T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI ÖZEL MATRİSLERDEN MDS MATRİSLERİN İNŞASI

YÜKSEK LİSANS TEZİ

Samet AYDOĞDU

Enstitü Anabilim Dalı	**:**	**MATEMATİK**
Enstitü Bilim Dalı	**:**	**CEBİR VE SAYILAR TEORİSİ**
Tez Danışmanı	**:**	**Prof. Dr. Mehmet ÖZEN**

KASIM 2017

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BAZI ÖZEL MATRİSLERDEN MDS MATRİSLERİN İNŞASI

YÜKSEK LİSANS TEZİ

Samet AYDOĞDU

Enstitü Anabilim Dalı : MATEMATİK

Enstitü Bilim Dalı : CEBİR VE SAYILAR TEORİSİ

Bu tez 17/11/2017 tarihinde aşağıdaki jüri tarafından oybirliği / oyçokluğu ile kabul edilmiştir.

Prof. Dr. Mehmet ÖZEN Jüri Başkanı	Prof. Dr. Bayram Ali ERSOY Üye	Doç. Dr. Yalçın YILMAZ Üye

BEYAN

Tez içindeki tüm verilerin akademik kurallar çerçevesinde tarafımdan elde edildiğini, görsel ve yazılı tüm bilgi ve sonuçların akademik ve etik kurallara uygun şekilde sunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, tezde yer alan verilerin bu üniversite veya başka bir üniversitede herhangi bir tez çalışmasında kullanılmadığını beyan ederim.

Samet AYDOĞDU

17/11/2017

TEŞEKKÜR

Yüksek lisans eğitimim boyunca değerli bilgi ve deneyimlerinden yararlandığım, her konuda bilgi ve desteğini almaktan çekinmediğim, araştırmanın planlanmasından yazılmasına kadar tüm aşamalarında yardımlarını esirgemeyen, teşvik eden, aynı titizlikte beni yönlendiren değerli danışman hocam Prof. Dr. Mehmet ÖZEN'e teşekkürlerimi sunarım.

Ayrıca bu çalışmamda her türlü yardımını esirgemeyen Arş. Gör. Halit İNCE'ye, N.Tuğba ÖZZAİM'e ve maddi manevi desteğini esirgemeyen aileme teşekkür ederim.

İÇİNDEKİLER

SİMGELER VE KISALTMALAR LİSTESİ

$B_d(R)$: R matrisinin diferansiyel dal sayısı

$B_l(R)$: R matrisinin lineer dal sayısı

C : Kod

d_h : Hamming Uzaklık

d_r : Rank Uzaklık

F : Cisim

$F[x]$: F cisminden katsayılı polinomlar kümesi

$\mathbb{F}_q$: q bir asal sayı olmak üzere q elemanlı sonlu cisim

$\mathbb{F}_{q^n}$: q bir asal sayı olmak üzere q^n elemanlı sonlu cisim

$\mathbb{F}_q^{\,m}$: q bir asal sayı olmak üzere q elemanlı m uzunluğundaki vektörler kümesi

$(\mathbb{F}_q^{\,m})^n$: $x=(x_1,...,x_n)$ olmak üzere $1\le i\le n$ için $x_i=(x_{i,1},...,x_{i,m})$ şeklindeki vektörler kümesi

$GL(m,\mathbb{F}_2)$: Elemanları $\mathbb{F}_2$ 'den olan tüm $m\times m$ tipindeki regüler matrisler kümesi

$M_{b\times b}(\mathbb{F}_q)$: Elemanları q elemanlı sonlu cismin elemanları olan $b\times b$ tipindeki blok matrisler kümesi

$M_{bn\times bn}(\mathbb{F}_q)$: Elemanları q elemanlı sonlu cismin elemanları olan $b\times b$ tipindeki blok matrislere sahip olan $n\times n$ tipindeki matrisler kümesi

V : Vektör Uzayı

XOR : Exclusive Or

W^{-1} : W matrisinin ters matrisi

W^T : W matrisinin transpoz matrisi

ŞEKİLLER LİSTESİ

ÖZET

Anahtar kelimeler: MDS matris, Dallanma sayısı, Blok şifreler, Kriptografi, Eş matris, Dairesel matris, Blok matris

Bu tezin başında, tez boyunca gerekecek olan temel cebirsel, lineer cebirsel ve kodlama teorisinin temellerini oluşturan tanımlamalara, önermelere ve ayrıca kriptoloji hakkında kısa bilgilere yer verilmiştir. Sonraki bölümde MDS matrislerin kriptoloji alanındaki önemi ve MDS matrisleri oluşturmak için yapılan çalışmalar hakkında bilgiler verilmiş olup bu çalışmalardan bazıları hakkında örnek teşkil etmesi açısından bahsedilmiş ve örnekler verilmiştir. Son bölümde 5×5 tipindeki dairesel matrislerin tersi kendisi olma ve MDS olma özelliği için izlenen yol gösterilmiştir. Daha sonra ise bu yola benzer şekilde 7×7 tipindeki dairesel matrislerin tersi kendisi olma ve MDS olma özelliklerine bakılmıştır.

CONSTRUCTION OF MDS MATRICES FROM SOME SPECIAL MATRICES

SUMMARY

Keywords: MDS Matrix, Brunch Number, Block Ciphers, Cryptography, Companion Matrix, Circulant Matrix, Block Matrix

In the beginning of this thesis, it is given basic definitions and theorems about algebraic, linear algebraic, coding theorotical concepts and also cryptology. In the next chapter, it is given information about the importance of MDS matrices in cryptology and the works done to construction MDS matrices. Some of these works have been mentioned and given examples. In the last chapter, it is shown how to construct of 5×5 circulant involutory MDS matrices. Then, in a similar way, involution and MDS properties of the 7x7 circulant matrices are examined.

BÖLÜM 1. GİRİŞ

1.1. Cebirsel Tanımlar

Tanım 1.1.1. x, y tamsayı ve z pozitif tamsayı olsun. Eğer z, $y-x$'i bölüyorsa bu durum $x \equiv y(\mathrm{mod}\, z)$ şeklinde yazılabilir ve bu ifadeye denklik denir. Ayrıca x, y'ye $(\mathrm{mod}\, z)$'ye göre denktir denir ve z tamsayısına da modulo denir [1].

Tanım 1.1.2. A bir küme olsun. A üzerinde tanımlı bir ikili işlem, $*: A \times A \to A$ bir fonksiyonudur. Eğer $(a,b) \in A \times A$ ise, A kümesinin tek bir elemanı (a,b) elemanına karşılık gelir ve $a * b$ ile gösterilir [2].

Tanım 1.1.3. $(A,*)$ üzerinde $*$ ikili işleminin tanımlandığı bir cebirsel yapı olsun.

1) $\forall a,b,c \in A$ için eğer $(a*b)*c = a*(b*c)$ ise, $*$ birleşmelidir.
2) $\forall a,b \in A$ için eğer $a*b = b*a$ ise, $*$ değişmelidir [2].

Tanım 1.1.4. G, $*$ ikili işlemi altında kapalı bir küme olsun. $(G,*)$ cebirsel yapısı aşağıdaki aksiyomları sağlıyorsa, $(G,*)$ bir *gruptur*.

1) $\forall a,b,c \in G$ için $(a*b)*c = a*(b*c)$ sağlanır. Yani $*$ işlemi G'de *birleşmelidir*.
2) $\forall x \in G$ için, öyle bir $e \in G$ vardır ki; $e*x = x*e = x$ sağlanır. e'ye G grubunun $*$ işlemine göre *birim* elemanı denir.
3) $\forall a \in G$ için, öyle bir $a' \in G$ vardır ki; $a*a' = a'*a = e$ sağlanır. a', a elemanının *tersi* denir.

Eğer $(G,*)$ grubu aşağıdaki özelliği de sağlıyorsa, G grubuna değişmeli grup denir. $\forall a,b \in G$ için $a*b = b*a$ sağlanır. Yani $*$ işlemi G'de *değişmelidir* [3].

Tanım 1.1.5. R boştan farklı bir küme ve bu küme üzerinde tanımlı ikili işlem + ve . olsun. Aşağıdaki aksiyomları sağlayan $(R,+,.)$ cebirsel yapısına bir halka denir.

1) $(R,+)$ bir değişmeli gruptur.
2) $\forall a,b,c \in R$ için $(a.b).c = a.(b.c)$ dir. Yani, . işleminin R'de birleşme özelliği vardır.
3) $a.(b+c) = a.b + a.c$ ve $(a+b).c = a.c + b.c$ dir. Yani, . işleminin + işlemi üzerine sağdan ve soldan dağılma özelliği vardır [4].

Tanım 1.1.6. R bir halka olsun. $\forall a,b \in R$ için $a.b = b.a$ ise R'ye değişmeli bir halka denir. Ayrıca $\forall a \in R$ için $1_R.a = a.1_R = a$ olmak üzere $1_R \in R$ mevcutsa R'ye birimli bir halka ve 1_R' ye de halkanın birim elemanı denir [4].

Tanım 1.1.7. R birimli ve değişmeli bir halka, $R - \{0_R\} = R^*$, ikinci işleme göre bir grup ise R'ye bir cisim denir [5].

Tanım 1.1.8. Eğer bir cisim sonlu elemana sahipse bu cisme sonlu cisim denir [1].

Teorem 1.1.1. q asal sayı ise $\mathbb{Z}_q$'ya bir cisim denir. [1].

Teorem 1.1.2. $\mathbb{Z}^*_q$, $\mathbb{Z}_q$'nun bir alt kümesi olup, çarpmaya göre tersi olan elemanları içerir ve ayrıca q asal ise $\mathbb{Z}^*_q$'a devirli grup denir[1].

Tanım 1.1.9. $\mathbb{Z}_q$ bir cisim olsun. $0 \neq \alpha \in \mathbb{Z}_q$ için α elemanının derecesi $\alpha^t = 1$ olacak şekilde en küçük t değeridir [1].

Tanım 1.1.10. Bir α elemanı $\bmod q$'ya göre $(q-1)$ derecesine sahip ise bu α elemanına ilkel (asal ya da primitive) eleman denir [1].

Teorem(Euler Teoremi) 1.1.3. $n \in \mathbb{Z}$ olsun. $(a,n)=1$ olan $\forall a \in \mathbb{Z}$ için $a^{\phi(n)} \equiv 1 (\mathrm{mod}\, n)$ veya $\overline{a}^{\phi(n)} = \overline{1}$ dir [5].

Teorem 1.1.4. $\phi(n)$, n sayısının asal çarpanların üsleri şeklinde yazılması ile elde edilebilir. n ve $\phi(n)$, q_i'ler farklı asal sayılar olacak şekilde $e_i > 0$ ve $1 \le i \le m$ için aşağıdaki şekilde gösterilir [1].

$$n = \prod_{i=1}^{m} q_i^{e_i} \ , \ \phi(n) = \prod_{i=1}^{m} (q_i^{e_i} - q_i^{e_i - 1})$$

Tanım 1.1.11. q bir asal sayı ve α'da $\mathrm{mod}\, q$'ya göre bir ilkel eleman olsun. Bu durumda $\exists \beta \in \mathbb{Z}^*_q$, $\beta = \alpha^i$ $(0 < i < q-2)$ olacak şekilde yazılabilir. $\beta = \alpha^i$'nin derecesi $\dfrac{q-1}{OBEB(q-1,i)}$ dir. O zaman $OBEB(q-1,i)=1$ ise β ilkel elemandır. Dolayısıyla $\mathrm{mod}\, q$'ya göre ilkel elemanların sayısı $\phi(q-1)$ dir [1].

Teorem 1.1.5. q bir asal sayı, $\alpha \in \mathbb{Z}^*_q$ olsun. O zaman $(q-1)$'i bölen bütün asal p değerleri için $\alpha^{\frac{q-1}{p}} (\mathrm{mod}\, q) \neq 1$ ise α'ya $\mathrm{mod}\, q$'ya göre ilkel eleman denir. [1].

Örnek 1.1.1. $q=13$ için ilkel elemanlar bulunsun. İlkel elemanların elde edilebilmesi için ilk olarak en küçük ilkel elemanın bulunması gerekir. Burada $q=13$ için en küçük ilkel eleman 2 dir. Bu durumda elde edilen en küçük ilkel eleman ile 1'den $q-1$'e kadar olan tüm tamsayılar aşağıdaki gibi elde edilir.

$2^0 \bmod 13 = 1$ $\qquad$ $2^6 \bmod 13 = 12$
$2^1 \bmod 13 = 2$ $\qquad$ $2^7 \bmod 13 = 11$
$2^2 \bmod 13 = 4$ $\qquad$ $2^8 \bmod 13 = 9$
$2^3 \bmod 13 = 8$ $\qquad$ $2^9 \bmod 13 = 5$
$2^4 \bmod 13 = 3$ $\qquad$ $2^{10} \bmod 13 = 10$
$2^5 \bmod 13 = 6$ $\qquad$ $2^{11} \bmod 13 = 7$

Daha sonra $OBEB(q-1,i)=1$ koşulunu sağlayan i değerleri bulunur. Bulunan bu i değerlerinin $2^i \bmod q$'da karşılık gelen değerleri ilkel elemanlar olacaktır. Verilen bu örnekte $OBEB(i,12)=1$ için i değerleri sırasıyla 1,5,7,11 dir. Bu durumda bu değerlerin sırasıyla $2^i \bmod q$'da yerine yazılmasıyla elde edilen ilkel elemanlar sırasıyla 2,6,11,7 olarak bulunur. Bu ilkel elemanlara cismin üreteci denir. Dolayısıyla $q=13$ için 2,6,11 ve 7 üreteç elemanları ile sonlu cisim oluşturulabilir.

$6^0 \bmod 13=1$	$7^0 \bmod 13=1$	$11^0 \bmod 13=1$
$6^1 \bmod 13=6$	$7^1 \bmod 13=7$	$11^1 \bmod 13=11$
$6^2 \bmod 13=10$	$7^2 \bmod 13=10$	$11^2 \bmod 13=4$
$6^3 \bmod 13=8$	$7^3 \bmod 13=5$	$11^3 \bmod 13=5$
$6^4 \bmod 13=9$	$7^4 \bmod 13=9$	$11^4 \bmod 13=3$
$6^5 \bmod 13=2$	$7^5 \bmod 13=11$	$11^5 \bmod 13=7$
$6^6 \bmod 13=12$	$7^6 \bmod 13=12$	$11^6 \bmod 13=12$
$6^7 \bmod 13=7$	$7^7 \bmod 13=6$	$11^7 \bmod 13=2$
$6^8 \bmod 13=3$	$7^8 \bmod 13=3$	$11^8 \bmod 13=9$
$6^9 \bmod 13=5$	$7^9 \bmod 13=8$	$11^9 \bmod 13=8$
$6^{10} \bmod 13=4$	$7^{10} \bmod 13=4$	$11^{10} \bmod 13=10$
$6^{11} \bmod 13=11$	$7^{11} \bmod 13=2$	$11^{11} \bmod 13=6$

Tanım 1.1.12. R bir halka, x bir bilinmeyen ve $a_0, a_1, ..., a_k$'lar R'nin elemanları olmak üzere,

$$a_0 + a_1 x + ... + a_k x^k$$

şeklindeki bir ifadeye R'den katsayılı bir polinom denir. R'den katsayılı tüm polinomlar kümesi $R[x]$ ile gösterilir [5].

Tanım 1.1.13. R bir halka olsun. Bütün katsayıları sıfır olan polinoma sıfır polinom denir. R nin her bir elemanıda bir polinom olarak düşünülebilir. Bu polinomlara sabit polinom denir [5].

Tanım 1.1.14. F bir cisim ve f , F 'de bir polinom olsun. $a_i \in F$ olmak üzere, $f(x) = \sum_{i=0}^{n} a_i x_i$ yazılsın. $a_n = 1$ olması durumunda f polinomuna monik polinom denir [6].

Tanım 1.1.15. F bir cisim ve $F[x]$ bir polinom kümesi olsun. Bir $p \in F[x]$ polinomu pozitif bir dereceye sahip ise ve $b, c \in F[x]$ polinomları için $p = b.c$ olmak üzere b ya da c polinomlarından herhangi biri sabit bir polinom ise o zaman $p \in F[x]$ polinomuna F üzerinde indirgenemez (yada $F[x]$'de indirgenemez (irreducible)) polinom denir. F üzerinde indirgenebilen $F[x]$'deki pozitif dereceli bir polinoma F üzerinde indirgenebilir (reducible) polinom denir [7].

Tanım 1.1.16. F bir cisim $S \subset F$ olsun. S kendi başına F cismindeki işlemlere göre bir cisim ise S 'ye F 'nin alt cismi denir [5].

Tanım 1.1.17. Kendinden başka hiç bir alt cismi bulunmayan bir cisme asal cisim denir [5].

Tanım 1.1.18. F cismi bir K cisminin alt cismi ise K'ya, F 'nin bir genişlemesi denir [5].

1.2. Lineer Cebirsel Tanımlar

Tanım 1.2.1. F cismi üzerinde tanımlı elemanları vektörler olan V kümesi aşağıdaki aksiyomları sağlıyorsa V kümesine vektör uzayı denir .

1) V kümesi toplama işlemine göre değişmeli bir gruptur.
2) $\forall a \in F$ ve $u \in V$ için $au \in V$ dir.
3) $\forall a, b \in F$ ve $\forall u, v \in V$ için $a(u+v) = au + av$ ve $(a+b)v = av + bv$ dir.
4) $\forall a \in F$ ve $\forall u \in V$ için $(ab)u = a(bu)$ dur.
5) $\forall u \in V$ için $1u = u$ dur [8].

Tanım 1.2.2. V bir vektör uzayı ve $0 \neq W \subset V$ olsun. Eğer W, vektör uzayının bütün aksiyomlarını sağlıyorsa W'ya V'nin bir alt uzayı denir [8].

Teorem 1.2.1. V bir vektör uzayı ve $0 \neq W \subset V$ olsun. W, aşağıdaki aksiyomları sağlıyorsa V vektör uzayının bir alt uzayıdır.

1) $\forall x, y \in W$ için $x + y = W$ dır.
2) $\forall a \in F$ için $ax \in W$ dır [8].

Tanım 1.2.3. r_i'ler skaler olmak üzere, n tane $v_1, v_2, ..., v_n$ vektörlerinin lineer birleşimi

$$v = r_1 v_1 + r_2 v_2 + ... + r_n v_n$$

şeklindedir. Eğer $A = \{v_1, v_2, ..., v_n\}$ ise A kümesinin bütün lineer birleşimlerinin kümesi $Sp(A)$ ile ifade edilmektedir. Ayrıca $Sp(A)$, V vektör uzayının bir alt uzayıdır [8].

Tanım 1.2.4. $A = \{v_1, v_2, ..., v_n\}$ olsun. $Sp(A)$, A kümesinin bütün lineer birleşimlerinin kümesi olmak üzere, $Sp(A)$ uzayına A kümesinin gerdiği (ürettiği) alt uzay denir. A kümesine de $Sp(A)$ alt uzayının bir üreteci denir [8].

Tanım 1.2.5. V vektör uzayında $v_1, v_2, ..., v_n$ vektörleri verilsin. Eğer, $r_1 v_1 + r_2 v_2 + ... + r_n v_n = 0$ olacak şekilde en az biri sıfırdan farklı olan $r_1, r_2, ..., r_n$ sayıları varsa $\{v_1, v_2, ..., v_n\}$ vektörlerinin kümesi lineer bağımlıdır denir. Eğer, $r_1 v_1 + r_2 v_2 + ... + r_n v_n = 0 \Rightarrow r_1 = r_2 = ... = r_n = 0$ ise lineer bağımsızdır denir [9].

