1979). ” Safeguarding Cryptographic Keys ”, IEEE Transaction on Information Theory, 48: 313–317.

[10] Landjev, I.N., (1999). “ The Mathematical Foundation of Secret Sharing”, InternationalWorkshop Information Security in the 21st Century Global Convergence, September 1999, Bansko.

[11] Brickell, E.F., (1990). “ Some Ideal Secret Sharing Schemes” Springer-Verlag: 468-475

[12] McEliece, R.J. ve Sarwate, D.V., (1981). ” On Sahring Secrets and Reed Solomon Codes”, Communications of the ACM, 24: 583-584

[13] Wildon, M., (2010) , Theory of Error Correcting Codes MT5461, http://www.ma.rhul.ac.uk/~uvah099/Maths/Codes10/MT54612010Notes.pdf, 27 Mart 2012.

[14] Asmuth, C. ve Bloom, J., (1983). ” A Modular Approach Key Safeguarding”, IEEE Transaction on Information Theory, 29: 208–210.

[15] Arda, D. ve Buluş, E., “Çin kalan teoremini kullanan bir gizlilik paylaşım şeması”,IV.İletişim Teknolojileri Ulusal Sempozyumu, Ekim-2009, Adana, 23-26.

[16] Li, Z., Xue, T. ve Lai, H., (2009). “ Secret Sharing Schemes from Binary Linear Codes”, ELSEVIER Information Sciences, 4412-4419.

[17] Ding, C., Kohel, D.R. ve Ling, S., (1999). “ Secret Sharing with a class of Ternary Codes”, ELSEVIER Theoretical Computer Science,285-298.

[18] Özadam, H., (2008). Construction of Secret Sharing Schemes Using Linear Codes, Dönem Projesi, ODTÜ Uygulamalı Matematik Enstitüsü, Ankara.

[19] Massey, J.L., (1993). “Minimal codewords and secret sharing”, 6th Joint Swedish- Russian Workshop On Information Theory, 276-279.

[20] Ashikhmin, A. ve Barg, A., (1994). “ Minimal Vectors in Linear Codes and Sharing of Secrets” , Fourth International Workshop Algebraic and Combinatorial Coding Theory,11-17 September 1994, Novgorod.

[21] Ashikhmin, A., Barg, A., Cohen, G. ve Huguet, L., (1995). “ Variations on Minimal Codewords in Linear Codes”, 11th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, 1995, London, 96-105.

[22] Ding, C. ve Yuan, J., (2003). “ Covering and secret sharing with linear codes”, In Discrete Mathematics and Theoretical Computer Science (Lecture Notes in ComputerScience), 2003, London, 11-25.

[23] Ding, C. ve Yuan, J., (2006). “ Secret Sharing Schemes from Three Classes of LinearCodes”, IEEE Transactions on Information Theory, 206-212.

[24] Rouayheb, E.S. ve Ramchandran, K., (2010). “Fractional Repetition Codes for Repair in Distributed Storage Systems, Forty-Eighth Annual Allerton Conference Allerton House, USA.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı **:**İbrahim Özbek

Doğum Tarihi ve Yeri **:**05/12/1987, Kayseri

Yabancı Dili: :İngilizce

E-posta: **:**iozbek@yildiz.edu.tr

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Lisans	Matematik	Yıldız Teknik Üniversitesi	2010
Lise	Fen Bilimleri	Mensucat Santral Lisesi	2006

İŞ TECRÜBESİ

Yıl	Firma/Kurum	Görevi
2011- …	Yıldız Teknik Üniversitesi	Araştırma Görevlisi