KOCAELİ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ ANABİLİM DALI

YÜKSEK LİSANS TEZİ

SIR GÖRÜNTÜ PAYLAŞIM ŞEMALARI ÜZERİNE BİR ÇALIŞMA

FATİH MOLLA

KOCAELİ 2018

K OCAELİ ÜNİVERSİTESİ

F EN BİLİMLERİ ENSTİTÜSÜ

BİLİŞİM SİSTEMLERİ MÜHENDİSLİĞİ

YÜKSEK LİSANS TEZİ

SIR GÖRÜNTÜ PAYLAŞIM ŞEMALARI ÜZERİNE BİR ÇALIŞMA

FATİH MOLLA

Doç. Dr. Selda ÇALKAVUR
Danışman, Kocaeli Üniversitesi .....

Doç. Dr. Murat GÜZELTEPE
Jüri Üyesi, Sakarya Üniversitesi .....

Dr. Öğr. Üyesi Adnan SONDAŞ
Jüri Üyesi, Kocaeli Üniversitesi .....

Tezin Savunulduğu Tarih: 14.05.2018

ÖNSÖZ VE TEŞEKKÜR

Çalışmalarım esnasında, beni yalnız bırakmayan, değerli görüş ve fikirleri ile bu teze yön veren ve her türlü desteğini esirgemeyen saygıdeğer hocam Sayın Doç. Dr. Selda Çalkavur'a katkılarından dolayı teşekkür etmeyi büyük bir borç bilir, saygılarımı sunarım. Bana her zaman destek olan kıymetli aileme teşekkür ederim.

Haziran - 2018 Fatih MOLLA

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

TABLOLAR DİZİNİ

SİMGELER VE KISALTMALAR

F_q veya GF(q)	:	Mertebesi $q = p^r$ (p asal, r pozitif tam sayı) olan Galois cismi
$(F_q)^n$	:	tüm $a = a_1 a_2 \ldots a_n, (a_i \in F_q)$ olan sıralı n-lilerinin kümesi
$d(x, y)$	:	x ve y vektörleri arasındaki Hamming uzaklığı
C	:	C kodu
d(C)	:	C kodunun minimum uzaklığı
wt(x)	:	$(F_q)^n$ deki bir x vektörünün ağırlığı
(n, M, d)-kod	:	n uzunluklu, M kodsözcüğü içeren ve minimum uzaklığı d olan kod
$[n, k, d]$-kod	:	uzunluğu n, boyutu k ve minimum uzaklığı d olan kod
$C^{\perp}$	:	C kodunun duali olan kod
G	:	C kodunun üreteç matrisi
H	:	$C^{\perp}$ kodunun üreteç matrisi
w_{min}	:	F_q üzerinde bir $[n, k]$-kod C deki sıfırdan farklı minimum ağırlık
w_{max}	:	F_q üzerinde bir $[n, k]$-kod C deki sıfırdan farklı maksimum ağırlık
s	:	Sır paylaşım şemasındaki sır
Γ	:	Sır paylaşım şemasının erişim yapısı

SIR GÖRÜNTÜ PAYLAŞIM ŞEMALARI ÜZERİNE BİR ÇALIŞMA

ÖZET

Sır görüntü paylaşım şemalarının incelendiği bu çalışma beş bölümden oluşmaktadır. Bölüm 1'de çalışmada kullanılacak olan matematiksel bilgiler özetlenmiştir. Bölüm 2'de Massey'in sır paylaşım şemasında kullanılan lineer kodlardan söz edilmiştir. Bölüm 3'te sır paylaşım şemaları açıklanmıştır. Bölüm 4'te sonlu cisim genişlemelerinden yararlanılarak yeni bir yaklaşım ile bir sır paylaşım şeması önerilmiştir. Ayrıca sır paylaşım şemalarının görüntüler üzerinde uygulanması açıklanmıştır. Bölüm 5'te elde edilen sonuçlar sunulmuştur.

Anahtar Kelimeler: Cisim Genişlemeleri, Görüntü Paylaşımı, Lineer Kodlar, Sır Paylaşım Şemaları.

A STUDY ON SECRET IMAGE SHARING SCHEMES

ABSTRACT

This study which examines secret sharing schemes consists of five sections. Section 1 gives the necessary concepts from Abstract Algebra which are used the dissertation. Section 2 discusses the linear codes for the Massey's secret sharing scheme. Section 3 contains an introduction to secret sharing schemes. In Section 4 a new secret sharing scheme is proposed by using field extensions. Moreover, this section explains the application of secret sharing schemes on images. Section 5 presents the results which are obtained.

Keywords: Field Extensions, Image Sharing, Linear Codes, Secret Sharing Schemes.

GİRİŞ

İnternetin yaygınlaşması ile bilgi güvenliği daha önemli bir hale gelmiştir. Siyasi, askeri ve tıbbi önem taşıyan görüntülerin, kötü niyetli kişiler tarafından ele geçirilmesine engel olmak amacıyla pek çok yöntem önerilmiştir. Kriptografi ve steganografi bu yöntemlerin en yaygın kullanılanlarıdır. Ancak bazen güvenliği tek bir noktada toplamak sakıncalı olabilir. Bunun yerine gizli bilgi parçalanarak, sırrın farklı yerlerde depolanması tercih edilmektedir. Bu sayede kötü niyetli kişilerin gizli bilgiye erişiminin önlenmesi hedeflenmektedir. Buradan hareketle sır paylaşım şemaları oluşturulmuştur. Önerilen sır görüntü paylaşım şemalarının büyük bir kısmında kayıplar meydana gelmektedir. Yani görüntü üzerindeki bazı piksellerin değerleri tam olarak tekrar elde edilememektedir. Kayıpların olmadığı sır görüntü paylaşım şemaları, kayıpsız olarak adlandırılmaktadır.

Bu çalışmada sonlu cisimler teorisinden yararlanılarak, sır paylaşım şemalarının görüntülere kayıpsız olarak uygulanması için yeni bir yaklaşım önerilmiştir.

Bir sır paylaşım şeması, yönetici, sır ve katılımcı adı verilen varlıklardan oluşur. Yönetici, sırrı paylaştıracak olan kişidir. Katılımcılar, sırrın paylaştırılacağı kimseler veya cihazlardır. Sır ise herkes tarafından bilinmemesi gereken gizli bilgidir. Sır paylaşım şemaları, sırrı paylaştırma ve sırrı tekrar oluşturma olmak üzere iki alt algoritmadan oluşur.

Sır paylaşım şemaları, pek çok bilim insanı tarafından çalışılan bir konudur. Bunlardan bazıları aşağıda özetlenmiştir.

Blakley [1], 1979 yılında banka şifresi gibi hassas bilgilerin tek bir kişi tarafından saklanması sonucu ortaya çıkan problemlere dikkat çekmiş ve bu problemleri önlemek için geometri tabanlı bir sır paylaşım şeması önermiştir.

Shamir [2], 1979 yılında Blakley'den [1] bağımsız olarak sonlu cisimler üzerinde polinom interpolasyonu tabanlı bir (k, n)-eşik sır paylaşım şeması önermiştir. Bu

şemanın parametreleri; s sırrı ($s \in GF(q)$), katılımcı sayısı n, eşik değeri k ($k \leq n$), sonlu cismin mertebesi q ($q > n$ ve q asal) dur. Sır paylaşım işlemi sonucunda yine GF(q) nun elemanı olan n adet sır parçası elde edilir. Ancak bu n tane katılımcıdan en az k tanesi bir araya gelerek sırra ulaşabilir.

Thien ve Lin [3], 2002 yılında görüntüler için bir sır paylaşım yöntemi önermiştir. Bu yöntem, Shamir'in şemasının görüntülere uygulanması olarak ele alınabilir. Burada üzerinde çalışılan sonlu cisim olarak GF(251) kullanılmıştır. Bunun nedeni 251 in, 255 ten küçük en büyük asal sayı olmasıdır. Yine erişim yapısı olarak (k, n)-erişim yapısı kullanılmaktadır ($k \leq n$). Bu yöntemde görüntünün boyutu 1/k oranında küçülmektedir. Dolayısı ile görüntünün depolama, iletme ve başka bir resmin içine steganografi gibi işlemler ile saklanması süreçleri, daha avantajlı hale getirilmektedir. Ancak bu yöntemde 250 den büyük değerler, GF(251) in elemanı olmadığı için kaybedilmektedir. Ayrıca polinomun katsayıları görüntü üzerinden seçildiğinden, başkatsayının sıfır olma ihtimali vardır. Bu ise ilgili pikselin, değerinin daha az katılımcı ile belirlenebileceğini göstermektedir. Fakat görüntü pekçok pikselden oluştuğu için bir noktanın değerinin bilinmesi, önemli bir problem değildir. İstisna bir örnek olarak, sıfır değerinin çok miktarda yer aldığı görüntüler verilebilir. Daha açık bir ifade ile sır parçaları, piksel değerlerinin rastgele seçildiği bir görünümden uzaklaşarak, sırra benzer bir görüntü haline dönüşebilir.

Yang [4], 2007 yılında görüntüler için Shamir'in sır paylaşım şemasını, $GF(2^8)$ üzerinde çalıştırarak kayıpsız bir şema önermiştir.

1. MATEMATİKSEL ALT YAPI

Bu bölümde sır paylaşım şemalarında kullanılacak matematiksel yapılara yer verilmiştir.

1.1. Cebirsel Yapılar

Tanım 1.1. A ve B boş olmayan iki küme olsun. $A \times B$ nin boş olmayan bir alt kümesine, A dan B ye bir bağıntı denir. $R \subseteq A \times B$ bir bağıntı ve $(a,b) \in R$ ise a elemanı R bağıntısına göre b ye bağlı denir ve aRb ile gösterilir [5].

Tanım 1.2. f, A dan B ye bir bağıntı olsun. $\forall\, a \in A$ için, a ya f ile bağlı B de bir ve yalnız bir b elemanı bulunabilirse, f ye A dan B ye bir fonksiyon veya dönüşüm (tasvir) denir ve $f : A \to B$ ile gösterilir [5].

$f : A \to B$ bir fonksiyon ise $a \in A$ ya f fonksiyonu ile karşılık gelen ve tek türlü olarak belirli olan $b \in B$ elemanı,

$(a,b) \in f \Leftrightarrow f(a) = b$

ile gösterilir ve b ye, f fonksiyonu altında a nın görüntüsü veya a ya f fonksiyonu altında b nin orjinali denir. Bağıntı olarak $(a,b) \in f$ gösterimi yerine fonksiyonlar için $f(a) = b$ gösterimi daha sık kullanılır [5].

Tanım 1.3 (İkili işlem). Herhangi bir M kümesi verildiğine göre, $M \times M$ yi M içine resmeden bir tasvir varsa, yani $a,b \in M$ olmak üzere her sıralanmış (a,b) çiftine tamamen belirli bir $c \in M$ tekabül ettirebiliyorsa, M de bir ikili işlem tanımlanmıştır denir. Bir ikili işlem, genellikle "$\circ$" işaretiyle gösterilir ve bu işlem sonucunda (a,b) den elde edilen eleman c olduğuna göre $c = a \circ b$ yazılır [6].

Tanım 1.4 (Cebirsel yapı). İçinde en az bir tane ikili işlem tanımlanmış bir kümeye bir cebirsel yapı denir. Örneğin bir M kümesinde "$\circ$" gibi bir ikili işlem tanımlanmış ise bu cebirsel yapı $\langle M, \circ \rangle$ şeklinde gösterilir [6].

Tanım 1.5. Bir M kümesinde tanımlanmış bir "$\circ$" ikili işlemi her $a, b, c \in M$ üçlüsü için $(a \circ b) \circ c = a \circ (b \circ c)$ özelliği gerçekliyorsa bu ikili işlem bir asosyatif (birleşmeli) işlem denir [6].

Tanım 1.6. Bir M kümesinde tanımlanmış bir "$\circ$" ikili işlemi her $a, b \in M$ ikilisi için $a \circ b = b \circ a$ özelliği gerçekliyorsa bu ikili işlem bir komütatif (değişmeli) işlem denir [6].

Tanım 1.7. Bir $\langle M, \circ \rangle$ cebirsel yapısında her $a \in M$ için $e_1 \circ a = a$ ($a \circ e_2 = a$) olacak şekilde bir e_1 (e_2) elemanı varsa e_1 e (e_2 ye) $\langle M, \circ \rangle$ cebirsel yapının bir sol (sağ) nötr elemanı denir. e, $\langle M, \circ \rangle$ nun hem bir sol, hem de bir sağ nötr elemanı ise, yani her $a \in \langle M, \circ \rangle$ için $e \circ a = a \circ e = a$ ise e ye $\langle M, \circ \rangle$ nun bir nötr elemanı veya etkisiz elemanı denir [6].

Tanım 1.8. Bir $\langle M, \circ \rangle$ cebirsel yapısında bir e nötr elemanı bulunsun. Eğer $a \in \langle M, \circ \rangle$ için $a^* \circ a = e$ ($a \circ a^{**} = e$) olacak şekilde bir $a^* \in \langle M, \circ \rangle$ ($a^{**} \in \langle M, \circ \rangle$) varsa a^* a (a^{**} a) a nın $\langle M, \circ \rangle$ daki bir sol (sağ) tersi denir. Bir $b \in M$, a nın hem bir sol, hem de bir sağ tersi ise, yani $b \circ a = a \circ b = e$ ise b ye a nın $\langle M, \circ \rangle$ daki bir tersi denir [6].

Tanım 1.9. İçinde asosyatif bir ikili işlem tanımlanmış olan tek işlemli bir cebirsel yapıya bir yarı grup denir [6].

Tanım 1.10. Birimli bir yarı gruba bir monoid denir [6].

Tanım 1.11. Bir $\langle G, \circ \rangle$ yarı grubunda her a, b eleman çiftine karşılık, $a \circ x = b$ ve $y \circ a = b$ olacak şekilde en az bir $x, y \in \langle G, \circ \rangle$ çifti varsa G ye "$\circ$" işlemine göre bir grup denir [6].

Tanım 1.12. Bir yarı grup, monoid veya grup içinde tanımlanmış olan ikili işlem komütatif ise o yarı grup, monoid veya gruba sırasıyla komütatif yarı grup, komütatif monoid, komütatif grup veya abelyen yarı grup, abelyen monoid, abelyen grup (abel grubu) denir [6].

Toplama işlemine göre bir komütatif yarı grup, monoid veya gruba additif yazılmış (toplamsal) bir yarı grup, monoid veya grup denir.

Komütatif olması gerekmeyen bir çarpma işlemine göre bir yarı grup, monoid veya grup verildiği takdirde buna da mültiplikatif yazılmış (çarpımsal) bir yarı grup, monoid veya grup denir.

Şimdi yukarıda tanımlanan cebirsel yapıların gerçekledikleri aksiyomları yazalım.

Yarı grup aksiyomları aşağıdaki gibidir.

i. $\forall\, a,b \in M$ için $a \circ b \in M$,
ii. $\forall\, a,b,c \in M$ için $(a \circ b) \circ c = a \circ (b \circ c)$.

Komütatif yarı grup aksiyomları aşağıdaki gibidir.

i. $\forall\, a,b \in M$ için $a \circ b \in M$,
ii. $\forall\, a,b,c \in M$ için $(a \circ b) \circ c = a \circ (b \circ c)$,
iii. $\forall\, a,b \in M$ için $a \circ b = b \circ a$.