Tanım 1.2.6. V bir vektör uzayı ve $A=\{v_1,v_2,...,v_n\}$ olsun. Eğer A kümesi aşağıdaki koşulları sağlıyorsa A'ya V 'nin bir tabanı veya bazı denir.

1) A kümesi lineer bağımsızdır.
2) A kümesi V 'yi gerer [9].

Tanım 1.2.7. V vektör uzayının herhangi bir tabanındaki vektörlerinin sayısına V 'nin boyutu denir [8].

Tanım 1.2.8. V ve W aynı K cismi üstünde vektör uzayları ve L, V uzayından W uzayına bir fonksiyon olsun. L fonksiyonu aşağıdaki özellikleri doğrularsa L'ye lineer dönüşüm adı verilir.

1) $\forall u,v\in V$ için $L(u+v)=L(u)+L(v)$,
2) $\forall c\in K$ ve $\forall u\in V$ için $L(cu)=cL(u)$ [10].

Tanım 1.2.9. $L:V\to W$ lineer bir dönüşüm olsun. $L(V)$ alt uzayı sonlu boyutlu ise bu uzayın boyutuna, L lineer dönüşümünün rankı denir ve bu sayı $rankL$ biçiminde gösterilir [10].

Tanım 1.2.10. $X=\{1,2,...,m\}$ ve $Y=\{1,2,...,n\}$ olsun. K, reel sayı cismini veya karmaşık sayı cismini göstermek üzere üstünde $X\times Y$ kümesinden K cismine giden bir fonksiyona, K cismi üstünde $m\times n$ tipinde bir matris denir [10].

Tanım 1.2.11. Bir matrisin bütün satır ve sütunları birbirinden doğrusal olarak bağımsız ise (lineer bağımsız ise) bu durumda bu matrise tam ranklı bir matris denir [11].

Tanım 1.2.12. Bir A kare matrisinin çarpmaya göre tersi yoksa bu matrise tekil (singüler) matris denir. A matrisinin çarpmaya göre tersi varsa bu durumda A matrisine tersinir (regüler ya da nonsingüler) matris denir [10].

Tanım 1.2.13. A, $n\times n$ biçiminde bir matris olsun.

$$f_A = \det(x\mathrm{I} - A)$$

eşitliği ile tanımlı f_A polinomuna, A matrisinin karakteristik polinomu denir [10].

Tanım 1.2.14. Bir A matrisinin minimal polinomu $m(A)=0$ olacak şekildeki en küçük dereceli monik polinomdur ve $m_A(x)$ şeklinde gösterilir [12].

Teorem 1.2.2. (Cayley-Hamilton Teoremi) Her kare matris kendi minimal polinomunu sağlar [12].

Tanım 1.2.15. (Alt Matris) Bir $A=(a_{ij})_{m\times n}$ matrisinde, k tane satır ve l tane sütun çıkarıldığında elde edilen $(m-k)\times(n-l)$ tipindeki yeni matrise A matrisinin alt matrisi denir [13].

Tanım 1.2.16. (Blok Matris) Bir $A=\begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & a_{m3} & a_{mn} \end{pmatrix}$ matrisi,

$r_1+r_2+\ldots+r_p=m$, $s_1+s_2+\ldots+s_q=n$ ve $(k=1,2,...,p\,;\ l=1,2,...,q)$ için $A_{kl}=(a_{ij})_{r_k\times s_l}$ ' ler A 'nın alt matrisleri olmak üzere $\begin{pmatrix} A_{11} & A_{12} & \dots & A_{1q} \\ A_{21} & A_{22} & \dots & A_{2q} \\ \vdots & \vdots & \vdots & \vdots \\ A_{p1} & A_{p2} & \dots & A_{pq} \end{pmatrix}$

şeklinde yazılabilir. Bu yazım şekline A matrisinin bloklara ayrılması denir [13].

Tanım 1.2.17. (Dairesel Matrisler) Her satır vektörünün bir önceki satır vektörüne göre bir elemanla döndürülmesi ile elde edilen $k\times k$ tipindeki bir matrise dairesel matris denir [14].

Tanım 1.2.18. (Eş (companion) Matrisler) $a(x) = a_0 + a_1 x + ... + a_{n-1} x^{n-1} + x^n$ monik polinomu için bir eş matris,

$$A = \begin{pmatrix} 0 & \dots & \dots & 0 & -a_0 \\ 1 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & \ddots & \vdots & -a_2 \\ \vdots & \ddots & \ddots & 0 & \vdots \\ 0 & \dots & 0 & 1 & -a_{n-1} \end{pmatrix}$$

şeklinde olan ve son sütunu $a(x)$ polinomunun kat sayıları ile oluşturulan $n \times n$ tipindeki bir kare matristir [15].

1.3. Lineer Kodlar

Tanım 1.3.1. $A = \{a_1, a_2, ..., a_q\}$ sonlu bir küme olsun. Bu kümeye alfabe yada q-lu alfabe denir. A^n ise A kümesinden alınan n-lileri temsil etsin. Bu durumda A^n kümesine sözler ailesi denir. A^n'nin herhangi bir C alt kümesine q-lu blok kodu, C'nin elemanlarına da kodsöz denir. $C \subset A^n$'nin M tane elemanı varsa C'ye, n uzunluğunda M elemanlı bir kod denir ve (n, M) ile gösterilir [16].

Tanım 1.3.2. x ve y aynı uzunlukta ve aynı alfabe üzerinde tanımlanmış n-liler olsun. x ve y'nin farklı bileşenlerinin sayısına, x ile y arasındaki Hamming uzaklık denir. $d(x, y)$ ile gösterilir [16].

Tanım 1.3.3. $d(C) = \min_{x,y \in C, x \neq y} d(x, y)$ sayısına C kodunun minimum uzaklığı denir. n uzunluğunda M elemana sahip ve minimum uzaklığı d olan bir kod (n, M, d) ile gösterilir [16].

Tanım 1.3.4. Bir $x=(x_1,x_2,...,x_n)$ vektörünün sıfırdan farklı elemanlarının sayısı x vektörünün Hamming ağırlığını verir. $w(x)$ ile gösterilir. Buradan, $d(x,y)=w(x-y)$ olduğu görülür [16].

Tanım 1.3.5. Bir C kodunun sıfırdan farklı kodsözlerinin ağırlıklarının en küçüğüne o kodun minimum ağırlığı denir [16].

Tanım 1.3.6. $C\subset V(n,q)$ alt kümesi $V(n,q)$ vektör uzayının bir alt uzayı ise C'ye bir lineer kod denir. C'nin boyutunun k olması durumunda C'ye $[n,k]$-kodu denir. C kodunun minimum uzaklığı d ise C'ye $[n,k,d]$-kodu denir [16].

Teorem 1.3.1. C bir lineer kod ise $d(C)=w(C)$ dir [16].

Tanım 1.3.7. C bir $[n,k]$-kodu olsun. Satırları C kodunun bazlarından oluşan $k\times n$ tipinde bir D matrisine C'nin bir üreteç matrisi denir [16].

Teorem 1.3.2. F_q cismi üzerinde bir $[n,k,d]$-kodu verildiğinde, ilk k sütunu k boyutlu I_k birim matris olan $G=[I_k\,|\,A]$ standart formdaki üreteç matrisine sahip bir koda denktir [16].

Tanım 1.3.8. $[n,k,d]$ parametreli bir C lineer kodu $k+d=n+1$ şartını sağlarsa böyle bir koda maksimum uzaklığa ayrılabilen (MDS) kod denir [17].

Tanım 1.3.9. $GF(2^m)$ sonlu cismi üzerinde $M=(\mathrm{I}_r\,|\,A)$ matrisi tarafından üretilen bir C kodu MDS ise $GF(2^m)$'den katsayılı r-boyutlu bir kare A matrisi de MDS dir [18].

Teorem 1.3.3. A, $k \times n-k$ tipinde bir matris olmak üzere $G=[\mathrm{I}|A]$ üreteç matrisine sahip olan bir C $[n,k,d]$ kodunun MDS olması için gerek ve yeter şart A 'nın her kare alt matrisinin regüler olmasıdır [19].

Teorem 1.3.4. C kodu $G=\left[I_k \mid A\right]$ standart formdaki üreteç matrisine sahip $[n,k]$ parametreli lineer bir kod ise C'nin dik tümleyeni ($C^{\perp}$) de $H=\left[-A^T \mid I_{n-k}\right]$ üreteç matrisine sahip bir $[n,n-k]$ lineer kod olur. H matrisine C kodunun kontrol matrisi denir [16].

Tanım 1.3.10. (Yığın (Bundle)) $\mathbb{F}$, q elemanlı sonlu bir cisim olsun. $\exists b,n$ pozitif tam sayıları için $y \in \mathbb{F}_q^{bn}$ olsun. Burada y vektörü $i=1,...,n$ için $y_i \in \mathbb{F}_q^b$, $y_i=(y_{i,1},...,y_{i,b})$ olmak üzere $y=(y_1,...,y_n)$ olacak şekilde n parçaya ayrılabilir. O zaman $\forall y_i$ değeri y vektörünün bir yığını olarak adlandırılır [20].

Tanım 1.3.11. $\mathbb{F}$, q elemanlı sonlu bir cisim olsun. $y \in \mathbb{F}_q^{bn}$ vektörünün yığın ağırlığı onun sıfırdan farklı yığınlarının sayısı olarak tanımlanır ve $w_b(y)$ ile gösterilir [20].

Örnek 1.3.1. b = 2 ve n = 6 olmak üzere y = (101000100111) vektörü alınsın. Bu vektör y = (10,10,00,10,01,11) olacak şekilde 6 parçaya ayrılabilir. Buradaki her iki uzunluğundaki parça y vektörünün bir yığını olarak adlandırılır ve yığın ağırlığı $w_b(y)=5$ dir.

Tanım 1.3.12. $\mathbb{F}$, q elemanlı sonlu bir cisim olsun. $y,z \in \mathbb{F}_q^{bn}$ iki vektör olsun. y ve z arasındaki yığın uzaklığı $w_b(y-z)$ olarak tanımlanır ve $d_b(y,z)$ ile gösterilir. $w_b(y)$ (yığın ağırlığı) ve $w_H(y)$ (hamming ağırlığı) çoğu durumda farklıdır [20].

Örnek 1.3.2. b = 3 ve n = 3 olmak üzere x = (111110100) ve y = (100100100) şeklinde iki vektör olsun. x ve y vektörleri $x=(111,110,100)$ ve $y=(100,100,100)$

olacak şekilde yığınlara ayrılsın. Bu durumda bu vektörler için sırasıyla $w_b(y)$, $w_H(y)$ bakılsın.

x vektörü için $w_b(y)=3,\ w_H(y)=6$ dır.

y vektörü için $w_b(y)=3,\ w_H(y)=3$ dür.

Tanım 1.3.13. (Difüzyon Tabakası) $\mathbb{F}_2$-lineer dönüşümlere difüzyon tabakaları denir ve difüzyon tabakaları difüzyon matris olarak da adlandırılır [20].

Tanım 1.3.14. (Diferansiyel Dal Sayısı) $M_{bn\times bn}(\mathbb{F}_2)$, elemanları 2 elemanlı sonlu bir cismin elemanları olan , $b\times b$ tipinde blok matrislere sahip olan $n\times n$ tipindeki matrisler kümesi olsun. $R\in M_{bn\times bn}(\mathbb{F}_2)$ matrisi $\exists b,n$ pozitif tam sayıları için bir difüzyon tabakası olsun. R difüzyon tabakasının diferansiyel dal sayısı

$$B_d(R)=\min\{w_b(x)+w_b(R(x))\,\big|\,x\in\mathbb{F}_2^{bn},\ x\neq 0\}$$

olarak tanımlanmaktadır. x vektörü $\mathbb{F}_2^{bn}$' de bir satır vektörü olarak yazılırsa $R(x)=x.R$ olur [20].

Tanım 1.3.15. (Lineer Dal Sayısı) $M_{bn\times bn}(\mathbb{F}_2)$ elemanları 2 elemanlı sonlu bir cismin elemanları olan , $b\times b$ tipinde blok matrislere sahip olan $n\times n$ tipindeki matrisler kümesi olsun. $R\in M_{bn\times bn}(\mathbb{F}_2)$ matrisi $\exists b,n$ pozitif tam sayıları için bir difüzyon tabakası olsun. R difüzyon tabakasının lineer dal sayısı

$$B_l(R)=\min\{w_b(x)+w_b(R^T(x))\,\big|\,x\in\mathbb{F}_2^{bn},\ x\neq 0\}$$

olarak tanımlanmaktadır. x vektörü $\mathbb{F}_2^{bn}$' de bir satır vektörü olarak yazılırsa $R^T(x)=x.R^T$ olur [20].

Tanım 1.3.16. (MDS Difüzyon Tabakası) $(\mathbb{F}_2{}^m)^n$ üzerinde bir $n \times n$ matrisinin maksimum dal sayısı (branch number) $n+1$ dir. O zaman $R \in M_{bn \times bn}(\mathbb{F}_2)$ matrisi $\exists b, n$ pozitif tamsayıları için bir difüzyon tabakası olsun. Eğer $B_d(R) = n+1$ ise R matrisine bir MDS difüzyon matrisi (tabakası) denir [20].

1.4. Kriptoloji

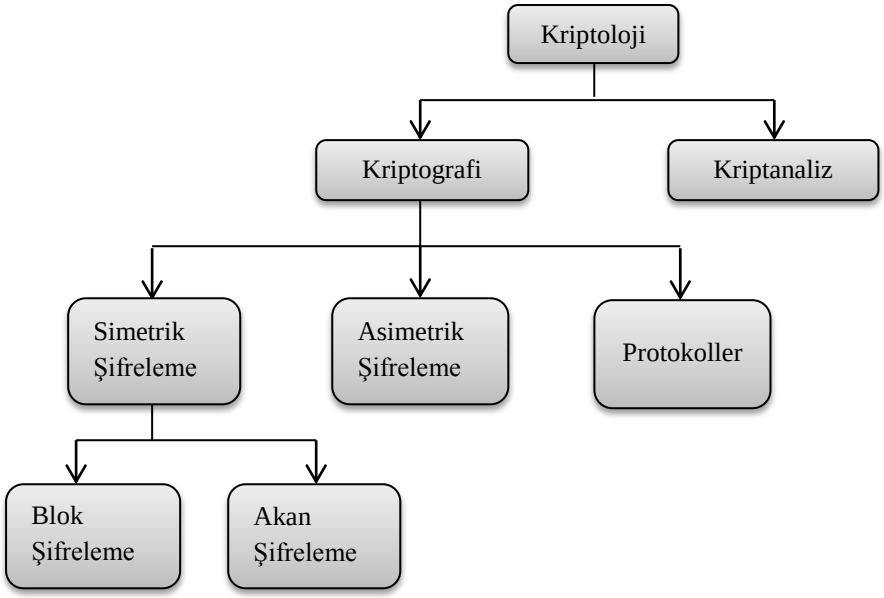
Daha geniş bilgi için [21,1] e bakılabilir. Kriptografi kelimesi duyulduğu zaman ilk olarak e-mail şifrelemesi, güvenli web site erişimi, banka uygulamaları için akıllı kartlar ya da 2. Dünya Savaşı boyunca Alman Enigma şifreleme makinesine karşı yapılan ünlü ataklar ve kod kırma gibi şeyler ile ilişkilendirilebilir.

Şekil 1.1. Alman enigma makinesi

Kriptografi kelimesi Yunanca gizli anlamına gelen “kryptos (kript)” ve yazı anlamına gelen “graphein (graf)” kelimelerinin türetilmesi ile oluşturulmuştur. Kriptografi, modern elektronik iletişimle yakından bağlantılı görünür. Fakat kriptografi oldukça eski bir iştir ve ilk örnekleri antik Mısır da standart olmayan ‘gizli’ hiyeroglif kullanıldığı zaman olan milattan önce yaklaşık 2000’li tarihlere kadar uzanır. Örneğin Antik Yunan da belirlenmiş gizli yazı durumları yani Spartalıların savaşlarda kullandığı ‘Scytale’ adlı gizli iletişim aracı ve antik Roma da kullanılan ünlü Sezar şifrelemesi vardır.

Şekil 1.2. Scytale

Kriptografi, Kriptolojinin alt dallarından biridir.



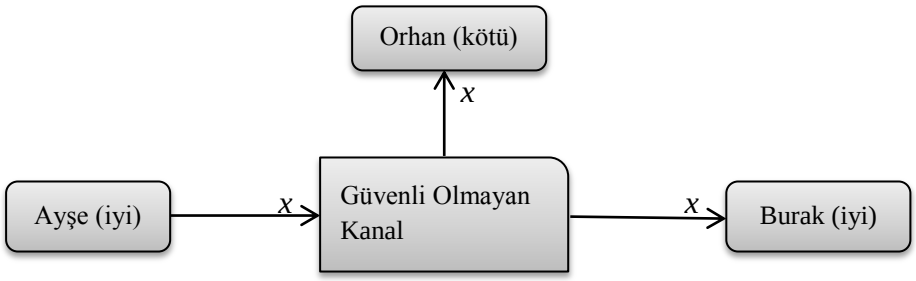
Şekil 1.3. Kriptoloji şeması

1.4.1. Kriptografi

Bir mesajın anlamını gizlemek amacıyla kullanılan bir gizli yazma bilimidir ve bilgi güvenliğini sağlayan matematiksel yöntemler bütünüdür. Bu yöntemler bir bilginin iletimi sırasında karşılaşılabilecek saldırılardan bilgiyi, göndereni ve alıcıyı korumayı amaçlar. Yani kriptografi, verinin güvenli bir şekilde iletilmesini sağlar. Bu yüzden güvenli bir şifreleme algoritmasının tasarımı kriptografi de çok önemlidir.

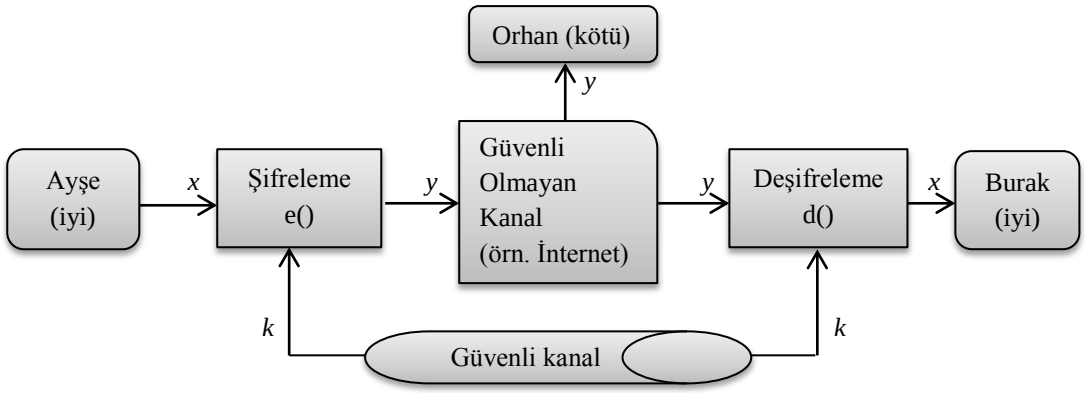
1.4.1.1. Simetrik şifreleme algoritmaları

Simetrik şifreleme verilecek olan örnekle en iyi şekilde açıklanabilir. Ayşe ve Burak güvenli olmayan bir kanal üzerinde iletişim kurmak isteyen iki kullanıcı olsun. Buradaki kanal terimi iletişim bağlantısı için genel bir terimdir. Bu kanal terimi yerine internet, wireless LAN iletişimi ya da herhangi diğer media iletişim türleri düşünülebilir. Asıl problem, örneğin bir Wi-Fi iletişiminin radyo sinyallerini dinleyerek yada bir internet yönlendiricisine saldırarak kanala erişim sağlamak isteyen kötü niyetli Orhan isimli bir kullanıcı ile başlar. Bu tip izinsiz dinlemeler gizli dinlemeler olarak adlandırılmaktadır. Açık olarak Ayşe ve Burak'ın, Orhan'ın dinleyemeyeceği şekilde iletişim kurabileceği pek çok durum vardır. Örneğin Ayşe ve Burak bir araba fabrikasında iki yetkili olsun ve onlar gelecek birkaç yılda yeni araba modellerinin tanıtımı için iş stratejisini içeren dokümanları göndersinler. Bu dokümanlar rakiplerinin eline ya da yabancı istihbarat ajanlarının eline geçmemelidir.



Şekil 1.4. Güvenli olmayan kanal üzerinde iletişim

Bu durumda, simetrik şifreleme güçlü bir çözüm sunar. Ayşe bir simetrik algoritma kullanarak onun mesajı *x*'i şifreler ve şifreli metin olan *y*'yi elde eder. Burak şifreli metini alır ve mesajı deşifreler. Eğer güçlü bir şifreleme algoritmasına sahip olunursa şifreli metin Orhan'a rastgele bir bilgi gibi gözükecek ve onun için yararlı olan herhangi bir bilgi içermeyecektir.



Şekil 1.5. Simetrik-anahtar kriptosistem

Şekil 1.5 deki *x*, *y* ve *k* değişkenleri kriptografi de önemlidir ve özel isimlere sahiptir:

1) *x*, şifresiz metin ya da açık metin olarak adlandırılmaktadır.
2) *y*, şifreli metin olarak adlandırılmaktadır.
3) *k*, anahtar olarak adlandırılmaktadır.
4) Tüm mümkün anahtarların kümesi anahtar uzayı olarak adlandırılmaktadır.

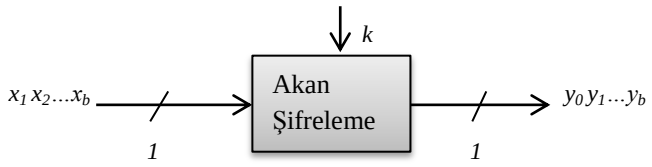
Ayşe ve Burak arasında anahtarın dağıtımı için güvenli bir kanala ihtiyaç vardır. Örneğin bu güvenli kanal Ayşe ve Burak arasında çanta taşıyan bir kişi olabilir fakat bu yöntem çok elverişsiz olur. Bu metodun çalıştığına dair iyi bir örnek, kablosuz yerel ağlarda Wi-Fi korumalı erişim şifrelemesinde kullanılan önceden paylaşılan anahtarlardır.

Diğer yandan önemli ve ayrıca da mantıksız olan bir olay hem şifreleme hem de deşifreleme algoritmalarının herkes tarafından bilinmesidir. Şifreleme algoritmasının gizli tutulması bütün sistemin kırılmasını daha da zorlaştırır. Fakat gizli algoritmalar ayrıca da test edilmeyen algoritmalar anlamına gelir. Bir şifreleme metodunun güçlü olup olmadığının bilinmesi için tek yol algoritmanın herkes tarafından bilinmesidir ve diğer kriptograflar tarafından analiz edilmesidir. Şifreleme algoritmaları herkes tarafından bilineceği için anahtarı elde eden biri için algoritmayı kırmak çok kolay olacaktır. Bu yüzden anahtarın iyi gizlenmiş olması gerekir. Buradan ise bir mesajı güvenli bir şekilde gönderme problemi, bir anahtarı gizli bir şekilde gönderme problemine dönüşecektir.

Simetrik şifrelemeler blok şifreler ve akan şifreler olmak üzere ikiye ayrılır.

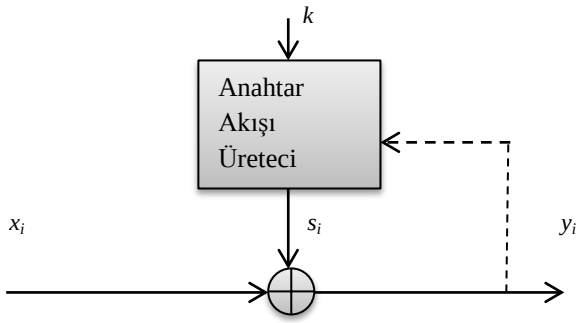
1.4.1.1.1. Akan şifreleme

Akan şifreleme her bir karakteri (bitleri) ayrı ayrı şifreler. Bu işlem, bir düz metinin her bir karakterine bir anahtar akışından (key stream) bir karakter (bit) ekleyerek gerçekleştirilir. Anahtar akışı sadece anahtara bağlı ise buna senkron akan şifrelemeler denir ve anahtar akışı ayrıca şifreli metine bağlı ise buna asenkron akan şifrelemeler denir.



Şekil 1.6. Bir akan şifreleme ile b bitlik şifreleme prensibi

Eğer Şekil 1.7 deki noktalı doğru parçası ile verilen kısım mevcutsa bu çeşit akan şifrelemelere asenkron akan şifrelemeler denir.

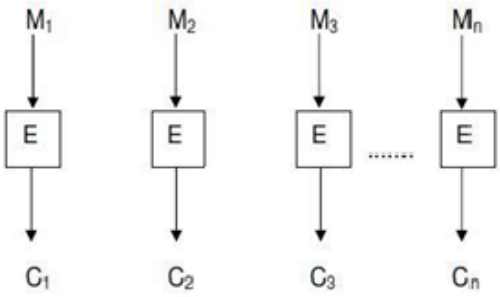


Şekil 1.7. Senkron ve asenkron akan şifreleme

1.4.1.1.2. Blok şifreleme

Blok şifreleme aynı anahtar ile düz metin bitlerinin bir bütün bloğunu aynı anda şifreler. Bu ise, verilen bir bloktaki herhangi düz metin bitinin şifrelenmesinin aynı bloktaki her diğer düz metin bitine bağlı olduğu anlamına gelir. Uygulamada, blok şifrelemelerin büyük çoğunluğu ya AES (gelişmiş şifreleme standartı) gibi 128 bit (16 byte) lik bir blok uzunluğuna sahiptir ya da DES (veri şifreleme standartı) veya 3DES gibi 64 bit (8 byte) lik bir blok uzunluğuna sahiptir. Şekil 1.8 de gösterilen

M_1,M_2,…,M_n düz metin bloklarının herbiri E şifreleme işleminden geçerek C_1, C_2,…,C_n şifrelenmiş metin blokları elde edilir.



Şekil 1.8. Blok şifreleme

1.4.1.1.2.1. S-kutuları (S-boxes)

Genellikle blok şifreleme algoritmalarında kullanılır ve blok şifrelemeler için önemli bir bileşendir. S-kutuları karma görevini üstlenirler ve şifre içerisinde hangi bit'in hangi bit ile yer değiştireceğini belirlerler. Algoritmanın lineer olmayan tek elemanıdır. Dolayısıyla güzel bir S-kutusunun seçilmesi şifrenin karmaşıklığını yani gücünü direkt etkilemektedir.

Blok şifreler ve akan şifreler karşılaştırılacak olursa;

1) Uygulamada, özellikle internet üzerinde şifrelenen bilgisayar iletişimi için blok şifreleme, akan şifrelemelerden daha sık kullanılmaktadır.
2) Akan şifreleme küçük ve hızlı olma eğiliminde olduğu için onlar özellikle küçük hesaplama kaynakları olan uygulamalar için örneğin cep telefonları ve diğer gömülü cihazlar için uygundur. Akan şifreleme için belirgin bir örnek, GSM cep telefonu standartının bir parçası olan ve ses şifrelemesi için kullanılan A5/1 şifresidir. Ancak bununla birlikte, akan şifrelemeler bazen ayrıca da internet trafiğini, özellikle de RC4 akan şifresini şifrelemek için kullanılmaktadır.
3) Bilindiği üzere akan şifrelemelerin blok şifrelemelerden daha verimli bir şekilde şifrelemeye eğilimli olduğu varsayılmaktadır. Yazılımı en iyi hale

getiren akan şifrelemeler için verimlilik, bir bitlik düz metini şifrelemek için onların daha az işlemci talimatına (ya da işlemci döngülerine) gerek duyması anlamına gelir. Donanımı en iyi hale getiren akan şifrelemeler için verimlilik, aynı veri hızındaki şifreleme için onların blok şifrelemelerden daha az kapıya (ya da daha küçük çip alanına) ihtiyaç duyması anlamına gelir. Ancak bununla birlikte, AES gibi modern blok şifreler ayrıca yazılım içinde çok verimlidir. Dahası, donanım için, çok kompakt akan şifrelemeler kadar verimli olan ayrıca PRESENT gibi son derece verimli blok şifrelemeler de vardır.

1.4.1.2. Asimetrik şifreleme algoritmaları

Asimetrik şifreleme algoritmalarında açık anahtar ve özel anahtar olmak üzere iki çeşit anahtar kullanılmaktadır. Asimetrik şifreleme ile iletişime geçecek taraflardan her birinin iki anahtarı mevcuttur. Bunlardan açık anahtar karşı tarafa iletilirken herkesin erişimine açıktır, özel anahtar ise kişiye özel olup sadece o kişinin erişiminde gizlidir. Bu anahtarlar birbirine matematiksel bir ilişkiyle bağlanmıştır. Asimetrik şifreleme algoritmalarına örnek olarak RSA, ECC ve ElGamal verilebilir. Temel olarak bir asimetrik şifreleme algoritması Şekil 1.9 ve Şekil 1.10 daki gibi çalışır.

Şekil 1.9. Açık anahtar ile asimetrik şifreleme

Şekil 1.10. Gizli anahtar ile asimetrik şifreleme

1.4.1.3. Protokoller

Kripto protokoller, kriptografik algoritmaların uygulanması ile ilgilenir. Simetrik ve asimetrik algoritmalar, güvenli internet iletişimi gibi uygulamaların gerçekleştirilebildiği yapı taşları olarak görülebilir.

Her Web tarayıcısında kullanılan Aktarım Katmanı Güvenliği (TLS) şeması kriptografik protokole bir örnektir. Açıkçası hash fonksiyonları algoritmaların üçüncü sınıfını oluşturur. Fakat aynı zamanda onlar simetrik şifrelemeler ile bazı özellikleri paylaşır. Uygulama sistemlerinde kriptografik uygulamaların çoğunda simetrik ve asimetrik algoritmalar (ve çoğu zaman hash fonksiyonları) tamamen birlikte kullanılmaktadır ve bu bazen hibrit şemalar olarak bahsedilmektedir. Her iki algoritma grubunun kullanılmasının amacı her ikisinin de belirli bir güce ve zayıflığa sahip olmasıdır.

1.4.1.4. Hash algoritmaları

Veri bütünlüğü ve kimlik doğrulama gibi uygulamalarda kullanılan Hash algoritmaları, değişik uzunluktaki bit dizilerini sabit uzunluklu bit dizilerine taşır. Kolay hesaplanabilen hash algoritmaları için gönderilecek mesajdan matematiksel yollarla sabit uzunlukta sayısal bilgi üretme işlemidir denilebilir. Üretilen bu anlamsız bilgiye mesaj özeti (hash değeri) denir. Hash algoritmaları geri dönüşümü olmayan, tek yönlü algoritmalardır. Algoritmada amaçlanan, aynı özeti veren iki farklı mesajın bulunmasının mümkün olmamasıdır.

1.4.2. Kriptanaliz

Kriptosistemlerin güvenliğini test eden bilimdir ve modern kriptosistemler için merkezi bir öneme sahiptir. Kripto metodlarını kırmayı deneyen insanlar olmaksızın kriptosistemlerin güvenli olup olunmadığı bilinemez. Bu yüzden kriptoanaliz bir kriptosistemin güvenliğini garanti etmenin tek yolu olduğu için kriptolojinin ayrılmaz bir parçasıdır.

Blok şifrelemeler çoğu şifrelemede inşa edilen en önemli yapı bloklarından biridir. Modern blok şifrelemeler çeşitli döngülerin sık sık tekrarlanmasıdır ve her döngü bir konfüzyon (karıştırma) tabakası ve bir difüzyon (yayılma) tabakasından oluşmaktadır. Matematiksel bakış açısından difüzyon tabakaları lineer fonksiyonlar ile oluşturulurken konfüzyon tabakaları genellikle non lineer (S-boxes) fonksiyonlarla oluşturulmaktadır. Difüzyon tabakaları hash fonksiyonları gibi diğer şifreleme ilkellerinde de olduğu gibi blok şifrelemelerde önemli bir rol oynar.

Bir yandan difüzyon tabakaları diferansiyel şifrelemeler ve lineer şifrelemeler gibi blok şifrelemeler üzerinde iyi bilinen ataklara karşı direnç sağlarken diğer yandan büyük ölçüde uygulamaların verimliliğini etkiler. Ayrıca lineer difüzyon tabakaları simetrik şifreleme algoritmaları için iç bağımlılık sağlayan simetrik şifrelemenin önemli bir bileşenidir. Bir difüzyon tabakasının performansı dal sayısı ile ölçülür. Şifrelemede bir difüzyon tabakasının dal sayısı ne kadar büyük olursa diferansiyel ataklara ve lineer ataklara karşı o kadar daha iyi olacaktır. Sınırlı kaynaklı bir çevrede güvenliği sağlamayı amaçlayan hafif-siklet şifrelemelerde bir lineer difüzyon tabakasını uygulamanın maliyeti ayrıca önemlidir ve hafif-siklet şifrelemelerin hızlı bir gelişimi ile daha büyük dal sayılı hafif-siklet lineer difüzyon tabakası inşa etme problemini araştırmak özel bir ilgi alanı olmuştur.

Lineer bir difüzyon tabakası $(\mathbb{F}_2{}^m)^n$ üzerinde lineer bir dönüşümdür ve ayrıca bir difüzyon matrisi olarak da adlandırılabilir. Burada m, bir S-kutusunun bit uzunluğudur ve n, lineer difüzyon tabakasının etki gösterdiği S-kutularının sayısıdır. Her lineer dönüşüm bir matris ile temsil edilebilir. O zaman lineer bir difüzyon tabakası genellikle bir $n \times n$ tipinde matris olarak temsil edilir ve matrisin girdileri $\mathbb{F}_2{}^m$ üzerinde lineer dönüşümler olarak görülebilir. $(\mathbb{F}_2{}^m)^n$ üzerinde bir $n \times n$ matrisinin maksimum dal sayısı (branch number) $n+1$ dir. Maksimum dal sayılı bir lineer difüzyon tabakasına mükemmel difüzyon tabakası ya da maksimum uzaklığa ayrılabilen (MDS) matrisler denir [29].

BÖLÜM 2. MDS MATRİSLER

Belirli miktarda güvenliği sağlamak için gerekli olan alanı küçültmede MDS matrislerin seçimi önemli bir rol oynar. MDS matrisleri inşa etmenin çeşitli yolları vardır. Bunlardan bazılarına bakılacak olursa [18,22,23] de tekrarlı (recursive) tarzda MDS matrisler verilmiştir. Bu yapı genellikle matris hesaplamaları için gerekli olan geçici hafızayı ve donanım alanını büyük ölçüde azaltır. Bu tekrarlı matrisler alan kazandırmada iyi bir yol olsa da matrisi uygulamak için artan döngü sayıları bir maliyet getirir. Diğer yandan büyük MDS matrislerin tasarımı için iki popüler bir yaklaşım vardır bunlardan biri [24,25] de kullanılan Cauchy matrisleridir diğeri ise [14,26,27] de kullanılan Vandermonde matrislerdir. Ayrıca [28] de hafif-siklet uygulamalar için uygun eş matrisler kullanarak da bazı MDS matrisler inşa edilmiştir.

Alan kazanmada bir MDS matris için ilginç olan diğer bir özellik matrisin tersinin kendisine eşit (involution) olmasıdır. Bu durumda böyle bir özelliğe sahip olan MDS matrisin kendisi, tersine eşit olacaktır. Bu ise şifreleme ve deşifreleme aşamasında sadece matrisin kendisinin kullanılması anlamına geleceğinden büyük bir fayda sağlayacaktır. MDS matrisi inşa etmenin ortak bir yolu sonlu cisimler üzerinde MDS kodlar kullanmaktır. Sonlu cisim elemanları ile çarpma yapmak sonlu cisim üzerindeki bir matrisin değerlendirilmesinde temel bir işlemdir. Genellikle bu işlem bilgisayar uygulamasında verimlilik bakımından ağır kalır. Uygulamanın verimliliğini (hız, kullanım alanı v.s.) artırmak için bir matris daha az sayıda farklı sonlu cisim elemanlarıyla inşa edilmelidir ve seçilen sonlu cismin elemanları düşük hamming ağırlığına sahip olmalıdır. Bu yüzden bazı matrisler dairesel matrislerde ve Hadamard matrislerde olduğu gibi az sayıda elemanlarla tanımlanabilir. Bu dairesel matrisler [29] da farklı bir yolla araştırılmıştır. Bu yolu esas alarak [30] da en hafif MDS matrisler araştırılmıştır. Son zamanlarda sonlu cisimler üzerindeki elemanlarla

çarpmayı hesaplamak için kullanılan indirgenemez polinomun seçimi de verimlilik bakımından büyük bir etkiye sahip olmuştur. Bu durum ise uyumlu matrisin bir satırını değerlendirmek için gerekli olan az sayıda XOR işlemine sahip hafif-siklet MDS matrisleri araştırmak için algoritmaların tasarlandığı [31] de araştırılmıştır. [20] de ise $\mathbb{F}_2$ sonlu cismi üzerinde blokların tümü belirli bir ilkel bloğun polinomları olan bir tür MDS difüzyon blok matrisleri açıklamak için yeni bir metod önerilmiştir ve difüzyon matrislerin MDS özelliğini devam ettiren yeni bir tür dönüşüm keşfedilip verilen bir MDS matristen bir seri yeni MDS matrisler üretilmiştir. Ayrıca bu tür dönüşümden bir denklik bağıntısı elde edilip MDS matrisleri araştırırken hesaplama miktarı büyük ölçüde azaltılmıştır.

Verilen bu bilgilerden sonra [20],[18],[28] numaralı çalışmalar örnek teşkil etmesi açısından sırasıyla biraz daha ayrıntılı şekliyle verilecektir. Bu bölümde verilecek olan tüm tanım, teorem, yardımcı teorem, önerme, durum ve sonuçlar için sırasıyla [20], [18] ve [28] numaralı çalışmalara bakılabilir.

2.1. Blok Şifreler ve Hash Fonksiyonları için Bir Tür MDS Blok Difüzyon Matrislerinin İnşası

Burada F cismi üzerindeki tüm $(s\times t)$ tipindeki matrislerden oluşan küme $M_{s\times t}(F_q)$ ile gösterilir. q asalın bir kuvveti olmak üzere $\mathbb{F}_q$, q elemanlı sonlu bir cisim olsun. V 'de n boyutlu $\mathbb{F}_q$ lineer uzay olsun. V üzerindeki her $\mathbb{F}_q$ lineer dönüşümü $M_{n\times n}(\mathbb{F}_q)$ 'da bir matris ile tanımlanır. Eğer R , $M_{n\times n}(\mathbb{F}_q)$ 'da bir matris ise $\forall x\in\mathbb{F}_q$ satır vektöründen $x.R$ 'ye yapılan eşleme $\mathbb{F}_q^n$ üzerinde R tarafından belirlenen bir $\mathbb{F}_q$ lineer dönüşümdür.

$\mathbb{F}_{q^n}$, $\mathbb{F}_q$ ' nun bir genişlemesi olsun. O zaman $\mathbb{F}_{q^n}$, n boyutlu bir lineer uzaydır. $\mathbb{F}_{q^n}$ 'de bir elemanla çarpma yapmak $\mathbb{F}_{q^n}$ üzerinde özel bir $\mathbb{F}_q$ lineer dönüşümdür.