Monoid aksiyomları aşağıdaki gibidir.

i. $\forall\, a,b \in M$ için $a \circ b \in M$,
ii. $\forall\, a,b,c \in M$ için $(a \circ b) \circ c = a \circ (b \circ c)$,
iii. $\exists\, e \in M$ ve $\forall\, a \in M$ için $e \circ a = a \circ e = a$.

Komütatif monoid aksiyomları aşağıdaki gibidir.

i. $\forall\, a,b \in M$ için $a \circ b \in M$,
ii. $\forall\, a,b,c \in M$ için $(a \circ b) \circ c = a \circ (b \circ c)$,
iii. $\forall\, a,b \in M$ için $a \circ b = b \circ a$,
iv. $\exists\, e \in M$ ve $\forall\, a \in M$ için $e \circ a = a \circ e = a$.

Grup aksiyomları aşağıdaki gibidir.

i. $\forall\, a,b \in G$ için $a \circ b \in G$,
ii. $\forall\, a,b,c \in G$ için $(a \circ b) \circ c = a \circ (b \circ c)$,
iii. $\forall\, a,b \in G$ ve $\exists\, x,y \in G$ için $a \circ x = b$ ve $y \circ a = b$.

Bu üç aksiyoma birinci takım grup aksiyomları denir.

Komütatif grup aksiyomları aşağıdaki gibidir.

i. $\forall\, a,b \in G$ için $a \circ b \in G$,

ii. $\forall\, a,b,c \in G$ için $(a \circ b) \circ c = a \circ (b \circ c)$,

iii. $\forall\, a,b \in G$ için $a \circ b = b \circ a$,

iv. $\forall\, a,b \in G$ ve $\exists\, x \in G$ için $a \circ x = b$.

Tanım 1.13. Bir G kümesinde aşağıdaki koşullara uyan bir "$\circ$" ikili işlemi tanımlanmış ise G ye "$\circ$" işlemine göre bir grup denir.

i. $\forall\, a,b \in G$ için $a \circ b \in G$,

ii. $\forall\, a,b,c \in G$ için $(a \circ b) \circ c = a \circ (b \circ c)$,

iii. $\forall\, a \in G$ için $e \circ a = a \circ e = a$ olacak şekilde en az bir $e \in G$ vardır,

iv. $\forall\, a \in G$ ye karşılık, $a^* \circ a = a \circ a^* = e$ olacak şekilde en az bir $a^* \in G$ vardır.

Bu dört aksiyoma 2. takım grup aksiyomları denir.

Örnek 1.1. Doğal sayılar $\langle N, + \rangle$ bir komütatif yarı gruptur. $\langle N, \cdot \rangle$ ise birimi 1 olan komütatif monoiddir.

Örnek 1.2. Tam sayılar $\langle Z, + \rangle$ bir komütatif gruptur. $\langle Z, \cdot \rangle$ ise birimi 1 olan komütatif monoiddir.

Örnek 1.3. Rasyonel sayılar $\langle Q, + \rangle$ ve $\langle Q - \{0\}, \cdot \rangle$ birer komütatif gruptur.

Örnek 1.4. Reel sayılar $\langle R, + \rangle$ ve $\langle R - \{0\}, \cdot \rangle$ birer komütatif gruptur.

Tanım 1.14. İçinde iki tane ikili işlem tanımlanmış bir cebirsel yapıya iki işlemli bir cebirsel yapı denir. Verilen küme M ve içinde tanımlanmış olan işlemler "$\circ$" ve "$*$" ise söz konusu olan cebirsel yapı, $\langle M; \circ, * \rangle$ şeklinde gösterilir.

Tanım 1.15. İki işlemli bir H cebirsel yapısı, "+" işaretiyle göstereceğimiz ve toplama işlemi adını vereceğimiz birinci işleme göre bir abel grubu, "$\cdot$" işaretiyle (veya elemanları yan yana yazarak) göstereceğimiz ve çarpma adını vereceğimiz ikinci işleme göre de bir yarı grup ise ve bundan başka, çarpma işlemi toplama işlemine

göre iki yanlı distribütif ise (yani her $a,b,c \in H$ üçlüsü için $a(b+c) = a \cdot b + a \cdot c$ ve $(b+c)a = b \cdot a + c \cdot a$ ise) H ya bir halka denir.

Tanım 1.16. Bir $\langle H;+,\cdot \rangle$ halkası verildiğine göre $\langle H;+ \rangle$ grubunun 0_H nötr elemanına H halkasının sıfırı denir. Özellikle H nın "$\cdot$" işlemine göre de 1_H gibi bir nötr elemanı varsa buna H halkasının birimi adı verilir ve bu durumda H ya birimli bir halka denir.

Tanım 1.17. Bir $\langle F;+,\cdot \rangle$ halkasında $F - \{0_F\}$ alt kümesi, "$\cdot$" işlemine göre bir grup oluşturuyorsa bu halkaya bir cisim denir.

Tanım 1.18. Bir halka (cisim) içinde tanımlanmış olan çarpma işlemi komütatif ise o halkaya (cisme) bir komütatif halka (komütatif cisim) denir.

Halka aksiyomları aşağıdaki gibidir.

i. $\forall a,b \in H$ için $a+b \in H$,
ii. $\forall a,b,c \in H$ için $(a+b)+c = a+(b+c)$,
iii. $\forall a,b \in H$ için $a+b = b+a$,
iv. $\forall a,b \in H$ için $a+x = b$ olacak şekilde bir $\exists\, x \in H$ vardır,
v. $\forall a,b \in H$ için $a \cdot b \in H$,
vi. $\forall a,b,c \in H$ için $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,
vii. $\forall a,b,c \in H$ için $a \cdot (b+c) = a \cdot b + a \cdot c$, $(b+c) \cdot a = b \cdot a + c \cdot a$.

Buradaki (i-iv) aksiyomları, $\langle H,+ \rangle$ nın bir abel grubu olduğunu, v ve vi aksiyomları, $\langle H,\cdot \rangle$ nın bir yarı grup olduğunu, vii aksiyomu ise "$\cdot$" işleminin "+" ya göre iki yanlı distribütif olduğunu ifade etmektedir.

Komütatif halka aksiyomları aşağıdaki gibidir.

i. (i-vi) halka aksiyomları aynen geçerlidir,
vii. $\forall a,b \in H$ için $a \cdot b = b \cdot a$,
viii. $\forall a,b,c \in H$ için $a(b+c) = a \cdot b + a \cdot c$.

Cisim aksiyomları aşağıdaki gibidir.

i. $\forall a,b \in F$ için $a+b \in F$,

ii. $\forall\, a,b,c \in F$ için $(a+b)+c = a+(b+c)$,

iii. $\forall\, a,b \in F$ için $a+b = b+a$,

iv. $\forall\, a,b \in F$ için $a+x = b$ olacak şekilde bir $\exists\, x \in F$ vardır,

v. $\forall\, a,b \in F$ için $a \cdot b \in F$,

vi. $\forall\, a,b,c \in F$ için $(a \cdot b) \cdot c = a \cdot (b \cdot c)$,

vii. $\forall\, a,b,c \in F$ için $a \cdot (b+c) = a \cdot b + a \cdot c$, $(b+c) \cdot a = b \cdot a + c \cdot a$,

viii. $\forall\, a,b \in F - \{0_F\}$ için $a \cdot b \in F - \{0_F\}$,

ix. $\forall\, a,b \in F - \{0_F\}$ için $a \cdot x = b$, $y \cdot a = b$ olacak şekilde $\exists\, x,y \in F - \{0_F\}$ vardır.

Komütatif cisim aksiyomları aşağıdaki gibidir.

i. (i-vi) numaralı cisim aksiyomları aynen geçerlidir.

vii. $\forall\, a,b \in F$ için $a \cdot b = b \cdot a$,

viii. $\forall\, a,b,c \in F$ için $a(b+c) = a \cdot b + a \cdot c$,

ix. $\forall\, a,b \in F - \{0_F\}$ için $a,b \in F - \{0_F\}$,

x. $\forall\, a,b \in F - \{0_F\}$ için $a \cdot x = b$ olacak şekilde $\exists\, x \in F - \{0_F\}$ vardır.

Tanım 1.19. H bir halka $0_H \neq a \in H$ olsun. Eğer $ab = 0_H$ ($ba = 0_H$) olacak şekilde bir $0_H \neq b$ varsa a elemanına, bir sol sıfır-bölen (sağ sıfır-bölen) ve eğer böyle bir $0_H \neq b \in H$ yoksa a ya, sol (sağ) sıfır-bölen değildir denir. Eğer a elemanı hem sol hem de sağ sıfır bölen ise a elemanına, bir sıfır-bölen denir.Şu halde 0_H, ne sıfır bölen ne de sıfır-bölen olmayan elemandır. Eğer H halkasında sıfır bölen varsa, H ye sıfır-bölenli halka; H de sıfır-bölen yoksa H ye sıfır-bölensiz halka denir [7].

Tanım 1.20. Değişmeli, birimli ve sıfır-bölensiz bir halkaya tamlık bölgesi denir [7].

1.2. Polinom Halkaları

Tanım 1.21. H bir halka, x bir bilinmeyen ve $a_0, a_1, \cdots, a_k \in H$ olmak üzere;
$a_0 + a_1 x + \cdots + a_k x^k$

şeklindeki ifadeye, katsayıları H de olan bir polinom denir. Katsayıları H de olan polinomlar kümesi H[x] ile gösterilir [8].

Tanım 1.22. $p(x) = a_0 + a_1x + \cdots + a_kx^k$ ve $q(x) = b_0 + b_1x + \cdots + b_tx^t$, H[x] de iki polinom olsun.
$p(x) = q(x) \Leftrightarrow a_i = b_i, \quad \forall\, i \geq 0.$
Daha açık bir ifade ile polinomların eşitliği, karşılıklı katsayıların eşit olması ile tanımlanır [8].

Tanım 1.23. $p(x) = a_0 + a_1x + \cdots + a_nx^n \in H[x]$ ve $a_n \neq 0$ ise a_n e, polinomun baş katsayısı ve n e de polinomun derecesi denir. Sıfır polinomunun derecesi $-\infty$ olarak tanımlanır [8].

Tanım 1.24. $p(x) = a_0 + a_1x + \cdots + a_mx^m$, $q(x) = b_0 + b_1x + \cdots + b_nx^n$ olsun. $\forall\, i \geq 0$ için, $c_i = a_i + b_i$ olmak üzere, p ve q polinomlarının toplamı $p(x) + q(x) = c_0 + c_1x + \cdots + c_tx^t$ ile tanımlanır [8].

Tanım 1.25. $p(x) = a_0 + a_1x + \cdots + a_mx^m$, $q(x) = b_0 + b_1x + \cdots + b_nx^n$ olsun. $\forall\, i \geq 0$ için, $c_i = a_ib_0 + a_{i-1}b_1 + \cdots + a_0b_i$ olmak üzere, polinomlarının çarpımı $p(x)q(x) = c_0 + c_1x + \cdots + c_kx^k$ ile tanımlanır [8].

Önerme 1.1. H bir halka ise H[x] de bir halkadır [8].

Önerme 1.2. H bir halka olsun [8].

i. H birimli ise H[x] de birimli,
ii. H değişmeli ise H[x] de değişmeli ve
iii. H tamlık bölgesi ise H[x] de tamlık bölgesidir.

Sonuç 1.1. F bir cisim ise F[x] de bir cisimdir [8].

Sonuç 1.2. H bir tamlık bölgesi ise $f, g \in H[x]$ için, $der(fg) = der(f) + der(g)$ dir [8].

1.3. Cisim Genişlemeleri

F bir cisim olsun. F nin bir K alt kümesi F deki işlemlere göre bir cisim ise K, F nin bir alt cismi adını alır. Bu bölümde F, K nın bir cisim genişlemesi olarak adlandırılır [9].

$K \neq F$ halinde K ya, öz alt cisim denir.

K, F_p (p asal) sonlu cismin bir alt cismi ise bu durumda K, 0 ve 1 elemanlarını içermelidir. Çünkü, verilen bir cebirsel yapının cisim olabilmesi için, bu yapı en az iki elemandan (halkanın sıfırı ve birimi) oluşmalıdır [9].

Dolayısıyla K, F_p nin diğer bütün elemanlarını içerir. Çünkü K, toplama işlemine göre kapalıdır [9].

F_p hiç öz alt cisim içermez. Yani F_p nin kendisinden başka hiç alt cismi yoktur [9].

Tanım 1.26. Öz alt cisimler içermeyen bir cisim, asal cisim adını alır [9].

Bu ifade; p mertebeli (p asal) herhangi bir cismin, bir asal cisim olduğunu gösterir. Q rasyonel sayılar cismi, asal cisme verilebilecek bir başka örnektir.

Verilen bir F cisminin alt cisimlerinin boş olmayan topluluğunun bir kesişimi, yine F nin bir alt cismidir. F nin tüm alt cisimlerinin bir kesişimi ise, kesinlikle bir asal cisimdir [9].

Tanım 1.27. K, F cisminin bir alt cismi ve M, F nin herhangi bir alt kümesi olsun. Bu durumda K(M); K ve M nin her ikisini de içeren, F nin tüm alt cisimlerinin kesişimi olan cisim olarak tanımlanır ve K nın elemanlarının eklenmesiyle elde edilen bir cisim genişlemesi adını alır [9].

Sonlu $M = \{\theta_1, \cdots, \theta_n\}$ kümesi için K(M) olarak, $K(\theta_1, \cdots, \theta_n)$ yazılır. M, bir tek $\theta \in F$ elemanını içeriyorsa bu durumda $L = K(\theta)$, K nın bir basit genişlemesi olarak ifade edilir ve θ, K üzerinde L nin tanımlayıcı bir elemanı adını alır.

K(M), kesinlikle K ve M nin her ikisini de içeren F nin en küçük alt cismidir.

Tanım 1.28. K, F nin bir alt cismi ve $\theta \in F$ olsun. θ, K daki katsayılarla trivial olmayan bir polinom denklemini sağlıyorsa, yani $a_n\theta^n + a_{n-1}\theta^{n-1} + \cdots + a_1\theta + a_0 = 0 (a_i \in K)$ (hepsi birden sıfır değil) ise bu durumda θ ya, K üzerinde cebirseldir denir. L nin her elemanı K üzerinde cebirsel ise; K nın L genişlemesi, K üzerinde bir cebir veya K nın bir cebirsel genişlemesi olarak adlandırılır [9].

Teorem 1.1. q mertebeli bir cismin var olması için gerek ve yeter koşul, q nun bir asal sayının kuvveti şeklinde olmasıdır. Yani; h pozitif bir tam sayı olmak üzere, $q = p^h$ biçiminde ifade edilir [9].

q mertebeli bir cisim genellikle, q mertebeli bir Galois Cismi olarak adlandırılır ve GF(q) şeklinde gösterilir. (Tez içerisinde GF(q) ve F_q aynı anlamda kullanılacaktır.) [9].

Tanım 1.29. F, K nın bir cisim genişlemesi olsun. F (K üzerinde bir sonlu vektör uzayı olarak), sonlu boyutlu ise F ye, K nın bir sonlu genişlemesi adı verilir. K üzerinde F vektör uzayının boyutu, K üzerinde F nin derecesi olarak adlandırılır ve [F : K] ile gösterilir [9].

Yardımcı Teorem 1.1. F , q elemanlı bir K alt cismini içeren sonlu cisim olsun. Bu durumda $m = [F : K]$ olmak üzere, $|F| = q^m$ dir. |F| ile, F cisminin eleman sayısı gösterilmektedir [9].

Teorem 1.2. F, bir sonlu cisim olsun. F nin karakteristiği p asalı ve onun asal alt cismi üzerinde F nin derecesi n olduğunda, F nin tam p^n elemanı vardır.

Tanım 1.30. (Primitif Eleman) GF(q) cisminde, bir $a \neq 0$ elemanının mertebesi $q-1$ ise yani, $a^n = 1$ şeklindeki en küçük pozitif n tam sayısı $q-1$ ise a ya, bir primitif eleman denir [9].

O zaman, GF(q) nun sıfırdan farklı elemanları, a nın kuvvetleriyle elde edilir.

Örnek 1.5. GF(7) de,

$3^1 = 3$
$3^2 = 2$
$3^3 = 6$
$3^4 = 4$
$3^5 = 5$
$3^6 = 1$

dir.

Yani, $3^{q-1} = 3^{7-1} = 3^6 = 1$ olup, 3 bir primitif elemandır.

Tanım 1.31. (Primitif Polinom) İndirgenemez bir p(x) polinomu ele alınsın. p(x) in derecesi m olsun. Eğer $p(x)|x^n + 1$ şeklindeki en küçük pozitif n tam sayısı $n = 2^m - 1$ ise p(x) polinomuna, bir "primitif polinom" denir [9].

Örnek 1.6. $p(x) = x^4 + x + 1$ olsun.

$p(x)|x^{15} + 1$ dir.

Fakat $1 \leq n < 15$ için, $p(x) \not| x^n + 1$ dir.

Şu halde; $n = 15 = 2^4 - 1$, $m = 4$ olup, $p(x) = x^4 + x + 1$ polinomu, primitiftir.

Örnek 1.7. $x^4 + x^3 + x^2 + x + 1$ polinomu, GF(2) de indirgenemezdir. Fakat primitif değildir.

$m = 4, \quad 2^4 - 1 = 15$ ve $5 < 15$ için $x^4 + x^3 + x^2 + x + 1 \quad | \quad x^5 + 1$ dir.

Örnek 1.8. $x^3 + x + 1$ polinomu GF(2) üzerinde indirgenemezdir. Bu nedenle $F_2[x]/(x^3 + x^2 + 1)$, 8 mertebeli bir cisimdir. Üstelik x, bu cismin bir primitif elemanıdır.

$$F_2[x]/(x^3 + x + 1) = \{0,\ 1,\ x,\ x^2,\ x^3 = x + 1,\ x^4 = x^2 + x,\ x^5 = x^2 + x + 1,\ x^6 = x^2 + 1\}$$

dir.

Not: Verilen bir m sayısı için, m dereceli primitif polinomların sayısı, birden fazla olabilir.

Tanım 1.32. Derecesi m den daha küçük olan F[x] deki tüm polinomların kümesi, $F^{(m)}[x]$ olarak tanımlanır. F^m deki her bir sözcük, $F^{(m)}$ deki bir polinoma karşılık gelir [10].

Örnek 1.9. $h(x) = 1 + x + x^4$ polinomu ele alınsın. $GF(2^2)$ de (1011)(1010) çarpımının sonucu aşağıdaki gibi bulunur.

$$\begin{aligned}(1011)(1010) \leftrightarrow \quad & (1 + x + x^3)(x + x^3) \\ & = x + x^2 + x^3 + x^6\end{aligned}$$

$$x \equiv x + x^2 + x^3 + x^6 \pmod{(1 + x + x^4)}$$

ifadesi elde edilir.

Bu nedenle $(1011)(1010) = 0100 \leftrightarrow x$ bulunur.

Örnek 1.10. $p(x) = x^4 + x + 1$ polinomunu kullanarak, $GF(2^4)$ cismi aşağıdaki gibi kurulur.

$$p(\alpha) = \alpha^4 + \alpha + 1 = 0$$

dır. Buradan, $\alpha^4 = \alpha + 1$ eşitliği kullanılarak, $GF(2^4)$ cismi kurulabilir.

Örneğin,

$$\alpha^5 = \alpha\alpha^4 = \alpha(\alpha + 1) = \alpha^2 + \alpha$$

$$\alpha^6 = \alpha^2\alpha^4 = \alpha^2(\alpha + 1) = \alpha^3 + \alpha^2$$

tür. İşlemlere bu şekilde devam edilirse, $p(x) = x^4 + x + 1$ ile üretilen $GF(2^4)$ ün elemanları, Tablo (1.1) de verildiği gibi bulunur.

1.4. Öklid Algoritması ve Çarpımsal Ters Bulma

Eğer a ve b pozitif tamsayılar ve $a > b$ ise $ebob(a, b) = ebob(b, a \bmod b)$ dir.

Algoritma 1.1 (Öklid Algoritması). İki pozitif tam sayının en büyük ortak bölenini bulmak için kullanılır [11].

GİRİŞ: a ve b ($a \geq b$) pozitif tamsayılar.

ÇIKIŞ: a ve b tam sayılarının en büyük ortak böleni.

1. $b \neq 0$ olduğu sürece alt işlemleri gerçekleştir.
   1.1. $r \leftarrow a \bmod b$
   1.2. $a \leftarrow b$
   1.3. $b \leftarrow r$
2. a tamsayısını döndür.

Tablo 1.1. $p(x) = x^4 + x + 1$ ile üretilen $GF(2^4)$ ün elemanları.

Sıralı dörtlü olarak	Polinom olarak	α nın kuvveti olarak
0000	0	-
0001	1	$\alpha^0 = 1$
0010	α	α
0100	α^2	α^2
1000	α^3	α^3
0011	$\alpha + 1$	α^4
0110	$\alpha^2 + \alpha$	α^5
1100	$\alpha^3 + \alpha^2$	α^6
1011	$\alpha^3 + \alpha + 1$	α^7
0101	$\alpha^2 + 1$	α^8
1010	$\alpha^3 + \alpha$	α^9
0111	$\alpha^2 + \alpha + 1$	α^{10}
1110	$\alpha^3 + \alpha^2 + \alpha$	α^{11}
1111	$\alpha^3 + \alpha^2 + \alpha + 1$	α^{12}
1101	$\alpha^3 + \alpha^2 + 1$	α^{13}
1001	$\alpha^3 + 1$	α^{14}

Örnek 1.11. 4864 ve 3458 sayıları için en büyük ortak böleni aşağıdaki gibi bulunur.

$$
\begin{aligned}
4864 &= 1 \cdot 3458 + 1406 \\
3458 &= 2 \cdot 1406 + 646 \\
1406 &= 2 \cdot 646 + 114 \\
646 &= 5 \cdot 114 + 76 \\
114 &= 1 \cdot 76 + 38 \\
76 &= 2 \cdot 38 + 0
\end{aligned}
$$

Sıfırdan farklı son kalan sayı 38, bu sayıların en büyük ortak bölenidir.

Algoritma 1.2 (Genişletilmiş Öklid Algoritması). Genişletilmiş Öklid Algoritması, en büyük ortak bölen d tam sayısının yanında $ax + by = d$ eşitliğindeki x ve y tamsayılarının bulunması için kullanılır [11].

GİRİŞ: a ve b ($a \geq b$) pozitif tamsayılar.

ÇIKIŞ: $d = ebob(a,b)$ ve $ax + by = d$ eşitliğini sağlayan x ve y tamsayıları.

1. Eğer $b = 0$ ise $d \leftarrow a$, $x \leftarrow 1$ ve $y \leftarrow 0$ ve çıkış.
2. $x_2 \leftarrow 1$, $x_1 \leftarrow 0$, $y_2 \leftarrow 0$, $y_1 \leftarrow 1$,
3. $b \neq 0$ olduğu sürece alt işlemleri gerçekleştir.
   3.1. $q \leftarrow \lfloor a/b \rfloor$, $r \leftarrow a - qb$, $x \leftarrow x_2 - qx_1$, $y \leftarrow y_2 - qy_1$, $a \leftarrow b$,
   3.2. $b \leftarrow r$, $x_2 \leftarrow x_1$, $x_1 \leftarrow x$, $y_2 \leftarrow y_1$, $y_1 \leftarrow y$,
4. $d \leftarrow a$, $x \leftarrow x_2$, $y \leftarrow y_2$ ve sonuçları döndür.

Algoritma 1.3. n modülüne göre çarpımsal ters bulma.

GİRİŞ: $a \in Z_{n^*}$

ÇIKIŞ: Eğer var ise $a^{-1} \bmod n$

1. Genişletilmiş Öklid Algoritması kullanılarak $d = ebob(a,b)$ bulunur ve $ax + by = d$ olacak şekilde x ve y değerleri bulunur [11].
2. Eğer $d \geq 1$ ise $a^{-1} \bmod n$ yoktur. Diğer durumda y değeri döndürülür.

Örnek 1.12. GF(37) cisminde 16 nın çarpımsal tersi aşağıdaki gibi bulunur.

Başlangıç;

$$a = 37, b = 16, x_2 = 1, x_1 = 0, y_2 = 0, y_1 = 1$$

1. İterasyon;

$$q = \lfloor a/b \rfloor = \lfloor 37/16 \rfloor = 2$$
$$r = a - q \cdot b = 37 - 2 \cdot 16 = 5$$
$$x = x_2 - q \cdot x_1 = 1 - 2 \cdot 0 = 1$$
$$y = y_2 - q \cdot y_1 = 0 - 2 \cdot 1 = -2$$
$$a = b = 16$$
$$b = r = 5$$
$$x_2 = x_1 = 0$$
$$x_1 = x = 1$$

$y_2 = y_1 = 1$

$y_1 = y = -2$

2. İterasyon;

$q = \lfloor a/b \rfloor = \lfloor 16/5 \rfloor = 3$

$r = a - q \cdot b = 16 - 3 \cdot 5 = 1$

$x = x_2 - q \cdot x_1 = 0 - 3 \cdot 1 = -3$

$y = y_2 - q \cdot y_1 = 1 - 3 \cdot (-2) = 5$

$a = b = 5$

$b = r = 1$

$x_2 = x_1 = 1$

$x_1 = x = -3$

$y_2 = y_1 = -2$

$y_1 = y = 7$

3. İterasyon;

$q = \lfloor a/b \rfloor = \lfloor 5/1 \rfloor = 5$

$r = a - q \cdot b = 5 - 5 \cdot 1 = 0$

$x = x_2 - q \cdot x_1 = 1 - 5 \cdot (-3) = 16$

$y = y_2 - q \cdot y_1 = -2 - 5 \cdot (7) = -37$

$a = b = 1$

$b = r = 0$

$x_2 = x_1 = -3$

$x_1 = x = 16$

$y_2 = y_1 = 7$

$y_1 = y = -37$

$b = 0$ olduğu için döngü sonlandırılacaktır. $d = ebob(a, b) = a = 1$, $x = x_2 = -3$ ve $y = y_2 = 7$ dir.

$ax + by = d$ den $37 \cdot (-3) + 16 \cdot 7 = 1$ bulunur. İşlemler yapıldığında eşitliğin doğru olduğu görülür.

Eğer işlemler $\pmod{37}$ ye göre yapılsaydı $37 \equiv 0 \pmod{37}$ olduğu için $16 \cdot 7 = 1$ bulunacaktır. Buradan $16^{-1} = 7$ olduğu görülür.

Tablo 1.2. 37 ve 16 için genişletilmiş öklid algoritması adımları.

İterasyon	q	r	x	y	a	b	x_2	x_1	y_2	y_1
Başlangıç	–	–	–	–	37	16	1	0	0	1
1	2	5	1	–2	16	5	0	1	1	–2
2	3	1	–3	5	5	1	1	–3	–2	7
3	5	0	16	–37	1	0	–3	16	7	–37

Algoritma 1.4. ($Z_n[x]$ için Genişletilmiş Öklid Algoritması) Katsayıları Z_n in elemanlarından seçilen polinomlar için genişletilmiş öklid algoritması [11].

GİRİŞ: $g(x), h(x) \in Z_n[x]$ iki polinom.

ÇIKIŞ: $d(x) = \text{ebob}(g(x), h(x))$ ve $g(x)s(x) + h(x)t(x) = d(x)$ eşitliğini sağlayan $s(x), t(x) \in Z_n[x]$.

1. Eğer $h(x) = 0$ ise $d(x) \leftarrow g(x)$, $s(x) \leftarrow 1$ ve $t(x) \leftarrow 0$ ve çıkış.
2. $s_2(x) \leftarrow 1$, $s_1(x) \leftarrow 0$, $t_2(x) \leftarrow 0$, $t_1(x) \leftarrow 1$,
3. $h(x) \neq 0$ olduğu sürece alt işlemleri gerçekleştir.
   - 3.1. $q(x) \leftarrow \lfloor g(x)/h(x) \rfloor$,
   - 3.2. $r(x) \leftarrow g(x) - q(x)h(x)$,
   - 3.3. $s(x) \leftarrow s_2(x) - q(x)s_1(x)$,
   - 3.3. $t(x) \leftarrow t_2(x) - q(x)t_1(x)$,
   - 3.5. $g(x) \leftarrow h(x)$,
   - 3.6. $h(x) \leftarrow r(x)$,
   - 3.7. $s_2(x) \leftarrow s_1(x)$,
   - 3.8. $s_1(x) \leftarrow s(x)$,
   - 3.9. $t_2(x) \leftarrow t_1(x)$,
   - 3.10. $t_1(x) \leftarrow t_2(x)$,
4. $d(x) \leftarrow g(x)$, $s(x) \leftarrow s_2(x)$, $t(x) \leftarrow t_2(x)$ ve sonuçları döndür.

Algoritma 1.5. F_{p^m} cisminde çarpımsal ters bulma [11].

GİRİŞ: $g(x) \in F_{p^m}$ ($f(x) \in Z_p[x]$ fonksiyonu, derecesi m olan ve Z_p üzerinde indirgenemez bir polinomdur ve F_{p^m} cisminin elemanları $Z_p[x]/f(x)$ şeklinde gösterilebilir.)

ÇIKIŞ: Eğer var ise $(g(x))^{-1} \in F_{p^m}$

1. Algoritma (1.4) teki Genişletilmiş Öklid Algoritması kullanılarak
   $g(x)s(x) + f(x)t(x) = 1$
   olacak şekilde s(x) ve t(x) polinomları bulunur.
2. Sonuç olarak s(x) polinomu döndürülür.

Örnek 1.13. $x^3 + x^2 + 1 \in Z_2[x]$ ve $x^2 + 1 \in Z_2[x]$ polinomları için d(x), s(x) ve t(x) polinomları aşağıdaki gibi bulunur.