$\forall \alpha \in \mathbb{F}_{q^n}$ için $f(x) = \alpha x$ olarak tanımlanan $f : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ yapılan eşleme $\mathbb{F}_{q^n}$ üzerinde bir $\mathbb{F}_q$ lineer dönüşümdür.

Tanım 2.1.1. $x \in \mathbb{F}_q^{bn}$ bir vektör $R \in M_{bn\times bn}(\mathbb{F}_q)$ bir matris olsun. $y = xR$ vektörüne R lineer dönüşümü altında x vektörünün görüntüsü denir. Yani

$i = 1,...,n$, $x_i \in \mathbb{F}_q^b$ için $x = (x_1,...,x_n)$ bir vektör ve $i, j = 1,...,n$, $R_{i,j} \in M_{b\times b}(\mathbb{F}_q)$

için $R = \begin{pmatrix} R_{1,1} & R_{1,2} & ... & R_{1,n} \\ R_{2,1} & R_{2,2} & ... & R_{2,n} \\ ... & ... & ... & ... \\ R_{n,1} & R_{n,2} & ... & R_{n,n} \end{pmatrix}$ bir matris olsun.

O zaman $j = 1,...,n$, $y_j \in \mathbb{F}_q^b$ ve $y_j = \sum_{i=1}^{n} x_i R_{i,j}$ olacak şekilde

$y = (y_1,...,y_n) = (x_1,...,x_n)\begin{pmatrix} R_{1,1} & R_{1,2} & ... & R_{1,n} \\ R_{2,1} & R_{2,2} & ... & R_{2,n} \\ ... & ... & ... & ... \\ R_{n,1} & R_{n,2} & ... & R_{n,n} \end{pmatrix}$ olur.

Tanım 2.1.2. F ve E, $F \subseteq E$ ve $E \subseteq F$ olacak şekilde iki cisim olsun. $N \in M_{b\times b}(E)$ bir kare matris olmak üzere $f(x) \in F[x]$ polinomu için $f(\mathrm{N}) = 0_b$ ise $f(x)$ polinomuna $F[x]$'de N'in sıfırlayıcı polinomu denir (0_b, $M_{b\times b}(F)$'de bir sıfır matristir).

Önerme 2.1.1. Bir W matrisinin minimal polinomu onun bütün sıfırlayıcı polinomlarını böler.

Önerme 2.1.2. F cismi üzerinde bir matrisin minimal polinomu ve karakteristik polinomu $F[x]$'de aynı indirgenemez çarpanlara sahiptir.

Önerme 2.1.3. $R \in M_{bn\times bn}(\mathbb{F}_2)$ matrisi $\exists b,n$ pozitif tamsayıları için bir difüzyon tabakası olsun. Varsayalım ki R matrisi $i,j=1,...,n$, $R_{i,j} \in M_{b\times b}(\mathbb{F}_2)$ için

$$R=\begin{pmatrix} R_{1,1} & R_{1,2} & ... & R_{1,n} \\ R_{2,1} & R_{2,2} & ... & R_{2,n} \\ ... & ... & ... & ... \\ R_{n,1} & R_{n,2} & ... & R_{n,n} \end{pmatrix}$$ olacak şekilde n^2 bloklara bölünsün.

O zaman R matrisinin MDS olması için gerek ve yeter şart bu blokların bazılarından oluşan R'nin her alt matrisinin regüler olmasıdır.

Yardımcı Teorem 2.1.1. Bir F cisim ve $R \in M_{bn\times bn}(F)$ matrisi $\exists b,n$ pozitif tamsayıları için bir blok matris olsun.

$$R=\begin{pmatrix} R_{1,1} & R_{1,2} & ... & R_{1,n} \\ R_{2,1} & R_{2,2} & ... & R_{2,n} \\ ... & ... & ... & ... \\ R_{n,1} & R_{n,2} & ... & R_{n,n} \end{pmatrix}$$ olacak şekilde $i,j=1,...,n$ için $R_{i,j} \in M_{b\times b}(F)$

blok matrisleri değişmeli çiftler (commute pairwise) dir. O zaman

$\det(R)=\det(\sum(-1)^{\tau(i_1,i_2,...,i_n)+\tau(j_1,j_2,...,j_n)} R_{i_1,j_1}R_{i_2,j_2}...R_{i_n,j_n})$ dir.

Başka bir deyişle eğer $R \in M_{bn\times bn}(F)$ blok matrisinin $i,j=1,...,n$ için $R_{i,j}$ blokları girdiler olarak alınıp $R \in M_{bn\times bn}(F)$ matrisi $n\times n$ matris olarak kabul edilirse bu durumda R blok matrisinin determinantı

$\det_s(R)=\sum(-1)^{\tau(i_1,i_2,...,i_n)+\tau(j_1,j_2,...,j_n)} R_{i_1,j_1}R_{i_2,j_2}...R_{i_n,j_n}$ dir.

O zaman $\det(R)=\det(\det_s(R))$ olur.

R difüzyon tabakasının MDS olup olmadığını kontrol etmek için matrisin tüm alt matrislerinin determinantlarının kontrol edilmesi gerekmektedir. Eğer bu determinantlar yardımcı teorem 2.1.1 ile hesaplanmak istenirse $R_{i,j}$ blok matrislerinin tümü değişmeli çiftler olmak zorundadır. Yani R difüzyon tabakası içinde bulunan her $R_{i,j}$ blok matris çiftlerinin birbirleri ile değişmeli olması gerekir.

Bu durumu sağlatmak çok zordur. Bu yüzden matris bloklarının tümü belirli bir ilkel bloğun polinomları olan belirli matris türleri üzerine odaklanılır. Ayrıntılı olarak bu gibi bir durum sadece $i, j = 1,...,n$ için R difüzyon tabakasının her $R_{i,j}$ bloğu belirli bir ilkel $W \in M_{b\times b}(\mathbb{F}_2)$ bloğunun bir polinomu olduğu zaman ele alınır.

Şimdi blokların tümü belirli bir $W \in M_{b\times b}(\mathbb{F}_2)$ bloğunun polinomlar olan blok difüzyon tabakalarına odaklanılacaktır.

Tanım 2.1.3. $i, j = 1,...,n$ $f_{i,j}(x) \in F_2[x]$ için $\forall R_{i,j}$ bloğu $f_{i,j}(W)$ 'ya eşit olsun.

O zaman; $\begin{pmatrix} f_{1,1}(x) & f_{1,2}(x) & ... & f_{1,n}(x) \\ f_{2,1}(x) & f_{2,2}(x) & ... & f_{2,n}(x) \\ ... & ... & ... & ... \\ f_{n,1}(x) & f_{n,2}(x) & ... & f_{n,n}(x) \end{pmatrix} \in M_{n\times n}(\mathbb{F}_2[x])$ polinom matrisi R' nin dış matrisi olarak adlandırılır.

Burada eğer W'nın minimal polinomu bilinirse R difüzyon tabakasının alt matrislerinin regüler olup olmadığını belirlemek için daha etkili bir yöntem aşağıdaki yardımcı teoremle verilir.

Yardımcı Teorem 2.1.2. F bir cisim, $W \in M_{b\times b}(F)$ bir matris, $F[x]$ polinom halkasında W'nın minimal polinomu $m_W(x)$ ve $h(x) \in F[x]$ olsun. O zaman $\det(h(W)) \neq 0$ olması için gerek ve yeter şart $Ebob(h(x), m_W(x)) = 1$ olmasıdır.

İspat: İlk olarak eğer bir polinom ailesinin en büyük ortak böleni 1'e eşit ise onlar aralarında asaldır. Varsayalım ki $h(W)$ regüler bir matris, $Ebob(h(x), m_W(x)) = d(x)$ ve $\deg(d) > 1$ olsun. O zaman $h(x) = r(x)d(x)$, $m_W(x) = t(x)d(x)$ olacak şekilde $r(x), t(x) \in F[x]$ vardır. Sonuç olarak $h(W) = r(W)d(W)$ ve $m_W(W) = t(W)d(W)$ elde edilir. $0_b = m_W(W) = t(W)d(W)$ ve $\deg(t) < \deg(m_W)$ denklemlerinden $t(W) \neq 0_b$ elde edilir. O zaman $d(W)$ singüler olarak elde edilir. Aksi takdirde $t(W) = 0_b$ olacaktır.

$h(W) = r(W)d(W)$ denkleminde $h(W)$ regüler olduğu için $d(W)$ regüler olarak elde edilir. Bu bir çelişkidir. Böylece $Ebob(h(x), m_W(x)) = 1$ olmak zorundadır.

Tersine varsayalım ki $Ebob(h(x), m_W(x)) = 1$ olsun. O zaman $h(x)r(x) + m_W(x)t(x) = 1$ olacak şekilde $r(x), t(x) \in F[x]$ vardır. Eğer $x = W$ yazılırsa $h(W)r(W) = \mathrm{I}_b$ elde edilir. Böylece $h(W)$ regüler olur.

Her alt matrisin determinantını hesaplamak yerine yardımcı teorem 2.1.2' den verilen teknik ile bir alt matrisin regüler olup olmadığını hesaplamak için yapılması gereken tek şey sembolik determinantı hesaplamaktır ve x'e göre bir polinom olarak ele alınan sembolik determinantın $m_W(x)$ ile aralarında asal olup olmadığını kontrol etmektir.

Bir ilkel W bloğunun minimal polinomu $\mathbb{F}_2[x]$'de indirgenemez olduğundan $f(x) \in \mathbb{F}_2[x]$ polinomunun $m_W(x)$ ile aralarında asal olması için gerek ve yeter şartın $f(x) \not\equiv 0 \bmod m_W(x)$ olduğu açıktır. Yani $f(x) \in \mathbb{F}_2[x]$ polinomu için $f(W)$' nın regüler olması için gerek ve yeter şart $f(x) \not\equiv 0 \bmod m_W(x)$ olmasıdır.

Örnek 2.1.1. $g(x) = x^3 + x + 1$ polinomu $\mathbb{F}_2[x]$'de monik indirgenemez polinom olsun. Ele alınan bu indirgenemez polinom ile bir R MDS difüzyon tabakası üretilsin.

İlk olarak $g(x) = x^3 + x + 1$ polinomunu kullanılarak eş matris yardımıyla ilkel bir W blok matrisi üretilsin. Eş matrisin genel tanımından

$$\begin{pmatrix} 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & -a_1 \\ 0 & \ddots & 0 & \vdots \\ 0 & 0 & 1 & -a_{b-1} \end{pmatrix} \quad (\mathbb{F}_2\text{'de } -a_i = a_i \text{ dir.})$$

$W = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$ olur. W matrisi $g(x)$ polinomunda yerine yazılsın.

$$g(W) = W^3 + W + 1 = \begin{pmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{pmatrix} + \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} = 0_{3\times 3}.$$

$g(x)$ polinomunun $\mathbb{F}_2[x]$'de W'nin karakteristik polinomu olduğu bilinmektedir. Hamilton-Cayley teoreminden $g(W) = 0_3$ olur. O zaman $m_W(x) \big/ g(x)$ dir.

Fakat $g(x)$ sadece iki monik çarpana sahiptir ve bunlar 1 ve $g(x)$ dir. 1 herhangi bir matrisin sıfırlayıcı polinomu kesinlikle olamaz ($g(1) \neq 0_b$). Bu durumda $g(x)$ polinomu $\mathbb{F}_2[x]$'de W'nin minimal polinomu olmak zorunda olur. Buradan $m_W(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$ indirgenemez minimal polinomu elde edilmiş olur.

$Ebob(f(x), m_W(x)) = 1$ şartı sağlanacak şekilde $\{1, x, x+1, x^2+1, x^2+x, x^2+x+1\}$ polinomları ele alınarak bir R matrisi oluşturulsun

$$R = \begin{pmatrix} 1 & x & x+1 \\ x^2+1 & x^2+x & 1 \\ x & x^2+x+1 & x+1 \end{pmatrix}.$$

Burada yardımcı teorem 2.1.2 yardımı ile $m_W(x) = x^3 + x + 1$ minimal polinomunun R matrisinin içindeki her bir $f(x)$ polinomuyla aralarında asal olduğu anlaşılır. Yani $Ebob(f(x), m_W(x)) = 1$ dir.

Buradan $f(x) \not\equiv 0 \bmod m_W(x)$ olduğundan $f(W)$ matrisleri regülerdir. Yani $\det(f(W)) \neq 0$ dır. Buradan ise R matrisinin tüm alt matrislerinin regüler olduğu

anlaşılır. R matrisinin kendisinin regüler olup olmadığına bakmak için $\det_s(R) = x^5 + x^3 + x^2 + x$ elde edilir. $x = W$ için $\det_s(R) \neq 0$ olur. Sonuç olarak ise R matrisinin MDS matris olduğu görülür.

2.2. Gabidulin Kodlardan Tekrarlı (Recursive) MDS Difüzyon Tabakalarının İnşası

2.2.1. Tekrarlı MDS difüzyon tabakaları

Simetrik şifrelemede etkili bir MDS difüzyon tabakasının inşasında ve donanımdaki uygulamalarında matrisin boyutu büyüdükçe büyük problemler ortaya çıkar. Bu problemlerden kaçınmak için $W = Z^r$ bir MDS matris olacak şekilde bir Z eş matrisi kullanılır. O zaman Z matrisinin uygulanması uygun olur ve tam difüzyon Z matrisinin r kez ötelenmesinden sonra elde edilir.

2.2.2. Gabidulin kodlardan MDS matrisler oluşturma

$p = 2$ olmak üzere $K = GF(p^m)$, $F = GF(p)$ taban cisminin m. dereceden bir genişlemesi olan sonlu bir cisim olsun ve E, $GF(p)$'nin vektör uzayı olan p tabanında her biri m uzunluğunda olan vektörler kümesi $GF(p)^m$'i göstersin. K cismi F üzerinde m boyutlu bir vektör uzayı olarak görülebilir.

Tanım 2.2.2.1. $x = (x_1, ..., x_n)$, $E = K^n$'nin bir elemanı olsun. x vektörünün (kodsözünün) rank ağırlığı (rankı), $\{x_1, ..., x_n\}$ tarafından üretilen F vektör uzayının boyutudur ve $rk(x)$ ile gösterilir.

Örnek 2.2.2.1. $K = GF(2^3) = GF(2)(\alpha)$ olmak üzere $x^3 + x^2 + 1$ polinomu $\alpha^3 + \alpha^2 + 1$ şeklinde yazılsın. F üzerinde K'nın bir bazı $S = (s_1, ..., s_m)$ olmak üzere $m = 3$ için $S = (s_1, s_2, s_3) = (1, \alpha, \alpha^2)$ olarak ele alınsın. O zaman $\alpha^3 = \alpha^2 + 1$ ve

$n=5$ için $x=(\alpha^5,\alpha,0,\alpha^4,\alpha)=(\alpha+1,\alpha,0,\alpha^2+\alpha+1,\alpha)$ vektörünün rankı hesaplansın.

$x=(x_1,...,x_5)$ vektörünün rankı, F taban cismindeki girdilerin her x_i koordinatının yerine geçerek $S=(1,\alpha,\alpha^2)$ bazı yardımıyla oluşturacağı matrisin rankı olacaktır.

Bu durumda

$$\begin{array}{ll} x_1=a_{11}.s_1+a_{21}.s_2+a_{31}.s_3 & x_1=a_{11}.1+a_{21}.\alpha+a_{31}.\alpha^2 \\ x_2=a_{12}.s_1+a_{22}.s_2+a_{32}.s_3 \text{ için} & x_2=a_{12}.1+a_{22}.\alpha+a_{32}.\alpha^2 \\ \vdots & \vdots \\ x_5=a_{15}.s_1+a_{25}.s_2+a_{35}.s_3 & x_5=a_{15}.1+a_{25}.\alpha+a_{35}.\alpha^2 \end{array}$$

dir. Burada her x_i vektörü sütun vektörü olarak alınırsa $x=(\alpha+1,\alpha,0,\alpha^2+\alpha+1,\alpha)$ vektörü yardımıyla

$$M_x=\begin{pmatrix} a_{11} & a_{12} & a_{13} & a_{14} & a_{15} \\ a_{21} & a_{22} & a_{23} & a_{24} & a_{25} \\ a_{31} & a_{32} & a_{33} & a_{34} & a_{35} \end{pmatrix}=\begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

matrisi elde edilir ve $rk(x)=3$ tür.

$d_r(a,b)=rk(a-b)$ bağıntısı $E=K^n$ vektör uzayı üzerinde bir uzaklık tanımlar.

Tanım 2.2.2.2. Yukarıda verilen bağıntıya göre rank uzaklığı, K^n uzayından seçilen herhangi *a* ve *b* vektörünün farkından elde edilen yeni *c* vektörünün rank ağırlığına denir.

Rank uzaklığı için $d_r(x,y)\le m$ şartı mevcuttur ve hamming uzaklığı ile arasında $d_r(x,y)\le d_h(x,y)$ bağıntısı vardır.

Tanım 2.2.2.3. C lineer kodunun rank uzaklığı (d_r), onun sıfırdan farklı kodsözlerinin en küçük rank ağırlığına eşittir.

Önerme 2.2.2.1. Eğer C kodu n uzunluğunda k boyutlu ve rank uzaklığı d_r olan bir lineer kod ise o zaman

1) $n \le m$ için $k + d_r \le n+1$
2) $n > m$ için $k.m + d_r.n \le (m+1).n$ olur.

Tanım 2.2.2.4. Yukarıda verilen sınıra ulaşan koda maksimum rank uzaklıklı (MRD) kod denir.

Eğer $n \le m$ durumu mevcut olursa o zaman herhangi bir MRD kod aynı zamanda bir MDS kod olur. Eğer $\left(\mathrm{I}_r | W \right)$ matrisi tarafından üretilen bir kod MRD özelliğine sahipse W kare matrisi de MRD özelliğine sahip olur. Hamming uzaklıkta da olduğu gibi eğer W matrisi MRD özelliğine sahipse o zaman hem W^{-1} hem de W^T MRD özelliğine sahip olur.

Tanım 2.2.2.5. $S = (s_1, s_2, ..., s_n)$ kümesi F cismi üzerinde lineer bağımsız olan K cisminin $n \le m$ elemanlı sıralı bir kümesi olsun. k boyutlu olan ve $S = (s_1, s_2, ..., s_n)$ kümesinden elde edilen Gabidulin kodu ($G_{S,k}$) $s_j^{[i]} = s_j^{p^i}$ olacak şekilde aşağıdaki üreteç matris tarafından üretilen bir koddur

$$G_{S,k} = \begin{pmatrix} s_1^{[0]} & s_2^{[0]} & \dots & s_n^{[0]} \\ s_1^{[1]} & s_2^{[1]} & \dots & s_n^{[1]} \\ \dots & \dots & \ddots & \dots \\ s_1^{[k-1]} & s_2^{[k-1]} & \dots & s_n^{[k-1]} \end{pmatrix}.$$

Tanım 2.2.2.6. $F = GF(2)$ üzerinde K sonlu cisminin bir bazı $S = (s_1, ..., s_m)$ olsun. $n = 2k$ oranlı herhangi bir Gabidulin kod (rank kodu) ($G_{S,r}$), K üzerinde

$[m=2r, r, r+1]$ parametrelerine sahip olan bir MRD koddur ve $r+1$ bu kodun hem minimum hamming uzaklığı hemde minimum rank uzaklığıdır.

Gabidulin koddan elde edilecek olan $(\mathrm{I}_k \,|W)$ sistematik üreteç matris için W matrisi K üzerinde büyüklüğü r olan bir kare matris ise W matrisi K üzerinde bir MDS matris olur.