Başlangıç;

$g(x) = x^3 + x^2 + 1,$
$h(x) = x^2 + 1,\ s_2(x) \leftarrow 1,$
$s_1(x) \leftarrow 0,\ t_2(x) \leftarrow 0,$
$t_1(x) \leftarrow 1$

1. İterasyon;

$q(x) \leftarrow \lfloor g(x)/h(x) \rfloor = \lfloor (x^3 + x^2 + 1)/(x^2 + 1)) \rfloor = x + 1$
$r(x) \leftarrow g(x) - q(x)h(x) = (x^3 + x^2 + 1) - (x^2 + 1) \cdot (x + 1) = x$
$s(x) \leftarrow s_2(x) - q(x)s_1(x) = 1 - (x + 1) \cdot 0 = 1$
$t(x) \leftarrow t_2(x) - q(x)t_1(x) = 0 - (x + 1) \cdot 1 = x + 1$
$g(x) \leftarrow h(x) = x^2 + 1$
$h(x) \leftarrow r(x) = x$
$s_2(x) \leftarrow s_1(x) = 0$
$s_1(x) \leftarrow s(x) = 1$
$t_2(x) \leftarrow t_1(x) = 1$
$t_1(x) \leftarrow t(x) = x + 1$

2. İterasyon;

$q(x) \leftarrow \lfloor g(x)/h(x) \rfloor = \lfloor (x^2+1)/(x)) \rfloor = x$

$r(x) \leftarrow g(x) - q(x)h(x) = (x^2+1) - (x) \cdot (x) = 1$

$s(x) \leftarrow s_2(x) - q(x)s_1(x) = 0 - (x) \cdot 1 = x$

$t(x) \leftarrow t_2(x) - q(x)t_1(x) = 1 - (x) \cdot (x+1) = x^2 + x + 1$

$g(x) \leftarrow h(x) = x$

$h(x) \leftarrow r(x) = 1$

$s_2(x) \leftarrow s_1(x) = 1$

$s_1(x) \leftarrow s(x) = x$

$t_2(x) \leftarrow t_1(x) = x + 1$

$t_1(x) \leftarrow t(x) = x^2 + x + 1$

3. İterasyon;

$q(x) \leftarrow \lfloor g(x)/h(x) \rfloor = \lfloor (x)/(1)) \rfloor = x$

$r(x) \leftarrow g(x) - q(x)h(x) = (x) - (x) \cdot (1) = 0$

$s(x) \leftarrow s_2(x) - q(x)s_1(x) = 1 - (x) \cdot (x) = x^2 + 1$

$t(x) \leftarrow t_2(x) - q(x)t_1(x) = (x+1) - (x) \cdot (x^2 + x + 1) = x^3 + x^2 + 1$

$g(x) \leftarrow h(x) = 1$

$h(x) \leftarrow r(x) = 0$

$s_2(x) \leftarrow s_1(x) = x$

$s_1(x) \leftarrow s(x) = x^2 + 1$

$t_2(x) \leftarrow t_1(x) = x^2 + x + 1$

$t_1(x) \leftarrow t(x) = x^3 + x^2 + 1$ $h(x) = 0$ olduğu için döngü sonlandırılacaktır. $d(x) = g(x) = 1$, $s(x) = s_2(x) = x$ ve $t(x) = t_2(x) = (x^2 + x + 1)$ bulunur. $g(x)s(x) + h(x)t(x) = d(x)$

$(x^3 + x^2 + 1)(x) + (x^2 + 1)(x^2 + x + 1) = 1$

$(x^4 + x^3 + x) + (x^4 + x^3 + x + 1) = 1$

eşitliğinin sağlandığı görülür. Ayrıca $d(x) = 1$ olduğu için $g(x)$ ve $h(x)$ polinomları aralarında asaldır.

$(h(x))^{-1} = x^2 + x + 1 \pmod{g(x)}$

$(x^2 + 1)^{-1} = x^2 + x + 1 \pmod{(x^3 + x^2 + 1)}$

2. LİNEER KODLAR

2.1. Giriş

Kodlama Teorisi, veri aktarım ve depolama süreçlerinde kanaldan kaynaklanan hataların tesbiti ve düzeltilmesi amacı ile ortaya çıkmıştır. Hata düzelten kodlarda temel olarak verinin kodlanması, kodlanan verinin kontrolü ve düzeltilmesi şeklinde üç süreç vardır.

Kodlama algoritmaları, blok kodlar ve konvolüsyonel kodlar olmak üzere iki gruba ayrılmaktadır. Bu çalışma ile ilgisi olmaması nedeniyle konvolüsyonel kodlara değinilmeyecektir.

Blok kodlar adından da anlaşıldığı üzere gibi verinin bloklara ayrıldığı ve işlemlerin bu bloklar üzerinde yapıldığı bir kodlama biçimidir.

Bütün kodsözcükleri aynı boyutta olan bir koda blok kod denir. Kod denilince genel olarak blok kod anlaşılır.

Tanım 2.1. (Hamming uzaklığı) x ve y vektörleri, $(F_q)^n$ in herhangi iki elemanı olsun. Bu iki vektörün Hamming uzaklığı, farklı konumlarının sayısıdır ve ”d(x, y)” ile gösterilir [12].

Hamming uzaklığı aşağıdaki koşulları sağlar ve bu nedenle bir metriktir.

1. $d(x,y) = 0 \iff x = y$,
2. Her $x, y \in (F_q)^n$ için $d(x,y) = d(y,x)$,
3. Her $x, y, z \in (GF(q))^n$ için $d(x,y) \leq d(x,z) + d(y,z)$.

Tanım 2.2. (Minimum uzaklık) Bir C kodunun farklı kodsözcükleri arasındaki uzaklıkların en küçüğü olarak tanımlanır ve d(C) ile gösterilir. Kodlar için önemli bir parameteredir. Kodun hata düzeltme yeteneği bu parametreye bağlıdır [12]. $d(C) = \min\{d(x,y) \mid x, \ y \in C, x \neq y\}$.

Bir kod uzunluk, kodsözcüğü sayısı ve minimum mesafe ile tanımlanabilir. n uzunluklu, M kodsözcüğüne sahip ve minimum mesafesi d olan bir kod (n, M, d)-kod olarak adlandırılır [12].

2.2. Lineer Kodlar

Tanım 2.3. Bir V kümesi üzerinde tanımlı $\oplus$ ve $\odot$ işlemlerine göre aşağıdaki özelliklerin hepsi sağlanıyorsa V ye bir reel vektör uzayı denir [13].

i. Her $u, v \in V$ için $u \oplus v \in V$ (Kapalılık özelliği)
ii. Her $u, v \in V$ için $u \oplus v = v \oplus u$ (Değişme özelliği)
iii. Her $u, v, z \in V$ için $u \oplus (v \oplus z) = (u \oplus v) \oplus z$ (Birleşme özelliği)
iv. Her $u \in V$ için $u \oplus 0 = 0 \oplus u = u$ olacak şekilde V de bir 0 elemanı vardır. (Toplamsal etkisiz eleman)
v. Her $u \in V$ için $u \oplus (-u) = (-u) \oplus u = 0$ olacak şekilde bir –u elemanı vardır. (Toplamsal ters ya da toplamsal invers)
vi. Her $u \in V$ ve her $c \in \mathbb{R}$ için $c \odot u \in V$ dir. (Skalerle çarpımın kapalılığı)
vii. Her $u, v \in V$ ve $c \in \mathbb{R}$ için $c \odot (u \oplus v) = (c \odot u) \oplus (c \odot v)$ dir.
viii. Her $u \in V$ ve her $c, d \in \mathbb{R}$ için $(c + d) \odot u = (c \odot u) \oplus (d \odot u)$ dur.
ix. Her $u \in V$ ve $c, d \in \mathbb{R}$ için $c \odot (d \odot u) = (c \cdot d) \odot u$ dur.
x. Her $u \in V$ için $1 \odot u = u$ dur.

Vektör uzayı V nin elemanlarına vektör, $\mathbb{R}$'nin elemanlarına skaler denir. $\oplus$ işlemine vektörel toplam, $\odot$ işlemine de skaler çarpım adı verilir. Yukarıdaki özellikler vektör uzayı aksiyomları olarak da adlandırılır [13].

Lineer kodlar incelenirken alfabe olarak F_q cismi alınır. (Burada q, bir asal sayının kuvveti şeklindedir.) $(F_q)^n$, F_q cismi üzerinde bir vektör uzayıdır.

GF(q) üzerinde bir lineer kod, $(F_q)^n$ vektör uzayının bir alt uzayıdır. Bu durumda $(F_q)^n$ vektör uzayının bir C alt kümesi ancak ve ancak,

1. Her $u, v \in C$ için $u + v \in C$
2. Her $u \in C$, $r \in F_q$ için $ru \in C$

koşullarını gerçekliyorsa, lineer bir koddur [12].

Tanım 2.4. C, $(F_q)^n$ vektör uzayının bir alt uzayı ise bu lineer C koduna, bir $[n,k]$-kod denir. Eğer C nin d minimum mesafesini belirtmek gerekirse bu kod, bir $[n,k,d]$-kod olarak adlandırılır [12].

Not: Lineer kodlar aşağıdaki iki özelliğe sahiptir [12].

1. q-lu bir $[n,k,d]$-kod aynı zamanda bir (n,q^k,d)-koddur. Fakat her (n,q^k,d)-kod bir $[n,k,d]$-kod değildir.
2. Her lineer kod, 0 vektörünü içerir.

Tanım 2.5 (Hamming Ağırlığı). $(F_q)^n$ deki bir x vektörünün sıfırdan farklı sembollerinin sayısına, x in Hamming ağırlığı denir ve wt(x) ile gösterilir. x in ağırlığı denilince, Hamming ağırlığı anlaşılacaktır [12].

Tanım 2.6. Satırları, lineer bir $[n,k]$ kodun bir tabanını oluşturan $k \times n$ matrise, kodun bir üreteç matrisi denir [12].

2.2.1. Lineer bir kod ile kodlama

C, üreteç matrisi G olmak üzere, F_q üzerinde bir $[n,k]$-kod olsun. C, q^k farklı mesajdan herhangi birini iletmek için kullanılabilir. Bu mesajlar, $(F_q)^k$ vektör uzayının q^k tane sıralı k-lıları ile tanımlanır. Bir $u = u_1u_2\ldots u_k$ mesaj vektörü, G nin satırları $r_1, r_2, \ldots, r_k$ olmak üzere,

$$uG = \sum_{i=1}^{k} u_i r_i$$

şeklinde kodlanır. Bu durumda uG, C nin bir kodsözcüğü olur. Kodlama fonksiyonu,

$$\varphi \rightarrow uG$$

dir [12].

2.2.2. Dual kod ve eşlik-denetim (parity-check) matrisi

$(F_q)^n$ de $u = (u_1, u_2, \ldots, u_n)$ ve $v = (v_1, v_2, \ldots, v_n)$ vektörlerinin iç çarpımı,

$< u, v >= u_1 v_1 + u_2 v_2 + \ldots + u_n v_n$

şeklinde tanımlanan skalerdir. Yani F_q nun bir elemanıdır.

Tanım 2.7. C, lineer bir [n,k]-kod olmak üzere, C nin her bir kodsözcüğüne ortogonal olan $(F_q)^n$ in vektörlerinin kümesine, C nin dual kodu denir ve $C^{\perp}$ ile gösterilir. Bir kodsözcüğünün $C^{\perp}$ ne ait olması için gerek ve yeter koşul v nin, G nin üreteç matrisinin her satırına ortogonal olmasıdır. Yani,

$v \in C^{\perp} \iff vG^T = 0$

dır [12]. (Burada G^T ile G nin transpozesi gösterilmektedir.)

Teorem 2.1. C, F_q üzerinde lineer bir [n,k]-kod olsun. Bu durumda, C nin $C^{\perp}$ dual kodu, lineer bir [n, n−k]-koddur [12].

Teorem 2.2. Herhangi bir [n,k]-kod için $(C^{\perp})^{\perp} = C$ dir [12].

Tanım 2.8. C, bir [n,k]-kod olmak üzere, $C^{\perp}$ nin bir H üreteç matrisine, C nin bir eşlik-denetim (parity-check) matrisi denir. Bu durumda H, bir $(n-k) \times n$ matristir ve $GH^T = 0$ eşitliğini gerçekler. H, C nin eşlik denetim matrisi ise,

$C = \{x \in (F_q)^n \mid xH^T = 0\}$

dır [12].

Bu yolla lineer bir kod, bir eşlik-denetim matrisi ile tamamen belirlenebilir [12].

Teorem 2.3. C, bir [n,k]-kod olmak üzere, C nin standart formdaki üreteç matrisi $G = [I_k|A]$ ise, C için bir eşlik-denetim matrisi $H = [-A^T \mid I_{n-k}]$ dir [12].

3. SIR PAYLAŞIM ŞEMALARI

3.1. Giriş

Sır paylaşım şemalarından, 1979'da Blakley [1] ve Shamir [2] söz etmektedir. Daha sonra bu konuda pek çok yeni yöntem önerilmiştir. Shamir'in sır paylaşım şeması ve Reed-Solomon Kodları arasındaki ilişki, 1981'de McEliece ve Sarwate [14] tarafından belirtilmiştir.

Massey [15], [16], sır paylaşımı için lineer kodlardan faydalanarak, ilgili kodun dualinin minimal kodsözcükleri ve erişim yapısı arasındaki ilişkiyi belirtmiştir.

Belli kodlar için minimal kodsözcükleri araştırılarak, bu kodların dual kodları üzerine kurulan sır paylaşım şemalarının erişim yapıları karakterize edilmiştir.

Sır paylaşımı, gizli bir bilgiyi (sır) bir yönetici tarafından, katılımcı kümesi olarak adlandırılan ve P ile gösterilen belli sayıdaki katılımcıya, sadece belli alt kümelerin sırrı bulabileceği şekilde dağıtılması işlemidir.

Sırra erişebilen alt kümelerin kümesine erişim yapısı denir ve Γ ile gösterilir. Eğer bir W alt kümesi, Γ erişim yapısının elemanı ise sırra ulaşılabilir. Aksi takdirde sırra erişilemez [17].

Tanım 3.1 (Monotonluk). Eğer P katılımcı kümesinin herhangi bir yetkili W alt kümesinin bütün üst kümeleri sırra ulaşabiliyorsa, bu erişim yapısı monoton olarak adlandırılır [17]. Burada yetkili sözcüğü ile, elemanları bir araya gelerek sırra erişebilen kümeden söz edilmektedir.
$W \in \Gamma$, $W \subset U \subseteq P \Rightarrow U \in \Gamma$.

Tanım 3.2 (Minimal Erişim Yapısı). Monoton bir erişim yapısı olan Γ nın bir elemanı olan W kümesinin bütün üst kümeleri de erişim yapısının elemanıdır. Erişim yapısını tanımlarken W kümesinin bütün üst kümelerini yazmak yerine sadece W kümesini

yazmak yeterlidir. Bu şekilde minimal kümelerin bir araya gelmesiyle oluşan kümeye minimal erişim yapısı denir [17].

$$\Gamma^{-} = \{W \in \Gamma \ : \ \forall \ W' \subset W, \ W' \notin \Gamma\} \ .$$

Tanım 3.3 (İdeallik). Katılımcılara verilen sır parçalarının boyutu, sırrın boyutuna eşit veya sırrın boyutundan küçük ise sır paylaşım şemasına ideal sır paylaşım şeması denir [17].

Tanım 3.4 (Mükemmellik). Herhangi bir sır paylaşım şeması aşağıdaki koşulları sağladığı takdirde, mükemmel sır paylaşım şeması olarak adlandırılır [17].

1. Bütün yetkili alt kümeler sırra ulaşabilmeli.
2. Bütün yetkisiz alt kümeler sır hakkında hiçbir bilgi elde edememeli.

İlk durum açıktır. İkinci durumda yetkisiz bir W' alt kümesinin katılımcıları sır parçalarını bir araya getirdiklerinde elde edecekleri bilgi, sır parçasını bir araya getirmeden önce sahip oldukları bilgi ile aynı olmalıdır.