Şimdi eğer bir Gabidulin kodu inşa etmek için bir polinom bazı seçilirse, Gabidulin koddan üretilen W MDS matrisine karşılık gelen tekrarlı bir difüzyon tabakası olan bir eş matrisi oluşturmanın mümkün olduğu gösterilsin.

$\alpha \in K = GF(2^m)$, F üzerinde $m.$ dereceden $P(X)$ indirgenemez polinomunun bir kökü olsun. F üzerinde K'nın bir polinom bazı $S=(1,\alpha,\alpha^2,...,\alpha^{m-1})$ şeklindedir. $0 \le i \le m-1$ için $e_i = \alpha^i$ olsun. $\forall i, j$ için $0 \le i+j < m$ olacak şekilde e_i' ler $e_i.e_j = e_{i+j}$ dir. $e^{[i]} = e^{2^i}$ kavramı kullanılarak $m=2r$ eşitliği vasıtasıyla $G_{S,r}$ Gabidulin kod üreteç matrisi

$$G_{S,r} = \begin{pmatrix} e_0 & e_1 & e_2 & \dots & e_{m-1} \\ e_0^{[1]} & e_1^{[1]} & e_2^{[1]} & \dots & e_{m-1}^{[1]} \\ e_0^{[2]} & e_1^{[2]} & e_2^{[2]} & \dots & e_{m-1}^{[2]} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ e_0^{[r-1]} & e_1^{[r-1]} & e_2^{[r-1]} & \dots & e_{m-1}^{[r-1]} \end{pmatrix}$$

şeklinde elde edilir.

r boyutlu L ve N kare matrisleri aşağıdaki gibi tanımlansın.
L matrisi, $G_{S,r}$ matrisinin ilk r sütunu alınarak elde edilsin.
N matrisi $G_{S,r}$ matrisinin 2. Sütunundaki $(e_1, e_1^{[1]}, e_1^{[2]}, ..., e_1^{[r-1]})$ katsayıları ile oluşturulan köşegen matris olsun.

Yardımcı Teorem 2.2.2.1. $0 \le i \le 1$ için

$$N^i L = \begin{pmatrix} e_i & e_{i+1} & e_{i+2} & \dots & e_{i+r-1} \\ e_i^{[1]} & e_{i+1}^{[1]} & e_{i+2}^{[1]} & \dots & e_{i+r-1}^{[1]} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ e_i^{[r-1]} & e_{i+1}^{[r-1]} & e_{i+2}^{[r-1]} & \dots & e_{i+r-1}^{[r-1]} \end{pmatrix}.$$

Özellikle $G_{S,r} = (L \,|\, N^r L)$ ve $M = (\mathrm{I}_r \,|\, L^{-1} N^r L)$ Gabidulin kodun sistematik üreteç matrisidir.

İspat: Bu durum $K = GF(p^m)$'nin $\forall e, \mathrm{g}$ elemanı, herhangi v tamsayısı ve $\forall\, i + j \le m$ için $(eg)^{[v]} = e^{[v]} g^{[v]}$ ve $e_i . e_j = e_{i+j}$ bağıntılarının doğrudan sonucudur.

Şimdi $W = L^{-1} N^r L$ MDS difüzyon matrisi ele alınsın. $0 \le i, j \le r$ için $W = (w_{ij})$ şeklinde belirlensin. O zaman θ eş matrisi, r. kuvvetin de bir eş difüzyon tabakası olan ve W matrisi ile bağlantılı ($\theta^r = W$) bir matristir.

Teorem 2.2.2.1. $\theta^r = L^{-1} N^r L = W$ dir.

İspat: $\theta^r = L^{-1} N^r L = W$ eşitliği için $\theta^r = L^{-1} N^r L$ eşitliğinde her iki taraf sırasıyla sağdan L^{-1} matrisi ile soldan L matrisi ile çarpılsın. Bu durumda $L \theta L^{-1} = N^r$ eşitliği elde edilir. Burada $(L \theta L^{-1})^r = L \theta^r L^{-1}$ olduğundan $L \theta L^{-1} = N$ eşitliğini ispatlamak yeterli olacaktır. $L \theta L^{-1} = N$ eşitliği eşitliğin her iki tarafından sağdan L matrisi ile çarpılsın. Buradan $L\theta = NL$ eşitliği elde edilir.

Yardımcı teoremden $0 \le i \le r$, $i = 1$ için $NL = \begin{pmatrix} e_1 & e_2 & \dots & e_r \\ e_1^{[1]} & e_2^{[1]} & \dots & e_r^{[1]} \\ \vdots & \vdots & \vdots & \vdots \\ e_1^{[r-1]} & e_2^{[r-1]} & \dots & e_r^{[r-1]} \end{pmatrix}$.

$0 \le i \le m-1$ için $(e_i, e_i^{[1]}, ..., e_i^{[r-1]})$ sütunu T_i ile gösterilsin. Bu kavram ile NL matrisinin yeni gösterimi $NL = (T_1 | T_2 | ... | T_r)$ şeklinde olur.

Buradan L matrisi $L = (T_0 | T_1 | ... | T_{r-1})$ şeklinde olur. θ bir eş matris olduğu için $L\theta$ matrisinin ilk $r-1$ sütunu L matrisinin son $r-1$ sütununun sadece bir pozisyon değişmesi ile elde edilir. Böylece $Z_r = L\theta_r$ olacak şekilde $L\theta = (T_1 | T_2 | ... | T_{r-1} | Z_r)$ matrisi elde edilir. Burada Z_r, θ eş matrisinin son sütunu yani W matrisinin ilk sütunu olmaktadır.

İspatın tamamlanması için $Z_r = T_r$ olduğunun gösterilmesi gerekmektedir. Şimdi $W = L^{-1} N^r L$ olduğunu hatırlansın. Buradan eşitliğin her iki tarafı soldan L matrisi ile çarpılırsa $LW = N^r L$ eşitliği elde edilir. L matrisinin ilk sütunu T_0 dır. Sonuç olarak LW matrisinin ilk sütunu $(e_r, e_r^{[1]}, ..., e_r^{[r-1]})$ olur. Yani T_r'ye eşit olur. Bu durumda LW matrisinin ilk sütunu $L\theta$ matrisinin son sütununa eşit olacağından $Z_r = T_r$ eşitliği sağlanmış olur.

Örnek 2.2.2.2. $K = GF(2^6)$ için $P(X) = x^6 + x + 1$ indirgenemez polinomu ele alınsın. $\alpha \in K = GF(2^6)$ indirgenemez polinomun kökü olsun. $m = 6$ olduğundan $P(\alpha) = \alpha^6 + \alpha + 1$ indirgenemez polinomu için polinom bazı $S = (1, \alpha, \alpha^2, ..., \alpha^{m-1})$ olacak şekilde $S = (1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5)$ bazı alınsın. Buradan $(m = 2r, r, r+1) = (6, 3, 4)$ parametrelerine sahip olan Gabidulin kodun üreteç matrisi üretilsin.

$m = 6$ ve $r = 3$ olduğundan Gabidulin kod oluşturmak için seçilen S bazından elde edilen $G_{S,r}$ matrisi

$$G_{S,3} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} \end{pmatrix} \text{ olur.}$$

Bu matris ayrıca $(m = 2r, r, r+1) = (6, 3, 4)$ parametreli bir MRD koddur. Elde edilen bu matriste gerekli satır indirgeme işlemleri yapılarak

$$G_{S,3} = \left(\underbrace{\begin{matrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{matrix}}_{I_{3\times 3}} \middle| \underbrace{\begin{matrix} \alpha^{7} & \alpha^{43} & \alpha^{37} \\ \alpha^{51} & \alpha^{54} & \alpha^{29} \\ \alpha^{36} & \alpha^{30} & \alpha^{56} \end{matrix}}_{W_{3\times 3}} \right)$$

üreteç matrisi elde edilir. Bu üreteç matristen elde edilecek olan $K = GF(2^6)$ üzerindeki bir C Gabidulin kodunun minimum hamming uzaklığı ve minimum rank uzaklığı 4'tür. Diferansiyel işleminin girdisi olan $x = (x_1, x_2, x_3) \in K^3$ vektörü için $x_i = (x_{i,1}, ..., x_{i,6}) \in F^6$ olmak üzere W matrisi yardımıyla $y = (y_1, y_2, y_3) = x.W^T$ olacak şekilde bir y çıktı vektörü elde edilir. Buradan x, y vektörleri birleştirilerek $c = (x \mid y)$ kodsözü oluşturulur.

Şimdi üreteç matristen oluşturulan MDS W matrisi için bu matrise karşılık gelen tekrarlı bir difüzyon matrisi olan bir eş matrisi oluşturmanın mümkün olduğu gösterilsin.

$$G_{S,3} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} \end{pmatrix}$$

matrisi için;

L matrisi, $G_{S,r}$ matrisinin $r = 3$ için ilk 3 sütunundan elde edilen bir matris olsun.

N matrisi, $G_{S,r}$ matrisinin 2. sütunundan oluşturulan bir köşegen matris olsun.

O zaman $L=\begin{pmatrix}1 & \alpha & \alpha^2\\ 1 & \alpha^2 & \alpha^4\\ 1 & \alpha^4 & \alpha^8\end{pmatrix}$ $N=\begin{pmatrix}\alpha & 0 & 0\\ 0 & \alpha^2 & 0\\ 0 & 0 & \alpha^4\end{pmatrix}$ olur.

Yardımcı teoremden $0\le i\le 3$ için $G_{S,r}=\left(L\middle|N^3L\right)$ ve üreteç matrisi $M=\left(\mathrm{I}_3\middle|L^{-1}N^3L\right)$ şeklinde elde edilir.

Buradan $N^3=\begin{pmatrix}\alpha^3 & 0 & 0\\ 0 & \alpha^6 & 0\\ 0 & 0 & \alpha^2\end{pmatrix}$ olmak üzere

$$N^3L=\begin{pmatrix}\alpha^3 & 0 & 0\\ 0 & \alpha^6 & 0\\ 0 & 0 & \alpha^2\end{pmatrix}\begin{pmatrix}1 & \alpha & \alpha^2\\ 1 & \alpha^2 & \alpha^4\\ 1 & \alpha^4 & \alpha^8\end{pmatrix}=\begin{pmatrix}\alpha^3 & \alpha^4 & \alpha^5\\ \alpha^6 & \alpha^8 & \alpha^{10}\\ \alpha^{12} & \alpha^{16} & \alpha^{20}\end{pmatrix}$$

elde edilir. $L^{-1}=\begin{pmatrix}\alpha^{29} & \alpha^{47} & \alpha^{19}\\ \alpha^{37} & \alpha^{12} & \alpha^{23}\\ \alpha^{23} & \alpha^{42} & \alpha^{16}\end{pmatrix}$ olmak üzere

$$L^{-1}N^3L=\begin{pmatrix}\alpha^{29} & \alpha^{47} & \alpha^{19}\\ \alpha^{37} & \alpha^{12} & \alpha^{23}\\ \alpha^{23} & \alpha^{42} & \alpha^{16}\end{pmatrix}\begin{pmatrix}\alpha^3 & \alpha^4 & \alpha^5\\ \alpha^6 & \alpha^8 & \alpha^{10}\\ \alpha^{12} & \alpha^{16} & \alpha^{20}\end{pmatrix}=\begin{pmatrix}\alpha^7 & \alpha^{43} & \alpha^{37}\\ \alpha^{51} & \alpha^{36} & \alpha^{29}\\ \alpha^{36} & \alpha^{30} & \alpha^{56}\end{pmatrix}$$

elde edilir. Bu durumda $M=\left(\mathrm{I}_3\middle|L^{-1}N^3L\right)$ olmak üzere

$$M=\left(\begin{array}{ccc|ccc}1 & 0 & 0 & \alpha^7 & \alpha^{43} & \alpha^{37}\\ 0 & 1 & 0 & \alpha^{51} & \alpha^{36} & \alpha^{29}\\ \underbrace{0 & 0 & 1}_{\mathrm{I}_{3\times 3}} & \underbrace{\alpha^{36} & \alpha^{30} & \alpha^{56}}_{W_{3\times 3}}\end{array}\right)$$

üreteç matrisi elde edilir. Şimdi $r=3$ için $\theta^3 = W$ olduğu gösterilsin.

MDS W matrisinin ilk sütunundan elde edilen θ eş matrisi $\theta = \begin{pmatrix} 0 & 0 & \alpha^7 \\ 1 & 0 & \alpha^{51} \\ 0 & 1 & \alpha^{36} \end{pmatrix}$ olur.

Buradan

$$\theta^3 = \begin{pmatrix} 0 & 0 & \alpha^7 \\ 1 & 0 & \alpha^{51} \\ 0 & 1 & \alpha^{36} \end{pmatrix}^3 = \begin{pmatrix} \alpha^7 & \alpha^{43} & \alpha^{37} \\ \alpha^{51} & \alpha^{54} & \alpha^{29} \\ \alpha^{36} & \alpha^{30} & \alpha^{56} \end{pmatrix} = W$$

olur. Buradan $r=3$ için θ'nın 3 kez ötelenmesi ile W matrisi elde edilmiş olur.

$n \le m$ durumu ele alınarak $m=6$ için verilen bu örnek $m=16$ için düşünülecek olursa $K = GF(2^{16})$ üzerinde MRD özellikli bir MDS matris elde edilebilir. Bu durum da $n=2r$ için $2 \le r \le 8$ aralığında $r \times r$'lik bir W MDS matrisi elde etmek mümkündür.

$n > m$ durumu için $n=2k$ oranı bozulacağından MRD özelliğine sahip MDS matris bulunmamaktadır.

2.3. Hafif-Siklet Şifrelemeler İçin Eş Matrislerden MDS Matrislerin İnşası

Keyfi l ve n sayıları için $\mathbb{F}_{2^n}$'de $(t_0,...,t_{l-1})^l$ şeklinde bir seri yapısı tanımlanmaktadır. Bu seriden elde edilen eş matris ile hafif-siklet şifrelemelerde kullanılan MDS matrisler aranır. $\mathbb{F}_2$ üzerinde *n*. dereceden indirgenemez polinomun kökü α olmak üzere $l=4,5$ için $(t_0,...,t_{l-1})^l$ serisinden elde edilecek olan eş matrisin *l*. derecesi ile elde edilen matris bir MDS matris olacak şekilde uygun t_i değerleri serbest bir şekilde seçilmektedir. Seçilecek olan değerler ile oluşturulacak olan eş matrisin kullanılacağı alanlarda etkili sonuçlar verebilmesi için en kompakt t_i değerleri olarak $\{1,\alpha,\alpha^2,\alpha+1\}$ elemanları alınır.

Tanım 2.3.1. En küçük n_s pozitif tamsayısı için $s \equiv s2^{n_s} (\text{mod}\, 2^n-1)$ olacak şekilde C_s siklotomik (cyclotomic) eş kümesi modulo (2^n-1)'e göre $C_s=\{s, s.2,..., s.2^{n_s-1}\}$ olarak tanımlanmaktadır. C_s'deki en küçük tamsayı s alt indisidir ve C_s'nin eş küme lideri olarak adlandırılmaktadır. C_s eş kümesinin boyutu n_s sayısı ile belirlenir ve kümedeki eleman sayısı $|C_s|$ ile gösterilir.

Tanım 2.3.2. Bütün eş küme liderlerinin kümesi $\Upsilon(n)$ ile gösterilir ve eş kümelerdeki hesaplamalar $\mathbb{Z}_{2^n-1}$'de modülo (2^n-1)' e göre yapılır.

Örnek 2.3.1. $n=3$ için siklomatik eş kümelerde bulunan elemanlar modülo (2^3-1) 'e göre 7 tanedir. Bunlar $C_0=\{0\}$, $C_1=\{1,2,4\}$, $C_3=\{3,6,5\}$ dir. Burada C_0 ve C_1 eş kümelerinin eleman sayıları sırasıyla $|C_0|=1$ ve $|C_1|=3$ tür. Tüm eş küme liderlerinin kümesi $\Upsilon(3)=\{0,1,3\}$ olarak gösterilebilir.

Tanım 2.3.3. p bir asal sayı olacak şekilde $\alpha \in \mathbb{F}_{p^n}$ olsun. $P(x)$ polinomu α'nın $\mathbb{F}_p$ üzerinde minimal polinomu olsun. $f(\alpha)=0$ olacak şekilde $f(x)$ polinomu $\mathbb{F}_p$ üzerinde herhangi bir polinom ise $P(x) \big/ f(x)$ dir. O zaman $\exists n$ için $t_0, t_1, t_2, ..., t_{l-1} \in \mathbb{F}_{2^n}$ olmak üzere $(t_0, ..., t_{l-1})$ serisinden elde edilen eş matris

$$\begin{pmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ t_0 & t_1 & \dots & \dots & \dots & t_{l-1} \end{pmatrix} \text{dir.}$$

Elde edilen bu matrisin polinomu $t_0 + t_1 x + t_2 x^2 + ... + t_{l-1} x^{l-1} + x^l$ dir.

Tanım 2.3.4. $(t_0, ..., t_{l-1})^{-1}$ serisi için eş matrisin tersi

$$\begin{pmatrix} \frac{t_1}{t_0} & \frac{t_2}{t_0} & \dots & \dots & \dots & \frac{1}{t_0} \\ 1 & 0 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

şeklindedir.

$l=4$ ya da $l=5$ için şifreleme işlemi $(t_0, ..., t_{l-1})^l$ serisi ile oluşturulan matrisin l kez tekrarlı kullanımı ile yürütülürken deşifreleme işlemi ise $(t_0, ..., t_{l-1})^{-1}$ serisi ile oluşturulan matrisin l kez tekrarlı kullanımı ile yürütülebilir. Burada $t_0 = 1$ olduğunda deşifreleme aşamasında yapılacak olan işlemlerin hızı şifreleme aşamasında yapılanlar kadar iyi olacaktır.

Durum 2.3.1. Bir MDS matrisin tüm girdileri sıfırdan farklıdır.

Yardımcı Teorem 2.3.1. Bir MDS matrisin tersinin tüm girdileri sıfırdan farklıdır.

Sonuç 2.3.1. $\mathbb{F}_{2^n}$ üzerinde herhangi 2×2 tipinde bir matrisin MDS olması için gerek ve yeter şart matrisin tam ranklı bir matris olmasıdır ve matrisin tersinin tüm girdilerinin sıfırdan farklı olmasıdır.

Durum 2.3.2. Eğer $l\times l$ tipinde bir regüler matrisin tersinin tüm girdileri sıfırdan farklı ise o zaman bu matrisin tüm $(l-1)\times(l-1)$ alt matrisleri regülerdir.

Sonuç 2.3.2. Tüm girdileri sıfırdan farklı olan $\mathbb{F}_{2^n}$ üzerindeki herhangi 3×3 tipindeki matrisin bir MDS matris olması için gerek ve yeter şart bu matrisin tam ranklı olmasıdır ve bu matrisin tersinin tüm girdilerinin sıfırdan farklı olmasıdır.

Önerme 2.3.1. Her girdisi sıfırdan farklı olan $\mathbb{F}_{2^n}$ üzerindeki herhangi 4×4 tipindeki matrisin bir MDS matris olması için gerek ve yeter şart tüm girdileri sıfırdan farklı bir ters matrise sahip olan bu matrisin tam ranklı bir matris olmasıdır ve bu matrisin tüm 2×2'lik alt matrislerinin tam ranklı olmasıdır.

Hafif-siklet şifrelemeler bellek bakımından kısıtlı alanlarda kullanıldığından burada yapılacak olan işlemlerin mümkün olduğunca az olması gerekecektir. Bu yüzden burada yapılacak olan matris çarpımları bilinen yöntemden biraz farklıdır. Bu işlemler kolay anlaşılması bakımından 2.3.1 alt başlığında verilecek olan örnekte adım adım gösterilecektir.

Şimdi $l=4$ ve keyfi n için düşük hamming ağırlıklı $t_0,t_1,t_2,t_3\in\mathbb{F}_{2^n}$ elemanları kullanılarak $(t_0,t_1,t_2,t_3)^4$ serisinin MDS özelliklerine bakılsın. $\mathbb{F}_2$ üzerinde *n*. dereceden indirgenemez polinomun kökü α olmak üzere t_i değerleri $1,\alpha,\alpha^2,\alpha+1$ olarak alınır ve t_i değerlerinde 1' lerin sayısı mümkün olduğu kadar arttırılmaya çalışılır. Çünkü bu şekilde şifreleme ve deşifreleme sürecinde yapılacak olan

işlemlerde kolaylık ve hız kazanımı olacaktır. Ayrıca incelenen bu serilerden elde edilen MDS matrisler hafif-siklet matrisler olup hafif-siklet kriptolojide kullanılır.

2.3.1. $(1,1,1,1)^4$ ve $(t_0,1,1,1)^4$ serilerinin MDS özelliklerinin incelenmesi

$(t_0,t_1,t_2,t_3)^4$ serisinde t_0, t_1, t_2 ve t_3 elemanlarının herhangi üçünün yada hepsinin 1 olduğu ele alınacak olursa bu seri ile oluşturulacak olan eş matrisin 4. kuvvetinin alınmasıyla elde edilecek olan matrisin elemanlarından bazıları 0 olacaktır. Dolayısıyla eş matris durum 2.3.1' den MDS matris olamayacaktır.

Örnek 2.3.1.1. $(\alpha,1,1,1)^4$ serisi ile üretilen eş matrisin MDS özelliğine bakılsın.

$(\alpha,1,1,1)$ serisi ile üretilen eş matris

$$(\alpha,1,1,1) = W = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \alpha & 1 & 1 & 1 \end{pmatrix} \text{ dir.}$$

$l = 4$ için $(\alpha,1,1,1)^4$ serisi hesaplansın.

Burada W matrisinin kendisi ile çarpılması durumunda W^2 matrisinin elde edilebilmesi için W matrisinin satır vektörleri bir durum yukarı kaydırılır ve 4. satırda bulunan $(\alpha,1,1,1)$ vektörünün W matrisi ile çarpımından elde edilen $(0,0,0,1)$ satır vektörü W^2 matrisinin 4. satırında yerine yazılır.

$$W.W = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \alpha & 1 & 1 & 1 \end{pmatrix} . \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \alpha & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ \alpha & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Yukarıda elde edilen W^2 matrisi W matrisi ile çarpılırken yine W^2 matrisinin satır vektörleri bir durum yukarı kaydırılır ve 4. satırdaki $(0,0,0,1)$ vektörünün W matrisi ile çarpımından elde edilen $(\alpha,1,1,1)$ vektörü elde edilecek olan W^3 matrisinin 4. satırına yazılır.

$$W^2.W=\begin{pmatrix}0&1&0&0\\0&0&1&0\\\alpha&1&1&1\\0&0&0&1\end{pmatrix}.\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\\alpha&1&1&1\end{pmatrix}=\begin{pmatrix}0&0&1&0\\\alpha&1&1&1\\0&0&0&1\\\alpha&1&1&1\end{pmatrix}$$

Elde edilen W^3 matrisinden W^4 matrisini elde etmek için yukarıdakine benzer işlemler yapılır ve aşağıdaki gibi W^4 matrisi elde edilir.

$$W^3.W=\begin{pmatrix}0&1&0&0\\\alpha&1&1&1\\0&0&0&1\\\alpha&1&1&1\end{pmatrix}.\begin{pmatrix}1&0&0&0\\0&1&0&0\\0&0&1&0\\\alpha&1&1&1\end{pmatrix}=\begin{pmatrix}\alpha&1&1&1\\0&0&0&1\\\alpha&1&1&1\\0&0&0&1\end{pmatrix}$$

Bu durumda $(\alpha,1,1,1)^4=W^4=\begin{pmatrix}\alpha&1&1&1\\0&0&0&1\\\alpha&1&1&1\\0&0&0&1\end{pmatrix}$ matrisi elde edilmiş olur.

Yukarıda da bahsedildiği gibi bu matrisin MDS matris olmadığı açıktır.

Bu örnekte de görüldüğü gibi t_0, t_1, t_2 ve t_3 elemanlarının herhangi üçünün ya da hepsinin 1 olduğu durumda elde edilecek olan matrislerden hiç biri MDS matris olmayacaktır.

O zaman t_0, t_1, t_2 ve t_3 elemanlarından herhangi ikisinin 1 olduğu durumlara bakılacaktır. Bu durumda t_0, t_1, t_2 ve t_3 elemanlarından herhangi ikisinin 1 olduğu ve

diğer iki elemanın ise $\{\alpha, \alpha^2, \alpha+1\}$ elemanlarından seçildiğinde elde edilecek olan seriler $(t_0, t_1, 1, 1)^4$, $(t_0, 1, t_2, 1)^4, (1, 1, t_2, t_3)^4, (1, t_1, t_2, 1)^4, (1, t_1, 1, t_3)^4, (t_0, 1, 1, t_3)^4$. Burada $(t_0, t_1, 1, 1)^4$, $(t_0, 1, t_2, 1)^4$ serileri ile üretilen matrisler MDS matris olmayacaktır. Çünkü bu serilerin 4. kuvveti ile elde edilecek olan matrisin hem elemanlarından bazıları 0 olacaktır hem de tam ranklı bir matris olmayacaktır. Bu durumda $(1, 1, t_2, t_3)^4$, $(1, t_1, t_2, 1)^4, (1, t_1, 1, t_3)^4$ ve $(t_0, 1, 1, t_3)^4$ serilerinin bu 4 genel durumu için MDS özelliğine bakılacaktır.

2.3.2. $(1,1,t_2,t_3)^4$ ve $(1,t_1,t_2,1)^4$ serilerinin MDS özelliklerinin incelenmesi

$\mathbb{F}_2$ üzerinde *n*. dereceden indirgenemez polinomun kökü α olmak üzere $\mathbb{F}_{2^n}$ üzerinde tanımlanan $S=(1,1,t_2,t_3)$ serisi için t_2, t_3 elemanları $\{\alpha, \alpha^2\}$ ya da $\{\alpha, \alpha+1\}$ elemanlarından seçildiği zaman ve $S=(1,t_1,t_2,1)$ serisi için t_1, t_2 elemanları $\{\alpha, \alpha^2\}$ ya da $\{\alpha, \alpha+1\}$ elemanlarından seçildiği zaman S^4 bir MDS matris olmaz. Fakat $\mathbb{F}_{2^n}$ üzerindeki $(1,1,t_2,t_3)^4$ ve $(1,t_1,t_2,1)^4$ serilerinin 1'in dışındaki t_1, t_2 ve t_3 elemanları farklı olursa ve elemanlar n'nin daha büyük değerleri için $\{\alpha+1, \alpha^2\}$ elemanlarından seçilirse bu seriler MDS olacaktır.

O zaman $(1,1,t_2,t_3)^4$ ve $(1,t_1,t_2,1)^4$ serileri için;

$n=5$ iken α'nın minimal polinomu x^5+x^3+1 ya da $x^5+x^4+x^3+x+1$ olduğu durumlar dışında $\forall n \geq 5$ için $(1,1,\alpha+1,\alpha^2)^4$ serisi MDS dir.

$n=4$ iken α'nın minimal polinomu x^4+x^3+1 ya da x^4+x+1 olduğu durumlar dışında ya da $n=5$ iken α'nın minimal polinomu x^5+x^2+1 ya da $x^5+x^4+x^3+x+1$ olduğu durumlar dışında $\forall n \geq 4$ için $(1,1,\alpha^2,\alpha+1)^4$ serisi MDS dir.

$n=5$ iken α'nın minimal polinomu x^5+x^3+1 ya da $x^5+x^4+x^3+x+1$ olduğu durumlar dışında $\forall n \geq 5$ için $(1,\alpha^2,\alpha+1,1)^4$ serisi MDS dir.

$n=4$ iken α'nın minimal polinomu x^4+x^3+1 ya da x^4+x+1 olduğu durumlar dışında ya da $n=5$ iken α'nın minimal polinomu x^5+x^2+1 ya da $x^5+x^4+x^3+x+1$ olduğu durumlar dışında $\forall n \geq 4$ için $(1,\alpha^2,\alpha+1,1)^4$ serisi MDS dir.

Burada verilen minimal polinomların $(1,1,t_2,t_3)^4$ ve $(1,t_1,t_2,1)^4$ serilerini MDS yapmamasının nedeni bu minimal polinomların bu seriler ile inşa edilen matrisin elemanlarından bazılarının kökü olup matrisin elemanlarını 0 yapmasıdır. Dolayısıyla durum 2.3.1'den bu minimal polinomlar bu matrisleri MDS yapmaz.

2.3.3. $(1,t_1,1,t_3)^4$ serisinin MDS özelliğinin incelenmesi

$(1,t_1,1,t_3)^4$ serisinin MDS olduğu durumlara bakılsın. Donanımda daha iyi bir kullanım alanı için serideki t_1 ve t_3 elemanları $t_1,t_3 \in \{\alpha,\alpha^2\}, t_1,t_3 \in \{\alpha,\alpha+1\}$ olacak şekilde ele alınır.

1) $\mathbb{F}_2$ üzerinde *n*. dereceden indirgenemez polinomun kökü α olsun ve $\mathbb{F}_{2^n}$ sonlu cismi üzerinde $W=(1,\alpha,1,\alpha^2)$ serisi 4×4 tipinde bir matris olsun. O zaman $n=6$ iken α'nın $x^6+x^5+x^4+x+1=0$ polinomunun kökü olduğu durum dışında $\forall n \geq 5$ için W^4 matrisi MDS matristir.

Diğer yandan $(1,\alpha,1,\alpha^2)^4$ serisi için ε, $\mathbb{F}_{2^n}$'de ilkel bir eleman olmak üzere $\exists i$ tamsayıları ve $\beta \in \mathbb{F}_{2^n}$ için $\beta=\varepsilon^i$ olacak şekilde $\alpha=\beta$ olarak ele alınırsa $(1,\beta,1,\beta^2)^4$ serisi elde edilir. Bu durum

2) $\mathbb{F}_{2^n}$ sonlu cismi üzerinde $W=(1,\beta,1,\beta^2)$ serisi 4×4 tipinde bir matris olsun. Ayrıca $i\in C_s$ olacak şekilde $\beta=\varepsilon^i$ olsun ve ε, $\mathbb{F}_{2^n}$ üzerinde ilkel bir eleman olsun. O zaman $|C_s|\geq5$ ise $|C_s|=6$ iken β'nın minimal polinomu $x^6+x^5+x^4+x+1$ olması durumu dışında W^4 matrisi daima bir MDS matristir.

şeklinde de ifade edilebilir

$\mathbb{F}_2$ üzerinde *n***.** dereceden indirgenemez polinomun kökü α olsun. $\mathbb{F}_{2^n}$ üzerinde $(1,\alpha,1,\alpha+1)^4$ serisi tanımlansın. Bu seri $1\leq n\leq3$ için MDS olmamaktadır. Fakat burada $\beta\in\mathbb{F}_{2^n}$ için $\alpha=\beta$ olarak alınırsa elde edilen $(1,\beta,1,\beta+1)^4$ serisi MDS olur ve aşağıdaki gibi ifade edilebilir.

3) $\mathbb{F}_{2^n}$ sonlu cismi üzerinde $W=(1,\beta,1,\beta+1)$ serisi 4×4 tipinde bir matris olsun. Ayrıca $\varepsilon,\mathbb{F}_{2^n}$'nin herhangi bir ilkel elemanı olsun ve $i\in C_s$ olacak şekilde $\beta=\varepsilon^i$ olsun. O zaman $|C_s|\geq4$ ise W^4 daima bir MDS matristir.

Bu durumda $\exists\beta\in\mathbb{F}_{2^n}$ için $(1,\beta,1,\beta^2)^4$ serisinden elde edilen matris MDS ise $(1,\beta,1,\beta^2)^{-4}$ ve $(1,\beta^2,1,\beta)^4$ serilerinden elde edilen matrisler de ayrıca MDS dir.

2.3.4. $(t_0,1,1,t_3)^4$ serisinin MDS özelliğinin incelenmesi

$1\leq n\leq4$ için, $\mathbb{F}_2$ üzerinde *n*. dereceden indirgenemez polinomun kökü α olmak üzere $\mathbb{F}_{2^n}$'de tanımlanan $W=(\alpha,1,1,\alpha+1),W'=(\alpha+1,1,1,\alpha),Q=(\alpha,1,1,\alpha^2)^4$ $Q'=(\alpha^2,1,1,\alpha)^4$ serilerinden MDS matrisler elde edilemez. Fakat sadece $n=4$ iken α'nın x^4+x+1 polinomunun kökü olduğu durumda $Q=(\alpha,1,1,\alpha^2)^4$ serisinden MDS matris elde edilebilir. Ayrıca keyfi n için $\mathbb{F}_{2^n}$ üzerinde $(t_0,1,1,t_3)^4$ serisinin elemanları $t_0,t_3\in\{\alpha,\alpha^2\}$ şeklinde seçilecek olursa $1\leq n\leq3$ için $\mathbb{F}_{2^n}$ üzerindeki bu

seriden elde edilen matris de incelendiğinde hiçbir MDS matris elde edilmez. Bu yüzden sıfırdan farklı $\beta \in \mathbb{F}_{2^n}$ elemanı için $\alpha = \beta$ olacak şekilde $(\beta,1,1,\beta^2)^4$ serisi incelenir.

1) $Q=(\beta,1,1,\beta^2)^4$ serisi $\mathbb{F}_{2^n}$ üzerinde tanımlı olsun. ε, $\mathbb{F}_{2^n}$'de ilkel eleman olsun. $i \in C_s$ olacak şekilde $\beta = \varepsilon^i$ olsun**.** O zaman $|C_s| \geq 4$ ise $|C_s| = 4$ iken β'nın minimal polinomları $x^4+x^3+x^2+x+1$ ve x^4+x^3+1 olduğu durum dışında ve $|C_s| = 7$ iken β'nın minimal polinomu $x^7+x^6+x^5+x^4+1$ olduğu durum dışında Q^4 her zaman bir MDS matristir

2.3.5. $(1,t_1,1,1,t_4)^5$ serisinin MDS özelliğinin incelenmesi

$t_0,t_1,t_2,t_3,t_4 \in \mathbb{F}_{2^n}$ ve $l=5$ olmak üzere t_0,t_1,t_2,t_3 ve t_4 değerlerinden dördü yada tamamı 1 olursa $(t_0,t_1,t_2,t_3,t_4)^5$ serisinden elde edilecek matrisin MDS olmayacağı Bölüm 2.3.1'dekine benzer şekilde görülebilir. Bu durumda $i \in C_s$ olmak üzere t_i değerlerinden herhangi üçü 1 olduğu zaman elde edilen serinin MDS olma durumuna bakılsın.

1) $\mathbb{F}_2$ üzerinde *n.* dereceden indirgenemez polinomun kökü α olmak üzere $W=(1,\alpha,1,1,\alpha^2)$, $W'=(1,\alpha^2,1,1,\alpha)$ serileri $\mathbb{F}_{2^n}$ üzerinde tanımlansın. O zaman $n=7$ iken α'nın, $x^7+x^3+x^2+x+1$, $x^7+x^6+x^5+x^2+1$, $x^7+x^6+x^5+x^4+1$ ya da $x^7+x^6+x^5+x^4+x^3+x^2+1$ polinomlarının kökü olduğu durumlar dışında ya da $n=8$ iken ve α'nın $x^8+x^7+x^6+x^4+x^3+x^2+1=0$ polinomunun kökü olduğu durum dışında $\forall n \geq 7$ için W^5 matrisi MDS matristir. Ayrıca $n=6$ iken α'nın minimal polinomu x^6+x^5+1 ya da $x^6+x^4+x^3+x+1$ olduğu zaman da W^5 serisi MDS dir. Diğer yandan $W'=(1,\alpha^2,1,1,\alpha)$ serisi için $n=8$ iken

α 'nın $x^8 + x^7 + x^6 + x^4 + x^3 + x^2 + 1 = 0$ polinomunun kökü olduğu durum dışında $\forall n \geq 8$ için W'^5 matrisi MDS matristir.

Verilen bu durumlar dışında $i \in C_s$ olmak üzere t_i değerlerinden herhangi üçü 1 olduğu zaman ve kalan iki değer de $\{\alpha, \alpha^2, \alpha + 1\}$ kümesindeki elemanlardan seçildiği zaman $(t_0, t_1, t_2, t_3, t_4)^5$ serisinden oluşturulacak olan matrisler MDS olmayacaktır.

BÖLÜM 3. DAİRESEL TERSİ KENDİSİ OLAN MDS MATRİSLER

[29] da $n=4,5$ ve $m=4,8$ için inşa edilen dairesel tersi kendisi olan (involutory) MDS matrisler verilmiştir. Bu bölümde, yapılan çalışmanın alt yapısını oluşturan [29] ile ilgili kısa bilgiler verilecektir ve [29] da $n=5$ ve $m=4,8$ için elde edilen 5×5'lik dairesel matrislerin tersi kendisi olma ve MDS olma özelliğine bakılırken izlenen yolun benzeri $n=7$ ve $m=4$ için elde edilen 7×7'lik dairesel matrislerin tersi kendisi olma ve MDS olma özelliklerine bakılırken kullanılacaktır. Bu bölümde verilecek olan tanım, teorem ve yardımcı teoremler için [29] numaralı çalışmaya bakılabilir.

3.1. Hafif-Siklet Dairesel Tersi Kendisi Olan MDS Matrislerin İnşası

Tanım 3.1.1. $x, y \in \mathbb{F}_2^m$ için eğer $W(x+y)=W(x)+W(y)$ ise $W:\mathbb{F}_2^m \to \mathbb{F}_2^m$ yapılan eşlemeye lineer eşleme denir. $\mathbb{F}_2$ üzerinde belirlenen $\mathbb{F}_2^m$'nin bir bazı için $\mathbb{F}_2^m$ üzerindeki bir lineer eşleme $\mathbb{F}_2$ üzerinde bir $m\times m$ matrisi ile temsil edilebilir ve W ile gösterilir.

Tanım 3.1.2. $GL(m,\mathbb{F}_2)$ kümesi, girdileri $\mathbb{F}_2$ üzerinde olan tüm $m\times m$ regüler matrisler kümesini göstermek üzere $W \in GL(m,\mathbb{F}_2)$ ve $x=(x_1,...,x_m)\in \mathbb{F}_2^m$ bir sütun vektörü için $W.x$ çarpımından elde edilecek sütun vektörünü değerlendirmek için gerekli olan XOR işlemlerinin sayısı W^* ile gösterilir. Yani $W(x)=W.x$'deki XOR işlemlerinin sayısı W^*'a eşit olmak üzere W matrisinin $i.$ satırındaki sıfırdan farklı girdilerin sayısı $w(W[i])$ ile gösterilsin. O zaman

$$W^* = \sum_{i=1}^{m} (w(W[\mathrm{i}]) - 1) \text{ dir.}$$

Tanım 3.1.3. $1 \le i, j \le n$ için $R_{i,j}$, $\mathbb{F}_2$ üzerinde $m \times m$ matris olmak üzere her lineer difüzyon $R = \begin{pmatrix} R_{1,1} & R_{1,2} & \cdots & R_{1,n} \\ R_{2,1} & R_{2,2} & \cdots & R_{2,n} \\ \vdots & \vdots & \cdots & \vdots \\ R_{n,1} & R_{n,2} & \cdots & R_{n,n} \end{pmatrix}$ şeklinde bir matris ile gösterilebilir.