Tanım 3.5 (Eşik Erişim Yapısı). Bu yapıda önemli olan, sırra ulaşmak isteyen alt kümenin boyutudur. Eğer alt kümenin boyutu belli bir eşik değere eşit veya üstünde ise sırra ulaşabilir, eğer altında ise ulaşması imkansızdır. Bir (k, n)-eşik erişim yapısı, sır paylaşım şemasında katılımcı kümesinin boyutunun n olacağını ve k veya daha çok elemanlı alt kümelerin sırra ulaşabileceğini ifade eder.

$$\Gamma = \{W \subset P \ : \ |W| \geq k\}$$

Sır paylaşım şemaları ile ilgili ilk çalışmalar eşik erişim yapısı üzerine kurulmuştur. Blakley [1] ve Shamir'in [2] çalışmaları bu erişim yapısı ile ilgilidir.

3.2. Blakley'in Sır Paylaşım Şeması

Blakley'in sır paylaşım şeması, sır paylaşım problemini çözmek için hiperdüzlem geometrisini kullanır. Sır, k-boyutlu uzayda bir nokta ve n tane parça, bu noktadan geçen afin hiperdüzlemlerdir.

Koordinatları bir F cisminde olan k-boyutlu uzayda bir afin düzlem, bir lineer denklem ile aşağıdaki şekilde tanımlanabilir.

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = b$$

Kesişim noktası, bu hiperdüzlemlerin herhangi bir k noktasının kesişimi bulunarak elde edilir. Sır, kesişim noktalarının herhangi bir koordinatı veya koordinatların herhangi bir fonksiyonu olabilir. Buradaki yapıda sır, kesişim noktasının ilk koordinatı olarak alınmaktadır.

Blakley'in bir (k, n)-sır paylaşım şemasında dağıtıcı, ilk elemanı sırra eşit olan ve diğer elemanları rastgele seçilerek oluşturulan k uzunluklu bir $X = (x_1, x_2, \ldots, x_k)$ vektörü seçer [17].

Her katılımcı için $1 \times k$ boyutunda bir $A_u = (a_{u_1}, a_{u_2}, \ldots, a_{u_k})$ vektörü rastgele seçilir. A_u vektörleri herkes tarafından bilinir [17].

$$y_u = A_u X^T = \sum_{i=0}^{k} a_{u_i} x_i$$

işlemi ile elde edilen skaler değer, u katılımcısına sır parçası olarak verilir. (Burada X^T ile X-in transpozesi belirtilmektedir.)

$u_i \in W$ katılımcısının parçalarını kullanarak aşağıdaki lineer denklem sistemi oluşturulur.

$$\begin{bmatrix} A_{u_1} \\ A_{u_2} \\ \vdots \\ A_{u_k} \end{bmatrix}_{k \times k} \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_k \end{bmatrix}_{k \times 1} = \begin{bmatrix} y_1 \\ y_2 \\ \vdots \\ y_k \end{bmatrix}_{k \times 1}$$

Bu sistem kısaca aşağıdaki gibi yazılabilir.

$$M_W X^T = Y_W^T$$

M_W, $k \times k$ boyutlu bir matristir ve bu matrisin elemanları, katılımcıların A_u vektörlerinden ibarettir. Y_W, $1 \times k$ uzunluğunda sır parçalarından oluşturulan bir vektördür [17]. Lineer denklem sistemi çözülerek, sırra ulaşılabilir.

W', eleman sayısı k' olan yetkisiz bir alt küme olsun ($k' < k$). W' alt kümesi için M_W matrisinin satır sayısı, sütün sayısından küçük olacaktır. Bu nedenle sır bulunamayacaktır [17].

Sır ve sır parçaları aynı kümenin elemanları olduğu için sır paylaşım şeması idealdir [17].

M_W nin non-singüler olma ihtimali oldukça yüksektir. Dolayısı ile yetkili alt kümeler çok yüksek bir olasılıkla sırra erişebilecektir ve alt kümeler sır hakkında hiçbir bilgi elde edemeyecektir. Buna karşın W alt kümesi için M_W nin singüler olabileceği durumlar da söz konusudur. Bu durumda W alt kümesi sırrı bulamaz. Bu nedenle Blakley'in sır paylaşım şeması her zaman mükemmel değildir [17].

Örnek 3.1. F_7 üzerinde tanımlanan ve sırrı 6 olan bir $(3,5)$-Blakley şeması aşağıdaki gibi kurulabilir. (F_7 üzerinde çalışıldığından, tüm cebirsel işlemler $\pmod 7$ ye göre yapılacaktır.)

Sır paylaşım şeması oluşturulurken ilk bileşeni sırra eşit olan 3 uzunluklu bir vektör seçilir. Bu vektörün diğer bileşenleri rastgele seçilir.

$X = (6,\ 3,\ 4)$

Katılımcıların vektörleri aşağıdaki gibi olabilir. Bu vektörler herkes tarafından bilinir.

$A_{u_1} = (0,\ 2,\ 2)$

$A_{u_2} = (1,\ 3,\ 3)$

$A_{u_3} = (1,\ 5,\ 5)$

$A_{u_4} = (0,\ 3,\ 2)$

$A_{u_5} = (5,\ 2,\ 5)$

Burada A_{u_i}, u_i $(1 \leq i \leq n)$ katılımcısına verilecek olan sır parçasını üretmek için kullanılan vektördür. Sır parçaları aşağıdaki gibi hesaplanır.

$$y_{u_1} = (0, \quad 2, \quad 2)(6, \quad 3, \quad 4)^T = 0$$
$$y_{u_2} = (1, \quad 3, \quad 3)(6, \quad 3, \quad 4)^T = 6$$
$$y_{u_3} = (1, \quad 5, \quad 5)(6, \quad 3, \quad 4)^T = 6$$
$$y_{u_4} = (0, \quad 3, \quad 2)(6, \quad 3, \quad 4)^T = 3$$
$$y_{u_5} = (5, \quad 2, \quad 5)(6, \quad 3, \quad 4)^T = 0$$

2, 4, 5 numaralı katılımcılar bir araya gelerek oluşturulan $W = \{2,4,5\}$ alt kümesi için sırra aşağıdaki gibi erişilir.

$$\begin{bmatrix} 1 & 3 & 3 \\ 0 & 3 & 2 \\ 5 & 2 & 5 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 6 \\ 3 \\ 0 \end{bmatrix}$$

Lineer denklem sistemi çözülürse $x_1 = 6, x_2 = 3, x_3 = 4$ bulunur. Buradan sır, 6 olarak bulunur.

Örnek 3.2. F_7 üzerinde tanımlanan ve sırrı 6 olan bir $(4,6)$-Blakley şeması aşağıdaki gibi kurulabilir.

Sır paylaşım şemasının oluşturulması.

$$X = (6, \quad 0, \quad 0, \quad 6)$$

Katılımcıların vektörleri aşağıdaki gibi olabilir. Bu vektörler herkes tarafından bilinir.

$$A_{u_1} = (1, \quad 4, \quad 2, \quad 0)$$
$$A_{u_2} = (0, \quad 1, \quad 5, \quad 5)$$
$$A_{u_3} = (1, \quad 3, \quad 1, \quad 1)$$
$$A_{u_4} = (2, \quad 1, \quad 6, \quad 0)$$
$$A_{u_5} = (6, \quad 0, \quad 4, \quad 0)$$
$$A_{u_6} = (2, \quad 3, \quad 4, \quad 4)$$

Sır parçaları aşağıdaki gibi hesaplanır.

$$y_{u_1} = (1,\ 4,\ 2,\ 0)(6,\ 0,\ 0,\ 6)^T = 6$$
$$y_{u_2} = (0,\ 1,\ 5,\ 5)(6,\ 0,\ 0,\ 6)^T = 2$$
$$y_{u_3} = (1,\ 3,\ 1,\ 1)(6,\ 0,\ 0,\ 6)^T = 5$$
$$y_{u_4} = (2,\ 1,\ 6,\ 0)(6,\ 0,\ 0,\ 6)^T = 5$$
$$y_{u_5} = (6,\ 0,\ 4,\ 0)(6,\ 0,\ 0,\ 6)^T = 1$$
$$y_{u_6} = (2,\ 3,\ 4,\ 4)(6,\ 0,\ 0,\ 6)^T = 1$$

1, 4, 5 numaralı katılımcılar bir araya gelerek oluşan $W = \{1,4,5\}$ alt kümesi için sır aşağıdaki gibi bulunur.

$$\begin{bmatrix} 1 & 4 & 2 & 0 \\ 2 & 1 & 6 & 0 \\ 6 & 0 & 4 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \begin{bmatrix} 6 \\ 5 \\ 1 \end{bmatrix}$$

Katsayı matrisinin indirgenmiş hali aşağıdaki gibidir.

$$\left[\begin{array}{cccc|c} 1 & 4 & 2 & 0 & 6 \\ 0 & 1 & 5 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{array}\right]$$

Lineer denklem sistemi çözüldüğünde sır $x_1 = 6$ olarak bulunur. Görüldüğü üzere sır paylaşım şemasının eşik değeri 4 olmasına rağmen sır 3 katılımcı ile bulunabilmiştir. Bu durum Blakley'in şemasının her zaman mükemmel olmamasından kaynaklanmaktadır.

3.3. Shamir'in Sır Paylaşım Şeması

Yönetici, sabit terimi sırra eşit ve derecesi $k-1$ olan rastgele bir $f(x) = \sum_{i=0}^{k-1} a_i x^i \in F_q[x]$ polinomu seçer. Her $u \in P$ katılımcısı için farklı bir $x_u \in F_q$ değeri seçer ve u katılımcısı için sır parçasını $y_u = f(x_u)$ işlemini yaparak bulur. x_u değeri kimlik olarak adlandırılır ve x_u herkes tarafından bilinir [17].

Bu şemada her katılımcı $k-1$ dereceli polinom üzerinde bir noktaya karşılık gelir. k katılımcılı $W = (u_1, u_2, \ldots, u_k)$ alt kümesi kullanılarak Lagrange Interpolasyonu ile f(x) polinomu tekrar bulunabilir. Böylece sırra erişilmiş olur [17].

Not: Shamir'in şeması, Blakley'in şemasının özel bir durumudur. k katılımcısı olan W koalisyonu için lineer denklem sistemi aşağıdaki gibidir [17].

$$\begin{bmatrix} 1 & x_{u_1} & x_{u_1}^2 & \ldots & x_{u_1}^{k-1} \\ 1 & x_{u_2} & x_{u_2}^2 & \ldots & x_{u_2}^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_{u_k} & x_{u_k}^2 & \ldots & x_{u_k}^{k-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{k-1} \end{bmatrix} = \begin{bmatrix} y_{u_i} \\ y_{u_i} \\ \vdots \\ y_{u_{k-1}} \end{bmatrix}$$

Blakley'in şeması gibi Shamir'in şeması da idealdir. Bununla birlikte yetkili bir W alt kümesi için M_W matrisi, kare Vandermonde matrisidir. Bu sebeple her zaman mükemmeldir. Eğer W' matrisi $k' < k$ ise katsayı matrisi $M_{W'}$ matrisinin satır sayısı, sütün sayısından küçüktür. Bu ise $M_{W'}$ nün çözülemeyeceği anlamına gelir [17].

Örnek 3.3. F_7 üzerinde tanımlanan, sırrı 6 ve erişim yapısı $(3,5)$ olan bir sır paylaşım şeması, Shamir'in yöntemi ile aşağıdaki gibi kurulabilir.

Sır parçaların üretmek için kullanılan fonksiyon,

$$f(x) = 3x^2 + 4x + 6 \in F_7[x]$$

olsun.

Sır parçaları,

$$f(1) = 3 \cdot 1^2 + 4 \cdot 1 + 6 = 6$$
$$f(2) = 3 \cdot 2^2 + 4 \cdot 2 + 6 = 5$$
$$f(3) = 3 \cdot 3^2 + 4 \cdot 3 + 6 = 3$$
$$f(4) = 3 \cdot 4^2 + 4 \cdot 4 + 6 = 0$$
$$f(5) = 3 \cdot 5^2 + 4 \cdot 5 + 6 = 3$$

şeklinde hesaplanır.

3, 4, 5 numaralı katılımcılar bir araya gelerek oluşan $W = \{3,4,5\}$ alt kümesi için sır aşağıdaki gibi bulunur.

$$f(x) = \sum_{j \in W} y_j l_j(x)$$

$$l_j(x) = \prod_{m \in W-\{j\}} \frac{x-m}{j-m}$$

$$l_3(x) = \frac{(x-4)}{(3-4)}\frac{(x-5)}{(3-5)} = [(x-4)6][(x-5)3] = (6x+4)(3x+6) = 4x^2+6x+3$$
$$l_4(x) = \frac{(x-3)}{(4-3)}\frac{(x-5)}{(4-5)} = [(x-3)1][(x-5)6] = (x+4)(6x+5) = 6x^2+x+6$$
$$l_5(x) = \frac{(x-3)}{(5-3)}\frac{(x-4)}{(5-4)} = [(x-3)4][(x-4)1] = (4x+2)(x+3) = 4x^2+6$$

$$f(x) = y_3 l_3(x) + y_4 l_4(x) + y_5 l_5(x)$$
$$f(x) = 3(4x^2+6x+3) + 0(6x^2+x+6) + 3(4x^2+6)$$
$$f(x) = (5x^2+4x+2) + (0) + (5x^2+4)$$
$$f(x) = 3x^2+4x+6$$

bulunur. Polinomun sabit terimi 6, aynı zamanda sır değeridir.

Bu örnek, aşağıdaki gibi de çözülebilir.

Sırrı oluşturmak için kullanılan $f(x) = \sum_{i=0}^{k-1} a_i x^i$ fonksiyonunu tekrar elde etmek için, katılımcı kimlik numaraları ve sır değerleri ile birinci dereceden üç bilinmeyenli denklem sistemi oluşturulur. Burada x değerleri ve bu değerlere karşılık gelen $y = f(x)$ değerleri bilinmektedir. Buradan hareketle f(x) fonksiyonunun katsayıları bulunur. Bu sistem çözülerek sır değerine ulaşılır.

$$y_{u_i} = f(x_{u_i}) = a_0 + a_1 x_{u_i} + a_2 x_{u_i}^2 + \ldots + a_{k-1} x_{u_i}^{k-1} \in F_q[x]$$

3, 4 ve 5 numaralı katılımcılar bir araya gelerek sır oluşturulacaktır.

$$f(3) = 3 \quad \Rightarrow \quad 3 = a_0 + 3a_1 + 3^2 a_2 \pmod 7$$
$$f(4) = 0 \quad \Rightarrow \quad 0 = a_0 + 4a_1 + 4^2 a_2 \pmod 7$$
$$f(5) = 3 \quad \Rightarrow \quad 3 = a_0 + 5a_1 + 5^2 a_2 \pmod 7$$

Bu denklem sistemi matris biçiminde yazılarak çözülebilir.

$$\begin{bmatrix} 3^0 & 3^1 & 3^2 \\ 4^0 & 4^1 & 4^2 \\ 5^0 & 5^1 & 5^2 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} y_3 \\ y_4 \\ y_5 \end{bmatrix} \pmod 7$$

$$\begin{bmatrix} 1 & 3 & 2 \\ 1 & 4 & 2 \\ 1 & 5 & 4 \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ a_2 \end{bmatrix} = \begin{bmatrix} 3 \\ 0 \\ 3 \end{bmatrix} \pmod 7$$

$$\left[\begin{array}{ccc|c} 1 & 3 & 2 & 3 \\ 1 & 4 & 2 & 0 \\ 1 & 5 & 4 & 3 \end{array}\right] \xrightarrow[l_3 \to 6l_1 + l_3]{l_2 \to 6l_1 + l_2} \left[\begin{array}{ccc|c} 1 & 3 & 2 & 3 \\ 0 & 1 & 0 & 4 \\ 0 & 2 & 2 & 0 \end{array}\right] \xrightarrow{l_3 \to 5l_2 + l_3} \left[\begin{array}{ccc|c} 1 & 3 & 2 & 3 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 2 & 6 \end{array}\right]$$

$$\xrightarrow{l_3 \to 4l_3} \left[\begin{array}{ccc|c} 1 & 3 & 2 & 3 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 3 \end{array}\right] \xrightarrow{l_1 \to l_1 + 4l_2 + 5l_3} \left[\begin{array}{ccc|c} 1 & 0 & 0 & 6 \\ 0 & 1 & 0 & 4 \\ 0 & 0 & 1 & 3 \end{array}\right] \pmod 7$$

$X = (6, \quad 4, \quad 3)$

bulunur. X vektörünün ilk bileşeni 6, aynı zamanda sır değeridir.