Tanım 3.1.4. $1 \le i, j \le n$ ve $1 \le k \le m$ için $R_{i,j}(x_k) = R_{i,j}.x_k$ olmak üzere $X = (x_1, ..., x_n) \in (\mathbb{F}_2^{\,m})^n$ için $R(X) = R.X = (\sum_{i=1}^{n} R_{1,i}(x_i), ..., \sum_{i=1}^{n} R_{n,i}(x_i))$ dir. Bu şekilde tanımlanan bir R lineer difüzyon matrisi için R^2 matrisi $m.n$'nci mertebeden birim matris olmak üzere $\forall X \in (\mathbb{F}_2^{\,m})^n$ için $R \circ R(X) = X$ ise R lineer difüzyonu tersi kendisi olan (involutory) olarak adlandırılır.

Tanım 3.1.5. $1 \le j_1 < ... < j_t \le n$ ve $1 \le k_1 < ... < k_t \le n$ için $J = [j_1, ..., j_t]$ ve $K = [k_1, ..., k_n]$, t uzunluğunda iki dizi olmak üzere R'nin t. mertebeden kare alt matrisleri $R(J, K) = (R_{j_l, k_p}, 1 \le l, p \le t)$ şeklinde tanımlanır.

Burada $R(J, K).(x_1, ..., x_t) = 0$ denkleminin sıfırdan farklı çözümünün olmaması için gerek ve yeter şart $R(J, K)$ matrisinin tam ranklı olmasıdır.

Teorem 3.1.1. $1 \le i, j \le n$ için $R = (R_{i,j})$ olmak üzere R matrisinin girdileri $\mathbb{F}_2$ üzerinde $m \times m$ matrislerdir. O zaman R matrisinin bir MDS matris olması için gerek ve yeter şart R'nin t. mertebeden tüm kare alt matrislerinin $1 \le t \le n$ için tam ranklı olmasıdır.

Yardımcı Teorem 3.1.1. $1 \le i, j \le 4$ için $R_i \in GL(m, \mathbb{F}_2)$ olmak üzere $R = \begin{pmatrix} R_1 & R_2 \\ R_3 & R_4 \end{pmatrix}$ olsun. Eğer $rank(R) = 2m$ ise o zaman $\sum_{i=1}^{4} R_i^* \ge 1$ dir.

İspat: Varsayalım ki $1 \le i \le 4$ için $R_i^* = 0$ olsun. O zaman $1 \le i \le 4$ için R_i regüler olduğu için R_i' nin her satır ve her sütununda tam olarak 1'e eşit tek eleman vardır. Bu ise $\sum_{j=1}^{m} R_i^*[j]$'nin her girdisinin 1'e eşit olduğu anlamına gelir. Bu yüzden $\sum_{i=1}^{2m} R^*[i]$' nin her girdisi 0'a eşittir. Bu da $rank(R) < 2m$ olduğu anlamına gelir.

I birim matris olmak üzere $\mathrm{I}, W, Q, E, U \in GL(m, \mathbb{F}_2)$ için $Circ(\mathrm{I}, W, Q, E, U)$ matrisi 5×5 tipinde dairesel bir matris olsun. Matrisin genel hali

$$Circ(\mathrm{I}, W, Q, E, U) = \begin{pmatrix} \mathrm{I} & W & Q & E & U \\ U & \mathrm{I} & W & Q & E \\ E & U & \mathrm{I} & W & Q \\ Q & E & U & \mathrm{I} & W \\ W & Q & E & U & \mathrm{I} \end{pmatrix}.$$

Bu dairesel matrisin $Circ(\mathrm{I}, W, Q, E, U)$ şekliyle gösterilen karekterizasyonunu basitleştirmek için matrisin tersi kendisi olma özelliği yardımcı olur. Çünkü bu özellik ile $R^2 = \mathrm{I}$ yani $R^2 = Circ(\mathrm{I}, W, Q, E, U).Circ(\mathrm{I}, W, Q, E, U) = Circ(\mathrm{I}, 0, 0, 0, 0)$ olması gerekir. Buradan gerekli işlemlerin yapılması ile

$$\mathrm{I}^2 + WU + UW + QE + EQ = \mathrm{I}$$

$$E^2 + QU + UQ = 0$$

$$W^2 + EU + UE = 0$$

$$U^2 + WQ + QW = 0$$

$$Q^2 + WE + EW = 0$$

eşitlikleri elde edilir. Matrisin elemanları $\mathbb{F}_2$ üzerinde olduğundan bu eşitliklerin sağlaması için $U=W$ ve $E=Q$ olması gerekir. Dolayısıyla $Circ(\mathrm{I},W,Q,E,U)$ şeklindeki matris $Circ(\mathrm{I},W,Q,Q,W)$ şeklindeki matrise dönüşür. Bu dönüşüm ile $W,Q\in GL(m,\mathbb{F}_2)$ için $Circ(\mathrm{I},W,Q,Q,W)$ tipindeki dairesel matrisler araştırılır ve bu durum ile araştırma uzayı da azalmış olur.

Yardımcı Teorem 3.1.2. $W,Q\in GL(m,\mathbb{F}_2)$ için $R=Circ(\mathrm{I},W,Q,Q,W)$ bir dairesel matris olsun. O zaman R matrisinin bir tersi kendisi olan matris olması için gerek ve yeter şart $W^2=WQ+QW=Q^2$ olmasıdır.

İspat: Matris çarpımıyla $R^2=Circ(\mathrm{I},W,Q,Q,W).Circ(\mathrm{I},W,Q,Q,W)$

$=Circ(\mathrm{I}^2,Q^2+QW+WQ,W^2+QW+WQ,W^2+WQ+QW,Q^2+WQ+QW)$

elde edilir.

Diğer yandan R'nin bir tersi kendisi olan matris olması için gerek ve yeter şart $R^2=Circ(\mathrm{I},0,0,0,0)$ olmasıdır. Buradan $Q^2+WQ+QW=0$, $W^2+QW+WQ=0$ denklemleri elde edilir. O zaman R'nin tersi kendisi olan bir matris olması için gerek ve yeter şart $W^2=WQ+QW=Q^2$ olmasıdır.

Yardımcı Teorem 3.1.3. Varsayalım ki $W,Q,E\in GL(m,\mathbb{F}_2)$ matrisleri $\mathbb{F}_2$ üzerinde $m\times m$ regüler matrisler olsun. Bu durumda aşağıdaki ifadeler sağlamaktadır.

1) $\begin{pmatrix}\mathrm{I} & W\\ Q & E\end{pmatrix}$ matrisinin tam ranklı bir matris olması için gerek ve yeter şart $rank(QW+E)=m$ olmasıdır.

2) $\begin{pmatrix}W & \mathrm{I}\\ Q & E\end{pmatrix}$ matrisinin tam ranklı bir matris olması için gerek ve yeter şart $rank(EW+Q)=m$ olmasıdır.

3) $\begin{pmatrix} W & Q \\ \mathrm{I} & E \end{pmatrix}$ matrisinin tam ranklı bir matris olması için gerek ve yeter şart $rank(WE+Q)=m$ olmasıdır.

4) $\begin{pmatrix} W & Q \\ E & \mathrm{I} \end{pmatrix}$ matrisinin tam ranklı bir matris olması için gerek ve yeter şart $rank(QE+W)=m$ olmasıdır.

$R=Circ(\mathrm{I},W,Q,Q,W)$ olsun. Teorem 3.1.1' e göre eğer R dairesel matrisi bir MDS matris ise o zaman onun tüm kare alt matrisleri tam ranklıdır. Yardımcı teorem 3.1.3' e göre 2×2 tüm kare alt matrisler incelenerek aşağıdaki durumlar elde edilir. Eğer R matrisi bir MDS matris ise bu durumda aşağıdaki matrisler regülerdir.

$$W+\mathrm{I}, W^2+\mathrm{I}, Q+\mathrm{I}, Q^2+\mathrm{I}, W^2+Q, W+Q^2, W+Q$$

$W^2+\mathrm{I}$ ve $Q^2+\mathrm{I}$ matrislerinin regüler matrisler olması için gerek ve yeter şart $W+\mathrm{I}$ ve $Q+\mathrm{I}$ matrislerinin regüler olmasıdır. Bu durumda elde edilen koşullar sadeleştirilerek aşağıdaki yeni durum elde edilir.

$$W+\mathrm{I}, Q+\mathrm{I}, W+Q^2, W^2+Q, W+Q$$

Yukarıdaki gözlemler esas alınarak aşağıdaki araştırma stratejisi elde edilir. İlk olarak $\Phi=W,Q$ olmak üzere $rank(\Phi+\mathrm{I})=m$ özelliğini sağlayan W ve Q matrisleri seçilir. Buradan W ve Q matrislerinin aday kümelerini içeren

$$G_{W,Q}=\left\{\Phi:\Phi\in G_{search}\,\middle|\, rank(\Phi+\mathrm{I})=m\right\}$$

kümesi elde edilir. Buradan $W\in G_{W,Q}$ için

$$G_Q=\left\{Q:Q\in G_{W,Q}\,\middle|\, \begin{array}{l} rank(W+Q)=m \wedge rank(W^2+Q)=m \wedge rank(W+Q^2)=m \\ \wedge\ W^2=WQ+QW \wedge W^2=Q^2 \end{array}\right\}$$

kümesindeki koşulları sağlayan Q matrisinin aday kümesi elde edilir. Son olarak $Q \in G_Q$ için R matrisinin teorem 3.1.1 yardımıyla MDS matris olup olmadığı test edilir.

Örneğin; $m = 4$ iken $GL(4, \mathbb{F}_2)$ üzerinde W ve Q matrisleri araştırılır. Bir tersi kendisi olan MDS $Circ(\mathrm{I}, W, Q, Q, W)$ matrisinin bir satırındaki girdilerinin XOR sayıları en az 4 tür. $W^* + Q^* = 2$ olmak üzere $Circ(\mathrm{I}, W, Q, Q, W)$ tersi kendisi olan dairesel MDS matrisler olacak şekilde 24 çift W ve Q matrisi vardır. Bu 24 adet MDS matris $Circ(\mathrm{I}, W, W^T, W^T, W)$ tipindedir ve 12 farklı W matrisi için $Circ(\mathrm{I}, W^T, W, W, W^T)$ tipindedir.

$m = 8$ iken $W^* + Q^* \leq 3$ olmak üzere $GL(8, \mathbb{F}_2)$ üzerinde W ve Q matrisleri araştırılır. Bu şekilde hiçbir tersi kendisi olan MDS matris elde edilmemektedir. Bu yüzden eğer $Circ(\mathrm{I}, W, Q, Q, W)$ bir tersi kendisi olan MDS matris ise o zaman $W^* + Q^* \geq 4$'tür. Buradan aşağıdaki sonuç elde edilir.

Teorem 3.1.2. $Circ(\mathrm{I}, W, Q, Q, W)$ matrisi bir 5×5 tersi kendisi olan MDS matris olacak şekilde $m = 4, 8$ için $W, Q \in GL(m, \mathbb{F}_2)$ matrisleri vardır. Eğer $Circ(\mathrm{I}, W, Q, Q, W)$ matrisi bir tersi kendisi olan MDS matris ise o zaman $W^* + Q^* \geq \frac{m}{2}$ dir.

3.2. 7x7'lik Dairesel Tersi Kendisi Olan Matrislerin İnşası

$m=4$ için $\mathrm{I},W,Q,E,U,Z,F \in GL(4,\mathbb{F}_2)$ ve I birim matris olmak üzere

$$R=Circ(\mathrm{I},W,Q,E,U,Z,F)=\begin{pmatrix} \mathrm{I} & W & Q & E & U & Z & F \\ F & \mathrm{I} & W & Q & E & U & Z \\ Z & F & \mathrm{I} & W & Q & E & U \\ U & Z & F & \mathrm{I} & W & Q & E \\ E & U & Z & F & \mathrm{I} & W & Q \\ Q & E & U & Z & F & \mathrm{I} & W \\ W & Q & E & U & Z & F & \mathrm{I} \end{pmatrix}$$

genel durumu göz önüne alınsın. Bu matristeki karekterizasyonu basitleştirmek için matris incelensin ve bu tipte olan matrislerin nasıl tersi kendisi olan matris olacağına bakılsın. İlk olarak bu genel durum olarak tanımlanan dairesel matrisin tersi kendisi olan matris olması için

$$R^2=Circ(\mathrm{I},W,Q,E,U,Z,F).Circ(\mathrm{I},W,Q,E,U,Z,F)=Circ(\mathrm{I},0,0,0,0,0,0)$$

olması gerekir. Buradan matris çarpımıyla

$$\mathrm{I}^2+WF+QZ+UE+EU+ZQ+FW=\mathrm{I}$$
$$W+W+QF+EZ+U^2+ZE+FQ=0$$
$$Q+W^2+Q+EF+UZ+ZU+FE=0$$
$$E+WQ+QW+E+UF+Z^2+FU=0$$
$$U+WE+Q^2+EW+U+ZF+FZ=0$$
$$Z+WU+QE+EQ+UW+Z+F^2=0$$
$$F+WZ+QU+E^2+UQ+ZW+F=0$$

denklemleri elde edilir. Verilen bu denklemleri basitleştirmek için $F = W$, $Z = Q$, $U = E$ alınarak ve $\mathbb{F}_2$ 'de çalışıldığı da göz önünde bulundurularak

$$\mathrm{I}^2 = \mathrm{I}$$
$$E^2 + QW + WQ + EQ + QE = 0$$
$$W^2 + EW + WE + EQ + QE = 0$$
$$Q^2 + WQ + QW + EW + WE = 0$$

denklemleri elde edilir. Buradan da anlaşılacağı üzere $R = Circ(\mathrm{I}, W, Q, E, U, Z, F) = Circ(\mathrm{I}, W, Q, E, E, Q, W)$ olacağı anlamına gelir. Şimdi aşağıda verilecek olan yardımcı teorem ile 7×7 'lik $R = Circ(\mathrm{I}, W, Q, E, E, Q, W)$ dairesel matrisinin tersi kendisi olan matris olma durumuna bakılsın.

Yardımcı Teorem 3.2.1. $W, Q, E \in GL(4, \mathbb{F}_2)$ olmak üzere $R = Circ(\mathrm{I}, W, Q, E, E, Q, W)$ matrisi bir dairesel matris olsun. O zaman R matrisinin bir tersi kendisi olan matris olması için gerek ve yeter şart $W^2 = WE + EW + QE + EQ$, $Q^2 = WQ + QW + WE + EW$, $E^2 = WQ + QW + QE + EQ$ eşitliklerinin aynı anda sağlanmasıdır.

İspat: $R^2 = Circ(\mathrm{I}, W, Q, E, E, Q, W).Circ(\mathrm{I}, W, Q, E, E, Q, W)$

$$= Circ\begin{pmatrix} \mathrm{I}^2, QW + EQ + E^2 + QE + WQ, W^2 + EW + EQ + QE + WE, WQ + QW + EW + Q^2 + WE, \\ WQ + QW + EW + Q^2 + WE, W^2 + EW + WE + EQ + QE, QW + WQ + EQ + QE + E^2 \end{pmatrix}$$

olur. Buradan R matrisinin bir tersi kendisi olan matris olması için gerek ve yeter şart $R^2 = Circ(\mathrm{I}, 0, 0, 0, 0, 0, 0)$ olmasıdır. Yani

$$\mathrm{I}^2 = \mathrm{I}$$

$$QW + EQ + E^2 + QE + WQ = 0$$

$$W^2 + EW + EQ + QE + WE = 0$$

$$WQ + QW + EW + Q^2 + WE = 0$$

$$WQ + QW + EW + Q^2 + WE = 0$$

$$W^2 + EW + EQ + QE + WE = 0$$

$$QW + EQ + E^2 + QE + WQ = 0$$

olmasıdır. Dolayısıyla R dairesel matrisinin bir tersi kendisi olan matris olması için gerek ve yeter şart $W^2 = WE + EW + QE + EQ$, $Q^2 = WQ + QW + WE + EW$, $E^2 = WQ + QW + QE + EQ$ olmasıdır. Bu durumda bu şartları sağlayan R dairesel matrisi bir tersi kendisi olan matris olacaktır. Bir matrisin MDS matris olabilmesi için onun tüm kare alt matrisleri regüler olmalıdır. O zaman matrisin regüler bir matris olması için aşağıdaki teorem verilsin.

Teorem 3.2.1. [32] Bir M kare matrisinin terslenebilir (regüler) olması için gerek ve yeter şart $M.x = 0$ homojen sisteminin sıfırdan farklı hiçbir çözümünün olmamasıdır.

İspat: Varsayalım ki M^{-1} vardır. O zaman $M.x = 0 \Rightarrow x = M^{-1}.0 = 0$ dır. Böylece eğer M terslenebilirse $M.x = 0$ sıfırdan farklı hiçbir çözüme sahip değildir. Diğer yandan $M.x = 0$ daima $x = 0$ çözümüne sahiptir. Eğer başka hiçbir çözüm yoksa o zaman M her bir pivot elemanla satırca eşelon forma indirgenebilir. Böylece M^{-1} hesaplanabilir.

Buradan teorem 3.2.1 ve yardımcı teorem 3.1.3 yardımıyla $R = Circ(\mathrm{I}, W, Q, E, E, Q, W)$ dairesel matrisinin MDS olup olmayacağına bakılsın.