3.4. Massey'in Sır Paylaşım Şeması

Massey ilgili çalışmasında, sır paylaşım şemaları ile lineer kodlar arasında bir bağlantı kurmuştur. Bu şemada erişim yapısı olarak, eşik erişim yapısı kullanılmamaktadır. Massey'in şemasının dezavantajlarından biri, erişim yapısının yönetici tarafından tam olarak belirlenememesidir. Erişim yapısı, üzerinde çalışılan lineer kodun dual kodu kullanılarak bulunur. Minimal erişim kümeleri ile dual kodun ilk bileşeni 1 olan minimal kodsözcükleri arasında bire-bir bir ilişki vardır.

Tanım 3.6 (Vektörün desteği). Bir kodsözcüğünün desteği, o kod sözcüğünün sıfırdan farklı pozisyonlarının kümesidir $c = \{c_0, c_1, \cdots, c_{n-1}\} \in (F_q)^n$ kod sözcüğü için,

$S(c) = \{0 \leq i < n \mid c_i \neq 0\}$

dır [18].

Tanım 3.7. $c_1, c_2 \in (F_q)^n$ olmak üzere c_1 kodsözcüğününün desteği, c_2 kod sözcüğünün desteğinin alt kümesi ise, c_2 kodsözcüğü, c_1 kodsözcüğünü örter denir [18].

Tanım 3.8 (Minimal kodsözcüğü). Sıfırdan farklı bir kod sözcüğü yalnızca kendisinin skaler katlarını örtüyorsa bu kodsözcüğüne, minimal kodsözcüğü denir [18].

Sır parçalarının oluşturulması için N katılımcılı bir sistemde kod uzunluğu $N+1$ olan bir kod seçilmelidir. Erişim yapısının oluşturulmasında, dual kodun belirlenmesi önemlidir. Dual kod oluşturulurken ilk bileşen, sırra erişim olup olmadığı ile ilgili bilgi verir. Eğer ilk bileşen 1 ve minimal kodsözcüğü ise sırra erişim vardır. Diğer bileşenler ise sırra erişebilecek katılımcıları belirtir. Örneğin A, B, C, D katılımcılarının olduğu bir sistemde sırra, $\{A, B\}$ katılımcılarının bir araya gelmesiyle erişilmesi isteniyorsa, dual kodun minimal kodsözcükleri içinde 11100 kodsözcüğü yer almalıdır. Burada ilk bileşen, bu kodsözcüğü ile tanımlanan kümenin sırra erişebileceğini ifade eder. İkinci bileşen, A katılımcısının bu kümenin içinde yer aldığını; üçüncü bileşen, B katılımcısının bu kümenin içinde olduğunu gösterir. Dördüncü ve beşinci bileşenler sıfır olduğu için C ve D katılımcılarının sır parçalarının bilinmemesinin önemi yoktur.

$\{A, B\}$ ve $\{B, C, D\}$ kümelerinin sırra erişebildiği bir sistemin eşlik-denetim matrisi aşağıdaki gibidir.

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix}_{2\times 5}$$

Bu eşlik-denetim matrisini, üreteç matris olarak kullanan ikili (binary) kodun kodsözcükleri aşağıdaki gibidir.

$C^{\perp} = \{11100, 01011, 10111, 00000\}$.

$C^{\perp}$ nin destek vektörleri aşağıdaki gibidir.

$S(11100) = \{0, 1, 2\}$

$S(01011) = \{1, 3, 4\}$

$S(10111) = \{0, 2, 3, 4\}$

$S(00000) = \varnothing$

Yukarıdaki destek vektörleri incelendiğinde (00000) vektörünün dışındaki tüm vektörlerin, minimal kodsözcüğü olduğu görülür. Bu minimal kodsözcükleri içerisinde ilk bileşeni 1 olanlar 11100 ve 10111 dir. Bu kodsözcükleri ile belirtilen katılımcı kümeleri sırra erişebilir.

Yukarıdaki eşlik-denetim matrisi ile üretilen C kodu aşağıdaki gibidir.

$C = \{00000, 11001, 11010, 00011, 10100, 01101, 01110, 10111\}.$

Sırrı oluşturmak için ilk bileşeni sırra eşit olan rastgele bir kodsözcüğü seçilir. Bu kodsözcüğünün ilk bileşeni gizlenir. İkinci bileşeni A katılımcısına sır parçası olarak verilir. Üçüncü bileşeni B katılımcısına verilir ve bu şekilde devam edilir.

Seçilen bu kodsözcüğü $v = \{v_1, v_2, v_3, v_4, v_5\} \in C$ olsun.

$\forall\, h \in C^{\perp}$ için $< v, h >= 0$ olur.

$h = 11100$ alınırsa $< v, h >= 1 \cdot v_1 + 1 \cdot v_2 + 1 \cdot v_3 + 0 \cdot v_4 + 0 \cdot v_5 = 0$ olur.

Yukarıdaki eşitlikten görülebileceği gibi v_2 ve v_3 değerleri bilinirse, v_1 bileşeni bulunur. v_2 ve v_3 sır parçaları A ve B katılımcılarına verilen sır parçalarıdır ve bu parçaların, sırra ulaşabilecekleri açıktır.

4. SIR GÖRÜNTÜ PAYLAŞIMI

Bu bölümün ilk kısmında cisim genişlemelerinden yararlanılarak yeni bir yaklaşım ile bir sır paylaşım şeması önerilmiştir. İkinci kısmında ise önerilen şemanın görüntülere uygulanması açıklanmıştır.

4.1. Cisim Genişlemeleri Üzerinde Sır Paylaşım Şeması

Burada bir cisim genişlemesi kullanılarak Shamir'in sır paylaşım şeması kurulmuştur. Sır paylaşım şemasının giriş ve çıkış değerleri tam sayılar olarak alınıp, işlemler polinomlar üzerinde yapılmıştır. Sonlu cisim genişlemesinin eleman sayısı $q = p^m$ (p asal sayı, $m \in Z^+$) dir. Sır ve katılımcıların kimlikleri,

$$M_q = \{a \mid 0 \leq a \leq q-1, a \in Z\} \tag{4.1}$$

kümesinin elemanlarından seçilmiştir. M_q ile GF(q) aynı kuvvettedir. Çünkü bu iki küme arasında aşağıdaki gibi üzerine (1-1) bir fonksiyon kurulabilir.

$$\begin{array}{lccccccc} M_q & = \{ & 0, & 1, & 2, & 3, & \cdots & q-1 \quad \} \\ & & \updownarrow & \updownarrow & \updownarrow & \updownarrow & \cdots & \updownarrow \\ GF(q) & = \{ & 0, & 1, & \theta, & (\theta+1), & \cdots & (\theta^{m-1}+\cdots) \quad \} \end{array}$$

Bu seçilen tam sayıların GF(q) nun elemanı olan polinomlar cinsinden yazılması, Algoritma (4.1) kullanılarak yapılır.

Algoritma 4.1. M_q kümesinin elemanlarının GF(q) nun elemanlarına dönüştürülmesi.
GİRİŞ: $a \in M_q$
ÇIKIŞ: $b \in GF(q)$

1. a, p tabanında m uzunluklu vektörler olarak yazılır.
2. Bu vektörler polinom biçiminde yazılır.

Örnek 4.1. $5 \in M_8$ nin polinom karşılığı $5 = (101)_2 = \theta^2 + 1 \in GF(8)$ olur.

Örnek 4.2. $5 \in M_9$ nin polinom karşılığı $5 = (12)_3 = \theta + 2 \in GF(9)$ olur.

İşlemlerin sonucunda elde edilen polinomların tekrar tam sayı biçiminde yazılması için Algoritma (4.2) kullanılır.

Algoritma 4.2. GF(q) nun elemanlarının M_q kümesinin elemanları cinsinden yazılması.
GİRİŞ: $b \in GF(q)$
ÇIKIŞ: $a \in M_q$

1. b, p tabanında m uzunluklu vektörler şeklinde yazılır.
2. Bu vektörler onluk tabanda yazılır.

Örnek 4.3. $\theta^2 + 1 \in GF(8)$ in tam sayı karşılığı $\theta^2 + 1 = (101)_2 = 5 \in M_8$ olur.

Örnek 4.4. $2\theta + 1 \in GF(9)$ in tam sayı karşılığı $2\theta + 1 = (21)_3 = 7 \in M_8$ olur.

Shamir'in şemasında olduğu gibi, polinomun sabit terimi a_0 sırra eşit ve a_i $(1 \leq i \leq k-1)$ katsayıları rastgele seçilerek $k-1$ dereceli bir p(x) polinomu oluşturulur.

$$p(x) = \sum_{i=0}^{k-1} a_i x^i \in M_q[x]. \tag{4.2}$$

Bu polinomun katsayıları GF(q) nun elemanları cinsinden yazılır.

$$t(x) = \sum_{i=0}^{k-1} b_i x^i \in (GF(q))[x]. \tag{4.3}$$

Katılımcıların kimlik numaraları $u_1, u_2, \cdots, u_n \in M_q$ olsun. Bu kimlik numaralarına, Algoritma (4.1) uygulanarak $v_1, v_2, \cdots, v_n \in GF(q)$ elemanları bulunur. Katılımcılara verilecek sır parçalarının GF(q) daki görüntüleri olan $r_1, r_2, \cdots, r_n \in GF(q)$ elemanları, (4.4) eşitliğindeki gibi bulunur.

$$r_i = t(v_i) \in GF(q) \tag{4.4}$$

Bulunan elemanlar, Algoritma (4.2) kullanılarak $y_1, y_2, \cdots, y_n \in M_q$ tam sayıları olarak yazılır ve katılımcılara dağıtılır.

Sırrın tekrar oluşturulması süreci de benzer şekilde olacaktır. $W = \{d_1, d_2, \cdots d_k\}$ $(d_1, d_2, \cdots, d_k \in M_q)$, k elemandan oluşan ve sırrı oluşturmak için bir araya gelen katılımcıların kimlik numaralarının bulunduğu bir küme olsun. (d_i, y_i) $(1 \leq i \leq k)$ ikilisinde d_i, katılımcının kimliğini; y_i, d_i katılımcısına ait sır parçasını ifade eder. Bu ikililer Algoritma (4.1) kullanılarak (v_i, r_i) $(v_i, r_i \in GF(q))$ polinom ikilileri şeklinde yazılır. Elde edilen bu ikililer Lagrange Interpolasyonu aracılığı ile t(x) polinomu tekrar elde edilir. t(x) polinomundan, Algoritma (4.2) kullanılarak p(x) polinomu elde edilir. Sır, Eşitlik (4.5) kullanılarak bulunur.

$$s = p(0) \tag{4.5}$$

Interpolasyon işleminde kullanılmak üzere polinomun (mod f(x)) e göre çarpımsal tersini bulmak için Algoritma (1.5) kullanılır.

Örnek 4.5. Katılımcı sayısı n = 5, eşik değeri k = 3 ve sır s = 4 parametrelerine sahip bir sır paylaşım şeması $GF(2^3)$ cisim genişlemesi üzerinde aşağıdaki gibi kurulur.

$f(x) = x^3 + x^2 + 1$ polinomu GF(2) de indirgenemezdir. Bu polinomun bir kökü θ olsun.

$$GF(8) = \{0, 1, \theta, \theta+1, \theta^2, \theta^2+1, \theta^2+\theta, \theta^2+\theta+1\}$$

$$\theta^1 = \theta$$
$$\theta^2 = \theta^2$$
$$\theta^3 = \theta^2 + 1$$
$$\theta^4 = \theta^2 + \theta + 1$$
$$\theta^5 = \theta + 1$$
$$\theta^6 = \theta^2 + \theta$$
$$\theta^7 = 1$$

M_8 ile GF(8) arasındaki ilişki aşağıdaki gibi olacaktır.

$0 \leftrightarrow 0$ $\quad$ $4 \leftrightarrow \theta^2$

$1 \leftrightarrow 1$ $\quad$ $5 \leftrightarrow \theta^2 + 1$

$2 \leftrightarrow \theta$ $\quad$ $6 \leftrightarrow \theta^2 + \theta$

$3 \leftrightarrow \theta + 1$ $\quad$ $7 \leftrightarrow \theta^2 + \theta + 1$

Sır parçalarını oluşturmak için kullanılacak p(x) polinomu,

$p(x) = x^2 + 5x + 4 \in M_8[x]$

dir.

Polinomun katsayıları GF(8) in elemanları şeklinde,

$t(x) = (1)x^2 + (\theta^2 + 1)x + (\theta^2)$

olarak yazılır.

Katılımcıların kimlik numaraları,

$u_1 = 1, \quad u_2 = 2, \quad u_3 = 3, \quad u_4 = 4, \quad u_5 = 5$

olsun. Bunlara GF(8) de karşılık gelen değerler,

$v_1 = 1, \quad v_2 = \theta, \quad v_3 = \theta + 1, \quad v_4 = \theta^2, \quad v_5 = \theta^2 + 1$

dir.

Sır parçaları aşağıdaki gibi bulunur.

$$\begin{aligned}
r_1 &= t(v_1) = t(1) = 0 &&\Rightarrow y_1 = 0\\
r_2 &= t(v_2) = t(\theta) = \theta^2 + \theta + 1 &&\Rightarrow y_2 = 7\\
r_3 &= t(v_3) = t(\theta + 1) = \theta + 1 &&\Rightarrow y_3 = 3\\
r_4 &= t(v_4) = t(\theta^2) = 0 &&\Rightarrow y_4 = 0\\
r_5 &= t(v_5) = t(\theta^2 + 1) = \theta^2 &&\Rightarrow y_5 = 4
\end{aligned}$$

3 katılımcı bir araya geldiğinde sırra ulaşabilecektir. Örneğin 2, 4 ve 5 numaralı katılımcıların sırra erişebildiği kabul edilsin. Bu katılımcılara karşılık gelen sır paylaşımları aşağıdaki gibidir.

$$\begin{aligned}
(d_2, y_2) = (2,7) &\rightarrow (v_2, r_2) = (\theta, \theta^2 + \theta + 1)\\
(d_4, y_4) = (4,0) &\rightarrow (v_4, r_4) = (\theta^2, 0)\\
(d_5, y_5) = (5,4) &\rightarrow (v_5, r_5) = (\theta^2 + 1, \theta^2)
\end{aligned}$$

$W = \{2,4,5\}$ ve $W' = \{\theta, \theta^2, \theta^2 + 1\}$ olmak üzere,

$$t(x) = \sum_{j \in W'} y_j l_j(x)$$

$$l_j(x) = \prod_{m \in W' - \{j\}} \frac{x - m}{j - m}$$

$$\begin{aligned} l_\theta(x) &= \frac{(x-(\theta^2))}{(\theta-(\theta^2))}\frac{(x-(\theta^2+1))}{(\theta-(\theta^2+1))} \\ &= [(x-(\theta^2))(\theta^2+\theta)^{-1}][(x-(\theta^2+1))(\theta^2+\theta+1)^{-1}] \\ &= [(x-\theta^2)(\theta)][(x-\theta^2+1)(\theta^2+1)] \\ &= (\theta^2+\theta+1)x^2+(\theta^2+\theta+1)x+(\theta^2) \end{aligned}$$

$$\begin{aligned} l_{\theta^2}(x) &= \frac{(x-(\theta))}{(\theta^2-(\theta))}\frac{(x-(\theta^2+1))}{(\theta^2-(\theta^2+1))} \\ &= [(x-(\theta))(\theta^2+\theta)^{-1}][(x-(\theta^2+1))(1)^{-1}] \\ &= [(x-\theta)(\theta)][(x-\theta^2+1)(1)] \\ &= (\theta)x^2+(\theta+1)x+(\theta+1) \end{aligned}$$

$$\begin{aligned} l_{\theta^2+1}(x) &= \frac{(x-(\theta))}{(\theta^2+1-(\theta))}\frac{(x-(\theta^2))}{(\theta^2+1-(\theta^2))} \\ &= [(x-(\theta))(\theta^2+\theta+1)^{-1}][(x-(\theta^2))(1)^{-1}] \\ &= [(x-\theta)(\theta^2+1)][(x-\theta^2)(1)] \\ &= (\theta^2+1)x^2+(\theta^2)x+(\theta^2+\theta) \end{aligned}$$

$$t(x) = \sum_{j \in W'} y_j l_j(x) = (\theta^2+\theta+1)l_\theta + (0)l_{\theta^2} + (\theta^2)l_{\theta^2+1}$$

$$\begin{aligned} t(x) = \; & (\theta^2+\theta+1)[(\theta^2+\theta+1)x^2+(\theta^2+\theta+1)x+(\theta^2)] \\ & +(0)[(\theta)x^2+(\theta+1)x+(\theta+1)] \\ & +(\theta^2)[(\theta^2+1)x^2+(\theta^2)x+(\theta^2+\theta)] \end{aligned}$$

$$\begin{aligned} t(x) = \; & ((\theta^4+\theta^2+1)x^2+(\theta^4+\theta^2+1)x+(\theta^4+\theta^3+\theta^2)) \\ & +((0)x^2+(0)x+(0)) \\ & +((\theta^4+\theta^2)x^2+(\theta^4)x+(\theta^4+\theta^3)) \end{aligned}$$

$$\begin{aligned} t(x) = \; & ((\theta)x^2+(\theta)x+(\theta^2+\theta)) \\ & +((0)x^2+(0)x+(0)) \\ & +((\theta+1)x^2+(\theta^2+\theta+1)x+(\theta)) \end{aligned}$$

$t(x) = (1)x^2 + (\theta^2 + 1)x + (\theta^2) \in (GF(8))[x]$

Buradan Algoritma (4.2) ile,

$p(x) = x^2 + 5x + 4 \in M_8[x]$

elde edilir. Dolayısı ile sırra,

$s = p(0) = 4$

şeklinde tekrar ulaşılır.

4.2. Sır Paylaşım Şemalarının Görüntülere Uygulanması

4.2.1. Giriş

Sayısal görüntü, doğadaki görüntülerin sensörler aracılığıyla bilgisayara aktarılmasıyla oluşur. Sayısal görüntüler, belli aralıklarla örneklenmiş sinyallerdir. Bu örnekleme noktalarına piksel (pixel – picture element) denir. Görüntü, temel olarak piksellerden oluşan iki boyutlu bir matristir. Bu matris oluşturulurken her piksel değerinin kaç bit olarak saklanacağı belirlenmelidir. Bu değere bit derinliği denir. Bit derinliği 8 olan bir resim için bir pikselin alabileceği en büyük değer 255 tir.

Genellikle renkli bir resim elde etmek için 3 bant kullanılır. Bu bantların her biri aynı boyutta bir matristir ve her matris ayrı bir renk bileşenini (kırmızı, yeşil, mavi) temsil eder.

4.2.2. Sır paylaşım şeması

Yüksekliği h ve genişliği w olan tek bantlı bir görüntü, I matrisi olarak ele alınsın. Burada yükseklik, matrisin satır sayısına; genişlik ise sütun sayısına karşılık gelmektedir. I matrisinin elemanlarının seçildiği sır uzayı, M_q olsun. Sır olarak I görüntüsünü ve erişim yapısı olarak (k, n)-eşik erişim yapısını kullanan bir sır paylaşım şeması aşağıdaki gibi oluşturulabilir.

$$I = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1w} \\ \vdots & \ddots & & \vdots \\ a_{h1} & a_{h2} & \cdots & a_{hw} \end{bmatrix}_{h\times w}, \quad a_{ij} \in M_q \tag{4.6}$$

I matrisi kullanılarak yüksekliği h ve genişliği $\lceil \frac{w}{k-1} \rceil$ olan polinomlardan oluşan P(x) matrisi üretilir. P(x) aşağıdaki şekilde oluşturulur.

$$P(x) = [p_{ij}(x)] = \begin{bmatrix} p_{11}(x) & p_{12}(x) & \cdots & p_{1w'}(x) \\ \vdots & \ddots & & \vdots \\ p_{h'1}(x) & p_{h'2}(x) & \cdots & p_{h'w'}(x) \end{bmatrix}, \quad h' = h,\ w' = \lceil \frac{w}{k-1} \rceil \tag{4.7}$$

$$p_{ij}(x) = rx^{k-1} + \sum_{t=0}^{k-2} a_{i'j'}x^t \in M_q[x], \quad i' = i,\ j' = (j-1)\cdot(k-1)+(k-t),\ r \in M_q - \{0\} \tag{4.8}$$

Burada a_{ij}; I matrisinin i. satır, j. sütun elemanına karşılık gelmektedir.

Bilindiği gibi $p_{ij}(x)$ polinomunun derecesi, $(k-1)$ dir. I matrisinin sütunları $(k-1)$ elemandan oluşan parçalara ayrılır. i inci satırdaki j inci parça $H_{ij} = [h_1, h_2, \cdots, h_{k-1}]$ vekörü ile ifade edilir. P(x) matrisinin p_{ij} $(1 \leq i \leq h', 1 \leq j \leq w')$ elemanını oluşturmak için H_{ij} vektörü kullanılır. H_{ij} vektörünün I matrisi üzerindeki ilk elemanı h_1; i inci satırda, $[(j-1)(k-1)+1]$ inci sütunda bulunur. $p_{ij}(x)$ polinomunun başkatsayısı, $M_q - \{0\}$ kümesinden rastgele seçilir. $p_{ij}(x)$ polinomunun, derecesi t $(0 \leq t \leq k-2)$ olan teriminin katsayısı, H_{ij} vektörünün $(k-t-1)$ inci elemanı olarak seçilir. Bu da I görüntüsü üzerinde i inci satırda, $[(j-1)\cdot(k-1)+(k-t)]$ inci sütuna denk gelir.

Algoritma (4.1) kullanılarak, elemanları M_q üzerinde tanımlı polinomlar olan P(x) matrisi, elemanları (GF(q))[x] halkasına ait polinomlar, T(x) matrisinin elemanları olarak yazılır.

$$T(x) = [t_{ij}(x)] = \begin{bmatrix} t_{11}(x) & t_{12}(x) & \cdots & t_{1w'}(x) \\ \vdots & \ddots & & \vdots \\ t_{h'1}(x) & t_{h'2}(x) & \cdots & t_{h'w'}(x) \end{bmatrix}, \quad t_{ij}(x) \in (GF(q))[x] \tag{4.9}$$

Shamir'in şemasında olduğu gibi her katılımcıya bir kimlik numarası belirlenir. $u_i \in M_q$ $(1 \leq i \leq n)$ ve her katılımcı için sır parçası (4.10) eşitliği ile bulunur.

Belirlenen kimlik numaraları, GF(q) üzerinde yapılacak işlemlerde kullanılmak üzere Algoritma (4.1) ile $v_i \in GF(q)$ $(1 \leq i \leq n)$ elemanlarına dönüştürülür. Sır parçasının GF(q) üzerindeki görüntüsü olan R_i $(1 \leq i \leq n)$ matrisi; (4.10) eşitliğindeki gibi T(x) matrisine, $v_i \in GF(q)$ $(1 \leq i \leq n)$ değerlerinin uygulanması ile bulunur.

$$R_i = T(v_i), \quad (1 \leq i \leq n) \tag{4.10}$$

daha açık bir ifade ile,

$$R_i = \begin{bmatrix} t_{11}(v_i) & t_{12}(v_i) & \cdots & t_{1w'}(v_i) \\ \vdots & \ddots & & \vdots \\ t_{h'1}(v_i) & t_{h'2}(v_i) & \cdots & t_{h'w'}(v_i) \end{bmatrix}_{h' \times w'} \tag{4.11}$$

dir.

Bulunan polinom matrisi Algoritma (4.2) kullanılarak elemanları M_q kümesinden seçilen, Y_i $(1 \leq i \leq n)$ matrisi olarak yazılır.

$$Y_i = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1w'} \\ \vdots & \ddots & & \vdots \\ a_{h'1} & a_{h'2} & \cdots & a_{h'w'} \end{bmatrix}_{h' \times w'} \tag{4.12}$$

4.2.3. Sırrın yeniden oluşturulması

Sırra ulaşabilmek için en az k adet sır parçasının bilinmesi gerekmektedir. Yani katılımcıların kimlik numaralarından oluşan $W = \{u_{t_i} \mid t_i \in M_q - \{0\}, 1 \leq i < n\}$ kümesinin sırra ulaşabilmesi için, kümenin eleman sayısının en az k olması gerekir. $(u_{t_i}, Y_{u_{t_i}})$ ikilisinde; i, katılımcının W kümesi içindeki sırasını; t_i, W kümesinin içinde i inci sırada yer alan katılımcının, katılımcı kümesindeki sırasını; u_{t_i}, katılımcı kümesi içinde sırası t_i olan elemanın kimlik numarasını ifade eder. $Y_{u_{t_i}}$, kimlik numarası u_{t_i} olan katılımcıya verilen sır parçasıdır. Bu ikililer Algoritma (4.1) kullanılarak GF(q) üzerinde tanımlı $(v_{t_i}, R_{u_{t_i}})$ ikililerine dönüştürülür.

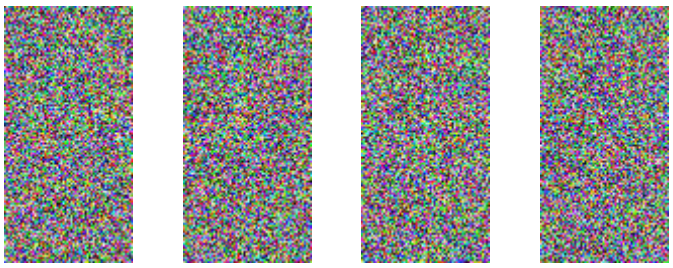
Elde edilen $(v_{t_i}, R_{u_{t_i}})$ ikilileri üzerinde Lagrange Interpolasyon kullanılarak, (GF(q))[x] polinom halkasında olan T(x) matrisi tekrar bulunur. Algoritma (4.2) ile katsayıları $M_q[x]$ in elemanı olan polinomlardan oluşan P(x) matrisi bulunur. Bu polinomun katsayıları ile görüntü tekrar oluşturulur.

Not: Renkli görüntüler için, bu işlemler resimde bulunan bant sayısı kadar tekrar edilir. Yaygın olarak kullanılan kırmızı, yeşil ve mavi renk bileşenlerinden oluşan görüntülerde, yukarıda tanımlanan işlemler her bant için ayrı ayrı yapılır ve sonuç olarak elde edilen matrisler birleştirilerek tekrar renkli bir görüntü oluşur.

(a) (b)

Şekil 4.1. Sır ve tekrar oluşturulmuş görüntü.

Şekil (4.1a)'da orijinal sır resmi, Şekil (4.2a)-(4.2d) te sır parçaları görülmektedir. Şekil (4.1b)'de, Şekil (4.2a), (4.2b) ve (4.2c) ye karşılık gelen sır parçaları kullanılarak elde edilen resim yer almaktadır.



(a) (b) (c) (d)

Şekil 4.2. (3,4)-eşik şemalı sır görüntü paylaşım şeması için sır parçalar.

Not: Sır parçaları kaydedilirken jpeg gibi kayıplı sıkıştırma yapan dosya formatları kullanılırsa, sır parçalarının değerinde gözle görülemeyecek kadar küçük değişiklikler meydana gelir. Bu da sırrın kaybedilmesi anlamına gelir. Zira, sır parçası üzerinde yapılacak küçük bir değişiklik, resmi tekrar oluştururken büyük bozulmalara sebep olabilir.

Örnek 4.6. Sır uzayı M_{256} olarak seçilsin. GF(256) cisim genişlemesini oluşturmak için kullanılacak indirgenemez polinom $f(x) = x^8 + x^4 + x^3 + x^2 + 1 \in (GF(2)[x])$ olsun. Aşağıda verilen I matrisi kullanılarak katılımcı sayısı 5 ve eşik değeri 3 olan sır paylaşım şeması aşağıdaki gibi oluşturulabilir.

$$I = \begin{bmatrix} 254 & 241 & 189 & 189 & 241 & 254 \\ 254 & 189 & 254 & 254 & 189 & 254 \\ 197 & 210 & 210 & 210 & 210 & 197 \\ 178 & 192 & 209 & 209 & 192 & 178 \\ 172 & 186 & 196 & 196 & 186 & 172 \\ 157 & 168 & 168 & 168 & 168 & 157 \end{bmatrix}_{6\times 6}$$

P(x) matrisi, baş katsayısı rastgele ve diğer katsayıları I matrisi üzerinden seçilerek aşağıdaki gibi oluşturulabilir.

$$P(x) = \begin{bmatrix} (2x^2 + 254x + 241) & (8x^2 + 189x + 189) & (64x^2 + 241x + 254) \\ (128x^2 + 254x + 189) & (x^2 + 254x + 254) & (8x^2 + 189x + 254) \\ (16x^2 + 197x + 210) & (128x^2 + 210x + 210) & (28x^2 + 210x + 197) \\ (196x^2 + 178x + 192) & (57x^2 + 209x + 209) & (59x^2 + 192x + 178) \\ (x^2 + 172x + 186) & (159x^2 + 196x + 196) & (56x^2 + 186x + 172) \\ (244x^2 + 157x + 168) & (209x^2 + 168x + 168) & (170x^2 + 168x + 157) \end{bmatrix}$$

P(x) matrisindeki polinomların katsayılarını GF(256) ya taşımak suretiyle elde edilen $T(x) = [t_{ij}(x)], t_{ij}(x) \in (GF(q))[x]$ matrisinin elemanları aşağıdaki gibidir.

$$t_{11}(x) = (\theta)x^2 + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)x + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + 1)$$
$$t_{12}(x) = (\theta^3)x^2 + (\theta^7 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + 1)x + (\theta^7 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + 1)$$
$$t_{13}(x) = (\theta^6)x^2 + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + 1)x + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)$$
$$t_{21}(x) = (\theta^7)x^2 + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)x + (\theta^7 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + 1)$$
$$t_{22}(x) = (1)x^2 + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)x + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)$$
$$t_{23}(x) = (\theta^3)x^2 + (\theta^7 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + 1)x + (\theta^7 + \theta^6 + \theta^5 + \theta^4 + \theta^3 + \theta^2 + \theta)$$
$$t_{31}(x) = (\theta^4)x^2 + (\theta^7 + \theta^6 + \theta^2 + 1)x + (\theta^7 + \theta^6 + \theta^4 + \theta)$$
$$t_{32}(x) = (\theta^7)x^2 + (\theta^7 + \theta^6 + \theta^4 + \theta)x + (\theta^7 + \theta^6 + \theta^4 + \theta)$$
$$t_{33}(x) = (\theta^4 + \theta^3 + \theta^2)x^2 + (\theta^7 + \theta^6 + \theta^4 + \theta)x + (\theta^7 + \theta^6 + \theta^2 + 1)$$
$$t_{41}(x) = (\theta^7 + \theta^6 + \theta^2)x^2 + (\theta^7 + \theta^5 + \theta^4 + \theta)x + (\theta^7 + \theta^6)$$

$$t_{42}(x) = (\theta^5+\theta^4+\theta^3+1)x^2+(\theta^7+\theta^6+\theta^4+1)x+(\theta^7+\theta^6+\theta^4+1)$$
$$t_{43}(x) = (\theta^5+\theta^4+\theta^3+\theta+1)x^2+(\theta^7+\theta^6)x+(\theta^7+\theta^5+\theta^4+\theta)$$
$$t_{51}(x) = (1)x^2+(\theta^7+\theta^5+\theta^3+\theta^2)x+(\theta^7+\theta^5+\theta^4+\theta^3+\theta)$$
$$t_{52}(x) = (\theta^7+\theta^4+\theta^3+\theta^2+\theta+1)x^2+(\theta^7+\theta^6+\theta^2)x+(\theta^7+\theta^6+\theta^2)$$
$$t_{53}(x) = (\theta^5+\theta^4+\theta^3)x^2+(\theta^7+\theta^5+\theta^4+\theta^3+\theta)x+(\theta^7+\theta^5+\theta^3+\theta^2)$$
$$t_{61}(x) = (\theta^7+\theta^6+\theta^5+\theta^4+\theta^2)x^2+(\theta^7+\theta^4+\theta^3+\theta^2+1)x+(\theta^7+\theta^5+\theta^3)$$
$$t_{62}(x) = (\theta^7+\theta^6+\theta^4+1)x^2+(\theta^7+\theta^5+\theta^3)x+(\theta^7+\theta^5+\theta^3)$$
$$t_{63}(x) = (\theta^7+\theta^5+\theta^3+\theta)x^2+(\theta^7+\theta^5+\theta^3)x+(\theta^7+\theta^4+\theta^3+\theta^2+1)$$

Katılımcıların kimlik numaraları $u_1 = 1$, $u_2 = 2$, $u_3 = 3$, $u_4 = 4$ ve $u_5 = 5$ olsun. Bunların GF(256) daki karşılıkları, $v_1 = 1$, $v_2 = \theta$, $v_3 = \theta+1$, $v_4 = \theta^2$, $v_5 = \theta^2+1$, olur.

Katılımcılara verilecek sır parçaları

$R_1 = T(1)$

$R_2 = T(\theta)$

$R_3 = T(\theta+1)$

$R_4 = T(\theta^2)$

$R_5 = T(\theta^2+1)$

olarak bulunur. Buradan sır parçalarının M_{256} daki karşılıkları aşağıdaki gibidir.

$$Y_1 = \begin{bmatrix} 13 & 8 & 79 \\ 195 & 1 & 75 \\ 7 & 128 & 11 \\ 182 & 57 & 73 \\ 23 & 159 & 46 \\ 193 & 209 & 159 \end{bmatrix} \quad Y_2 = \begin{bmatrix} 24 & 250 & 28 \\ 102 & 27 & 185 \\ 5 & 81 & 12 \\ 142 & 138 & 195 \\ 251 & 23 & 37 \\ 120 & 134 & 66 \end{bmatrix} \quad Y_3 = \begin{bmatrix} 228 & 79 & 173 \\ 24 & 228 & 12 \\ 208 & 3 & 194 \\ 248 & 98 & 56 \\ 86 & 76 & 167 \\ 17 & 255 & 64 \end{bmatrix}$$

.

$$Y_4 = \begin{bmatrix} 14 & 243 & 105 \\ 138 & 49 & 176 \\ 252 & 85 & 119 \\ 238 & 5 & 2 \\ 32 & 246 & 217 \\ 29 & 163 & 117 \end{bmatrix} \quad Y_5 = \begin{bmatrix} 242 & 70 & 216 \\ 244 & 206 & 5 \\ 41 & 7 & 185 \\ 152 & 237 & 249 \\ 141 & 173 & 91 \\ 116 & 218 & 119 \end{bmatrix}$$

En az 3 katılımcı, Bölüm (4.1) de açıklanan yöntem ile görüntüyü tekrar oluşturur.

4.3. Cisim Genişlemesi Kullanımının Avantajları

Bilindiği üzere bilgisayar ortamında bir dosya, 1 bit (1 veya 0 değerini temsil eden bilgi) dizisi ile ifade edilir. 8 bitten oluşan bir bit dizisi, bayt (byte) olarak adlandırılır. Bir bayt ondalık olarak ifade edilirse (0-255) arasında değer alır ve M_{256} nın bir elemanıdır. Sonuç olarak m bayttan oluşan bir D dosyası, elemanları M_{256} kümesinden seçilen bir vektör olarak ifade edilebilir.

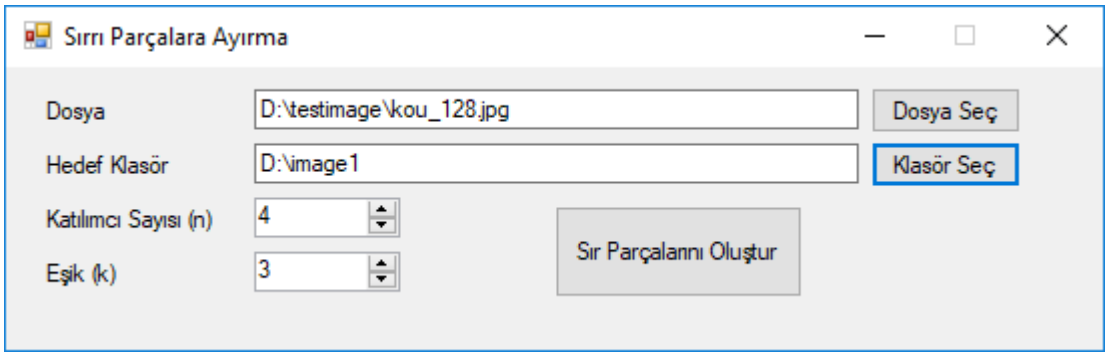
$$D = \begin{pmatrix} a_1 & a_2 & \cdots & a_m \end{pmatrix}$$

Bölüm (4.2) de oluşturulan sır paylaşım şeması kullanılarak herhangi bir dosya (metin, görüntü, video, vb.) sır olarak alınır. Sır paylaşım şemalarında yapılan işlemler bu dosyaya uygulanabilir. Bölüm (4.2) de oluşturulan sır paylaşım şemasında katılımcılar, sırrın görüntü olduğu bilgisine sahiptir. Aynı şema yukarıda bahsedilen şekilde uygulanırsa bu bilgi de gizlenmiş olur. Sır paylaşım şeması GF(256) üzerinde tanımlı olduğu için kayıpsız bir şemadır. İşlemler Shamir'in sır paylaşım şeması kullanılarak GF(251) de yapılsaydı, bu durumda 250 den büyük değerler kaybedilecekti. Bunun sonucunda dosyada bozulmalar olacaktı. Bu bozulmalar Bölüm (4.2) deki gibi görüntüler üzerinde gözle görülemeyecek kadar önemsizdir. Fakat diske yazılmış bayt dizileri için durum böyle değildir. Dosya içinde önemli bir baytın kaybedilmesi, bütün dosyanın kaybedilmesine sebep olabilir. Örneğin bir görüntü dosyası içinde yazan boyut bilgisi kaybedilirse, resim tekrar oluşturulamaz.

4.4. Görüntü Paylaşım Uygulaması

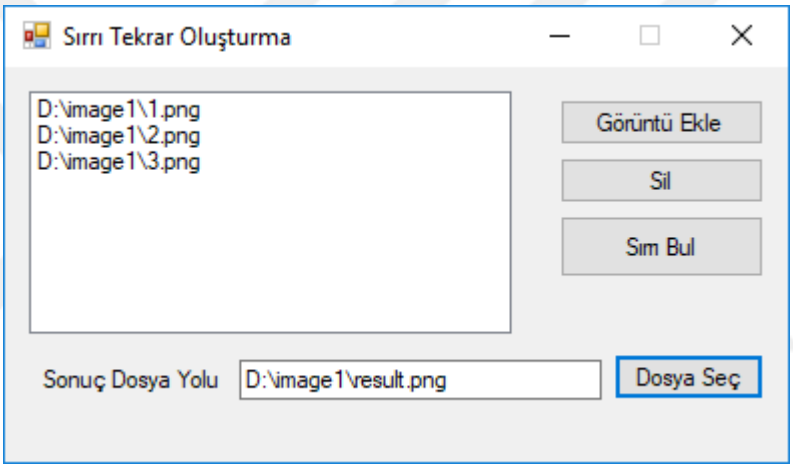
Sır görüntü paylaşım şeması için iki adet program yazılmıştır. Programlar C# programlama dili kullanılarak yazılmıştır. İlk program sır parçalarını oluşturmak için (Şekil (4.3)), ikinci program sır parçalarından sırra tekrar ulaşmak için (Şekil (4.4)) kullanılacaktır.

Şekil (4.3)'de sırrı parçalara ayırmak için kullanılan uygulama ekranı görülmektedir. Burada sır görüntü dosyası ve sır parçalarının kaydedileceği klasör seçilir. Katılımcı



Şekil 4.3. Sır paylaşım uygulama ekran görüntüsü

sayısı ve eşik değeri belirlenir. Oluşan dosyaların ismi, katılımcının kimlik numarası olarak alınır. Kimlik numaraları 1 den başlayarak sıra ile verilir.



Şekil 4.4. Sırrı tekrar oluşturan uygulama ekran görüntüsü

Şekil (4.4)'deki ekranda Görüntü Ekle butonuna basılarak sır parçaları seçilir. Dosya Seç butonu ile sonucun kaydedileceği dosya seçilerek sır bulunabilir.

5. SONUÇ

Yapılan çalışmada sonlu cisimlerden faydalanarak, görüntüler üzerinde kayıpsız bir sır paylaşım şeması önerilmiştir. Elde edilen sır paylaşım şemasının, sayısal ortamda bulunan bütün dosyalara uygulanabileceği gösterilmiştir.

Bu sır paylaşım şeması oluşturulurken, Shamir'in şemasının çalışma prensibinden yararlanılmıştır. Bu sistemde amaç; sırrın parçalara ayrılarak kullanıcılara dağıtılması ve belli sayıda katılımcının bir araya gelerek sırra tekrar ulaşabilmesidir. Dolayısı ile bu yöntem, güvenliği tek bir yerde toplamadığı için riski azaltmakta ve bozulmalara karşı da sistemi garanti altına almaya çalışmaktadır. Şemanın ideal ve mükemmel olması ve veri ile birlikte ekstra yüklerin oluşmamasından dolayı, çalışmalar bu şema üzerinde yapılmıştır.

Tezde sunulan sır paylaşım şemasının kurulumunda, sonlu cisimler teorisine girilmesi ile bu yöntem daha kullanışlı hale getirilmiştir. Daha açık bir ifade ile, hatalı kullanıcılara karşı sistem, garanti altına alınmaya çalışılmıştır.

Kullanılan yöntem, diğer sır paylaşım şemalarına da uygulanarak, yeni sonuçlar elde edilebilir.

KAYNAKLAR

[1] Blakley G. R., Safeguarding cryptographic keys, *Proc. 1979 National Computer Conf.*, New York, 4-7 Haziran 1979.

[2] Shamir A., How to share a secret, *Communications of the ACM*, DOI:10.1002/er.907.

[3] Thien C. C., Lin J. C. , Secret image sharing, *Computer and Graphics*, DOI:10.1016/S0097-8493(02)00131-0.

[4] Yang C. N., Chen T. S., Yu K. H., Wang C. C., Improvements of image sharing with steganography and authentication, *Journal of Systems and Software*, DOI:10.1016/j.jss.2006.11.022.

[5] Çallıalp F., *Soyut Matematik*, 1. Baskı, Birsen Yayınevi, İstanbul, 2015.

[6] Şenkon H., *Soyut Cebir Dersleri*, İstanbul Üniversitesi, İstanbul, 1993.

[7] Ağargün A. G., Ersoy B. A., Oral K. H., Alan M., Aygör N. K., *Soyut Cebir*, Birsen Yayınevi, 1. Baskı, İstanbul, 2015.

[8] Çallıalp F., *Örneklerle Soyut Cebir*, 1. Baskı, Birsen Yayınevi, İstanbul, 2013.

[9] Lidl, R., Niderreiter, H., *Finite Fields*, 1. ed., Cambridge University, 1984.

[10] Çalkavur S., BCH Kodları, Yüksek Lisans Tezi, İstanbul Kültür Üniversitesi, Fen Bilimleri Enstitüsü, İstanbul, 2006, 237090.

[11] Menezes A. J., Oorschot P. V. C., Vanstone S. A., *Handbook of Applied Cryptography,*, 1. ed., CRC Press Inc., Boca Raton, FL, USA, 1996.

[12] Hill R., *A First Course in Coding Theory*, 1. ed., Oxford University, Oxford, 1986.

[13] Ağargün A. G., Burhanzade H., *Lineer Cebir ve Çözümlü Problemleri*, 1. Baskı, Birsen Yayınevi, İstanbul, 2017.

[14] McEliece R. J., Sarwate D. V. On sharing secrets and reed-solomon codes, *Commun. Assoc. Comp.*, DOI:10.1145/358746.358762.

[15] Massey J. L., Minimal codewords and secret sharing, *Proc. 6th Joint Swedish-Russian Workshop on Information Theory*, Mölle, Sweden, Aug. 1993.

[16] Massey J. L., Some applications of coding theory, Cryptography, Codes and Ciphers: Cryptography and Coding IV, 1995.

[17] Yılmaz, R., Some Ideal Secret Sharing Schemes, Yüksek Lisans Tezi, Bilkent Üniversitesi, Fen Bilimleri Enstitüsü, Ankara, 2010, 275041.

[18] Yuan J., Ding C., Secret Sharing Schemes from Three Classes of Linear Codes, *IEEE Trans. on Inf. Theory*, DOI: 10.1109/TIT.2005.860412.

KİŞİSEL YAYINLAR VE ESERLER

[1] **Molla F.**, Çalkavur S., A New Approach to Construct Secret Sharing Schemes Based on Field Extensions, *European Journal of Pure and Applied Mathematics*, 2018, **11**(2).

ÖZGEÇMİŞ

Fatih Molla, 1989 yılında İstanbul'da doğdu. Liseyi Abdurrahman ve Nermin Bilimli Anadolu Meslek Lisesinde okudu. Lisans eğitimini Kocaeli Üniversitesi, Teknik Eğitim Fakültesi, Bilgisayar Öğretmenliği Bölümünde 2011 yılında tamamladı. Halen özel sektörde yazılım uzmanı olarak çalışmaktadır.