İlk olarak $W, Q, E \in GL(m, \mathbb{F}_2)$ için $m = 4$ olmak üzere 7×7'lik $R = Circ(\mathrm{I}, W, Q, E, E, Q, W)$ tipinde olan dairesel matrislerin 2×2'lik alt

matrislerinin regüler olup olmayacağına bakılsın. $R = Circ(\mathrm{I}, W, Q, E, E, Q, W)$ dairesel matrisinin $W, Q, E \in GL(4, \mathbb{F}_2)$ matrisleri ile oluşturulan 441 adet 2×2'lik alt matrisi vardır. $W, Q, E \in GL(4, \mathbb{F}_2)$ ve $X = (x_1, ..., x_7) \in (\mathbb{F}_2^{\,4})^7$ olmak üzere R dairesel matrisinin 2×2'lik alt matrislerinin regüler matris olup olmadığı durumlara yardımcı teorem 3.1.3 yardımıyla bakılır ve elde edilen durumlar içerisinden aşağıdaki belirsizlik arz eden durumlar elde edilir.

$$(W+Q).x_1+(Q+E).x_5=0 \qquad (W+E).x_1+(Q+E).x_2=0$$
$$(W+Q).x_1+(Q+E).x_7=0 \qquad (W+E).x_1+(Q+E).x_3=0$$
$$(W+Q).x_1+(Q+E).x_2=0 \qquad (W+E).x_1+(Q+E).x_6=0$$
$$(W+Q).x_1+(Q+E).x_4=0 \qquad (W+E).x_1+(Q+E).x_7=0$$
$$(W+Q).x_2+(Q+E).x_3=0 \qquad (W+E).x_2+(Q+E).x_1=0$$
$$(W+Q).x_2+(Q+E).x_5=0 \qquad (W+E).x_2+(Q+E).x_3=0$$
$$(W+Q).x_2+(Q+E).x_6=0 \qquad (W+E).x_2+(Q+E).x_4=0$$
$$(W+Q).x_2+(Q+E).x_1=0 \qquad (W+E).x_2+(Q+E).x_7=0$$
$$(W+Q).x_3+(Q+E).x_4=0 \qquad (W+E).x_3+(Q+E).x_4=0$$
$$(W+Q).x_3+(Q+E).x_6=0 \qquad (W+E).x_3+(Q+E).x_5=0$$
$$(W+Q).x_3+(Q+E).x_2=0 \qquad (W+E).x_3+(Q+E).x_1=0$$
$$(W+Q).x_3+(Q+E).x_7=0 \qquad (W+E).x_3+(Q+E).x_2=0$$
$$(W+Q).x_4+(Q+E).x_5=0 \qquad (W+E).x_4+(Q+E).x_2=0$$
$$(W+Q).x_4+(Q+E).x_7=0 \qquad (W+E).x_4+(Q+E).x_3=0$$
$$(W+Q).x_4+(Q+E).x_1=0 \qquad (W+E).x_4+(Q+E).x_5=0$$
$$(W+Q).x_4+(Q+E).x_3=0 \qquad (W+E).x_4+(Q+E).x_6=0$$
$$(W+Q).x_5+(Q+E).x_1=0 \qquad (W+E).x_5+(Q+E).x_3=0$$
$$(W+Q).x_5+(Q+E).x_6=0 \qquad (W+E).x_5+(Q+E).x_4=0$$
$$(W+Q).x_5+(Q+E).x_2=0 \qquad (W+E).x_5+(Q+E).x_6=0$$
$$(W+Q).x_5+(Q+E).x_4=0 \qquad (W+E).x_5+(Q+E).x_7=0$$
$$(W+Q).x_6+(Q+E).x_3=0 \qquad (W+E).x_6+(Q+E).x_1=0$$
$$(W+Q).x_6+(Q+E).x_2=0 \qquad (W+E).x_6+(Q+E).x_4=0$$
$$(W+Q).x_6+(Q+E).x_7=0 \qquad (W+E).x_6+(Q+E).x_5=0$$
$$(W+Q).x_6+(Q+E).x_5=0 \qquad (W+E).x_6+(Q+E).x_7=0$$
$$(W+Q).x_7+(Q+E).x_4=0 \qquad (W+E).x_7+(Q+E).x_1=0$$
$$(W+Q).x_7+(Q+E).x_6=0 \qquad (W+E).x_7+(Q+E).x_2=0$$
$$(W+Q).x_7+(Q+E).x_1=0 \qquad (W+E).x_7+(Q+E).x_5=0$$
$$(W+Q).x_7+(Q+E).x_3=0 \qquad (W+E).x_7+(Q+E).x_6=0$$

$$(W+Q).x_1+(W+E).x_3=0$$
$$(W+Q).x_1+(W+E).x_4=0$$
$$(W+Q).x_1+(W+E).x_5=0$$
$$(W+Q).x_1+(W+E).x_6=0$$
$$(W+Q).x_2+(W+E).x_4=0$$
$$(W+Q).x_2+(W+E).x_5=0$$
$$(W+Q).x_2+(W+E).x_6=0$$
$$(W+Q).x_2+(W+E).x_7=0$$
$$(W+Q).x_3+(W+E).x_1=0$$
$$(W+Q).x_3+(W+E).x_5=0$$
$$(W+Q).x_3+(W+E).x_6=0$$
$$(W+Q).x_3+(W+E).x_7=0$$
$$(W+Q).x_4+(W+E).x_1=0$$
$$(W+Q).x_4+(W+E).x_2=0$$
$$(W+Q).x_4+(W+E).x_6=0$$
$$(W+Q).x_4+(W+E).x_7=0$$
$$(W+Q).x_5+(W+E).x_1=0$$
$$(W+Q).x_5+(W+E).x_2=0$$
$$(W+Q).x_5+(W+E).x_3=0$$
$$(W+Q).x_5+(W+E).x_7=0$$
$$(W+Q).x_6+(W+E).x_1=0$$
$$(W+Q).x_6+(W+E).x_2=0$$
$$(W+Q).x_6+(W+E).x_3=0$$
$$(W+Q).x_6+(W+E).x_4=0$$
$$(W+Q).x_7+(W+E).x_2=0$$
$$(W+Q).x_7+(W+E).x_3=0$$
$$(W+Q).x_7+(W+E).x_4=0$$
$$(W+Q).x_7+(W+E).x_5=0$$

Bir matrisin MDS matris olması için bütün alt kare matrislerinin terslenebilir olması gerekir ve bu alt kare matrislerden herhangi biri bu şartı sağlamaz ise matris MDS matris olmaz. Teorem 3.2.1'de de olduğu gibi bir W kare matrisinin regüler olması için gerek ve yeter şart $W.x=0$ homojen denkleminin sadece $x=0$ çözümüne sahip olmasıdır.

Fakat yukarıda elde edilen durumlarda teorem 3.2.1'de verilen durum söz konusu olamayacağından dolayı $W,Q,E \in GL(4,\mathbb{F}_2)$ matrislerinden elde edilen $(W+Q)$, $(W+E)$, $(Q+E)$ tipindeki matrislerin regüler olma durumundan bahsedilemez. Dolayısıyla 2×2' lik alt matrislerin hepsi regüler olmaz. Diğer yandan 3×3, 4×4, 5×5, 6×6, 7×7'lik alt kare matrislerin regüler olma durumuna teorem 3.1.1 yardımıyla bakılmaktadır. Fakat 2×2' lik alt matrislerin tümü regüler olmadığından bu tipteki matrislerin regüler olma durumunun bakılmasına da gerek duyulmayacaktır. Bu durumda R matrisi bir MDS matris olamaz.

Buradan sonuç olarak tersi kendisi olan fakat MDS olmayan bir $R = Circ(\mathrm{I},W,Q,E,E,Q,W)$ dairesel matrisi elde edilir. Ayrıca $R = Circ(\mathrm{I},W,Q,E,E,Q,W)$ dairesel matrisinden tersi kendisi olan matrisleri bulduran algoritma magma ile yazılmış olup ekte verilmiştir.

BÖLÜM 4. SONUÇLAR VE ÖNERİLER

Kriptoloji ile ilgili ve bu alanda kullanılan MDS matrisler ile ilgili yapılan çalışmalar hakkında bilgiler verildi. 5×5 tipindeki dairesel tersi kendisi olan MDS matrisleri elde etmek için kullanılan yöntem incelendi. Sonra ilk olarak 7×7 tipindeki dairesel matrisin genel hali elde edildi ve tersi kendisi olma özelliği sağlatıldı. Daha sonra bu matrisin MDS matris olup olmama durumuna bakıldı ve bu matristen 7×7 tipinde MDS matrisler elde edilemeyeceği görüldü.

Yapılacak olan daha ileri çalışmalar ile incelemeler yapılabilir.

KAYNAKLAR

[1] Sakallı, M.T., Yavuzer Aslan, F., Blok Şifrelerde Kullanılan Doğrusal Dönüşüm Yapılarının İncelenmesi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği, 2012.

[2] Galovich,S., Intoduction to Mathematical Structures, Routledge, 2002.

[3] Fraleigh,J., A First Course In Abstract Algebra, Pearson Education, 2003.

[4] Hungerford, Thomas W., Algebra, Springer, 2000.

[5] Çallıalp, F., Örneklerle Soyut Cebir, Birsen Yayınevi, 2009.

[6] Wan, Zhe X., Finite Fields and Galois Rings, World Scientific, 2012.

[7] Lidl, R., Niederreiter, H., Introduction to Finite Fields And Their Applications, Cambridge University Press, 1986.

[8] Hill, R., Kolman, B., Elementary Lineer Algebra, Prentice Hall, 2000.

[9] Roman, S., Advanced Lineer Algebra, Graduate Texts in Mathematics, Springer, 2000.

[10] Sabuncuoğlu A., Lineer Cebir, Nobel Yayın, 2008.

[11] http://bilgisayarkavramlari.sadievrenseker.com/2012/04/16/matrisin-derecesi-matrix-rank/, Erişim Tarihi : 11.10.2016.

[12] Taşçı D.,Lineer Cebir, Gazi Kitabevi, 2005.

[13] ÇETİN, N., ORHUN, N., Lineer Cebir, Anadolu Üniversitesi Yayınları No:1074, Açıköğretim Fakültesi Yayınları No:589, 1998.

[14] Gupta, K.C., Ray, I.G., On Constructions of Involutory MDS Matrices. In AFRICACRYPT 2013, pp. 43-60, Springer, 2013.

[15] http://mathworld.wolfram.com/CompanionMatrix.html, Erişim Tarihi : 09.02.2017.

[16] Roman, S., Coding and Information Theory, Graduate Texts in Mathematics, Springer Verlag, 1992.

[17] Ling, S., Xing, C., Coding Theory, Cambridge University Press, 2004.

[18] Berger, T.P., Construction of Recursive MDS Diffusion Layers from Gabidulin Codes, INDOCRYPT 2013, LNCS, vol. 8250, pp. 274-285, Springer, 2013.

[19] MacWilliams, F.J., Sloane, N.J.A., The Theory of Error-Correcting Codes, North Holland Publishing Co., 1998.

[20] Zhao, R., Zhang, R., Li, Y., Wu, B., On Constructions of a Sort of MDS Block Diffusion Matrices for Block Ciphers and Hash Functions, IACR Cryptology ePrint Archive . 2015.

[21] Paar, C., Pelzl, J., Understanding Cryptography, Springer Verlag, 2010.

[22] Sajadieh, M., Dakhilalian, M., Mala, H., Sepehrdad, P., Recursive Diffusion Layers for Block Ciphers and Hash Functions, FSE 2012, LNCS, vol. 7549, pp. 385-401, Springer, 2012.

[23] Augot, D., Finiasz, M., Exhaustive Search for Small Dimension Recursive MDS Diffusion Layers for Block Ciphers and Hash Functions, In ISIT, pp. 1551-1555, 2013.

[24] Youssef, A.M., Mister, S., Tavares, S.E., On the Design of Linear Transformations for Substitution Permutation Encryption Networks, SAC'97, pp. 1-9, 1997.

[25] Nakara Jr, J., Abrahao, E., A New Involutory MDS Matrix for the AES. International Journal of Network Security, vol. 9(2), pp. 109-116, 2009.

[26] Lacan, J., Fimes, J., Systematic MDS Erasure Codes Based on Vandermonde Matrices. IEEE Trans. Commun. Lett., vol 8(9), pp. 570-572, 2004.

[27] Sajadieh, M., Dakhilalian, M., Mala, H., Omoomi, B., On Construction of Involutory MDS Matrices from Vandermonde Matrices in $GF(2^q)$, Des. Codes Cryptogr., vol. 64, pp. 287-308, Springer, 2012.

[28] Gupta, K.C., Ray, I.G., On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography, CD-ARES 2013 Workshops, LNCS, vol. 8128, pp. 29-43, Springer, 2013.

[29] Li, Y., Wang, M., On the Constructions of Lightweight Circulant Involutory MDS Matrices. In: FSE. LNCS, Springer, 2016.

[30] Bai, J., Wang, D., The Lightest 4×4 MDS Matrices over $GL(4,\mathbb{F}_2)$. Cryptology ePrint Archive: Report 2016/1131, 2016.

[31] Sim, S.M., Khoo, K., Oggier, F., Peyrin, T., Lightweight MDS Involution Matrices, In: Leander, G., Demirci, H. (eds.) FSE 2015, LNCS, Springer, 2015.

[32] Cherney, D., Denton, T., Thomas, R., Waldron, A., Linear Algebra. pp. 154, Davis California, 2013.

EKLER

```
K := GF(2);
boy := 7;
MR1 := MatrixRing(K, 4);
MR4 := MatrixRing(MR1, boy);
function by_one(block)
        k := #block;
        block := block cat block;
        block2 := [];
        for i := 1 to k do
           block2[i] := block[(i+boy-1)];
        end for;
        return block2;
end function;
function Circulant(block)
        k := #block;
        blocks := [];
        Append(~blocks,block);
        for i := 1 to k-1 do
           block := by_one(block);
           Append(~blocks,block);
        end for;
        return blocks;
end function;
function isMDS(M,boy)
S := {1..boy};
for s1 in Subsets(S,2) do
   i1 := Setseq(s1)[1];
   i2 := Setseq(s1)[2];
   for s2 in Subsets(S,2) do
      j1 := Setseq(s2)[1];
      j2 := Setseq(s2)[2];
      W1 := HorizontalJoin(M[i1][j1],M[i1][j2]);
      W2 := HorizontalJoin(M[i2][j1],M[i2][j2]);
      W :=  VerticalJoin(W1,W2);
```

```
        if IsSingular(W) then return false; end if;
    end for;
end for;
for s1 in Subsets(S,3) do
    i1 := Setseq(s1)[1];
    i2 := Setseq(s1)[2];
    i3 := Setseq(s1)[3];
    for s2 in Subsets(S,3) do
        j1 := Setseq(s2)[1];
        j2 := Setseq(s2)[2];
        j3 := Setseq(s2)[3];
       P1 := [M[i1][j1],M[i1][j2],M[i1][j3]];
        P2 := [M[i2][j1],M[i2][j2],M[i2][j3]];
        P3 := [M[i3][j1],M[i3][j2],M[i3][j3]];
        W1 := HorizontalJoin(P1);
        W2 := HorizontalJoin(P2);
        W3 := HorizontalJoin(P3);
        P := [W1,W2,W3];
        W := VerticalJoin(P);
        if IsSingular(W) then return false; end if;
    end for;
end for;
for s1 in Subsets(S,4) do
    i1 := Setseq(s1)[1];
    i2 := Setseq(s1)[2];
    i3 := Setseq(s1)[3];
    i4 := Setseq(s1)[4];
    for s2 in Subsets(S,4) do
        j1 := Setseq(s2)[1];
        j2 := Setseq(s2)[2];
        j3 := Setseq(s2)[3];
        j4 := Setseq(s2)[4];
        P1 := [M[i1][j1],M[i1][j2],M[i1][j3],M[i1][j4]];
        P2 := [M[i2][j1],M[i2][j2],M[i2][j3],M[i2][j4]];
        P3 := [M[i3][j1],M[i3][j2],M[i3][j3],M[i3][j4]];
        P4 := [M[i4][j1],M[i4][j2],M[i4][j3],M[i4][j4]];
        W1 := HorizontalJoin(P1);
        W2 := HorizontalJoin(P2);
        W3 := HorizontalJoin(P3);
        W4 := HorizontalJoin(P4);
        P := [W1,W2,W3,W4];
        W := VerticalJoin(P);
```

```
      if IsSingular(W) then  return false; end if;
   end for;
end for;
//5 için:
for s1 in Subsets(S,5) do
   i1 := Setseq(s1)[1];
   i2 := Setseq(s1)[2];
   i3 := Setseq(s1)[3];
   i4 := Setseq(s1)[4];
   i5 := Setseq(s1)[5];
   for s2 in Subsets(S,5) do
      j1 := Setseq(s2)[1];
      j2 := Setseq(s2)[2];
      j3 := Setseq(s2)[3];
      j4 := Setseq(s2)[4];
      j5 := Setseq(s2)[5];
      P1 := [M[i1][j1],M[i1][j2],M[i1][j3],M[i1][j4],M[i1][j5]];
      P2 := [M[i2][j1],M[i2][j2],M[i2][j3],M[i2][j4],M[i2][j5]];
      P3 := [M[i3][j1],M[i3][j2],M[i3][j3],M[i3][j4],M[i3][j5]];
      P4 := [M[i4][j1],M[i4][j2],M[i4][j3],M[i4][j4],M[i4][j5]];
      P5 := [M[i5][j1],M[i5][j2],M[i5][j3],M[i5][j4],M[i5][j5]];
      W1 := HorizontalJoin(P1);
      W2 := HorizontalJoin(P2);
      W3 := HorizontalJoin(P3);
      W4 := HorizontalJoin(P4);
      W5 := HorizontalJoin(P5);
      P := [W1,W2,W3,W4,W5];
      W := VerticalJoin(P);
      if IsSingular(W) then  return false; end if;
   end for;
end for;
//6 için:
for s1 in Subsets(S,6) do
   i1 := Setseq(s1)[1];
   i2 := Setseq(s1)[2];
   i3 := Setseq(s1)[3];
   i4 := Setseq(s1)[4];
   i5 := Setseq(s1)[5];
   i6 := Setseq(s1)[6];
   for s2 in Subsets(S,6) do
      j1 := Setseq(s2)[1];
      j2 := Setseq(s2)[2];
```

```
      j3 := Setseq(s2)[3];
      j4 := Setseq(s2)[4];
      j5 := Setseq(s2)[5];
      j6 := Setseq(s2)[6];
      P1 := [M[i1][j1],M[i1][j2],M[i1][j3],M[i1][j4],M[i1][j5],M[i1][j6]];
      P2 := [M[i2][j1],M[i2][j2],M[i2][j3],M[i2][j4],M[i2][j5],M[i2][j6]];
      P3 := [M[i3][j1],M[i3][j2],M[i3][j3],M[i3][j4],M[i3][j5],M[i3][j6]];
      P4 := [M[i4][j1],M[i4][j2],M[i4][j3],M[i4][j4],M[i4][j5],M[i4][j6]];
      P5 := [M[i5][j1],M[i5][j2],M[i5][j3],M[i5][j4],M[i5][j5],M[i5][j6]];
      P6 := [M[i6][j1],M[i6][j2],M[i6][j3],M[i6][j4],M[i6][j5],M[i6][j6]];
      W1 := HorizontalJoin(P1);
      W2 := HorizontalJoin(P2);
      W3 := HorizontalJoin(P3);
      W4 := HorizontalJoin(P4);
      W5 := HorizontalJoin(P5);
      W6 := HorizontalJoin(P6);
     P := [W1,W2,W3,W4,W5,W6];
      W := VerticalJoin(P);
      if IsSingular(W) then  return false; end if;
   end for;
end for;
//7 için:
for s1 in Subsets(S,7) do
   i1 := Setseq(s1)[1];
   i2 := Setseq(s1)[2];
   i3 := Setseq(s1)[3];
   i4 := Setseq(s1)[4];
   i5 := Setseq(s1)[5];
   i6 := Setseq(s1)[6];
   i7 := Setseq(s1)[7];
   for s2 in Subsets(S,7) do
      j1 := Setseq(s2)[1];
      j2 := Setseq(s2)[2];
      j3 := Setseq(s2)[3];
      j4 := Setseq(s2)[4];
      j5 := Setseq(s2)[5];
      j6 := Setseq(s2)[6];
      j7 := Setseq(s2)[7];
      P1 := [M[i1][j1],M[i1][j2],M[i1][j3],M[i1][j4],M[i1][j5],M[i1][j6],M[i1][j7]];
      P2 := [M[i2][j1],M[i2][j2],M[i2][j3],M[i2][j4],M[i2][j5],M[i2][j6],M[i2][j7]];
      P3 := [M[i3][j1],M[i3][j2],M[i3][j3],M[i3][j4],M[i3][j5],M[i3][j6],M[i3][j7]];
      P4 := [M[i4][j1],M[i4][j2],M[i4][j3],M[i4][j4],M[i4][j5],M[i4][j6],M[i4][j7]];
```

```
      P5 := [M[i5][j1],M[i5][j2],M[i5][j3],M[i5][j4],M[i5][j5],M[i5][j6],M[i5][j7]];
      P6 := [M[i6][j1],M[i6][j2],M[i6][j3],M[i6][j4],M[i6][j5],M[i6][j6],M[i6][j7]];
      P7 := [M[i7][j1],M[i7][j2],M[i7][j3],M[i7][j4],M[i7][j5],M[i7][j6],M[i7][j7]];
      W1 := HorizontalJoin(P1);
      W2 := HorizontalJoin(P2);
      W3 := HorizontalJoin(P3);
      W4 := HorizontalJoin(P4);
      W5 := HorizontalJoin(P5);
      W6 := HorizontalJoin(P6);
      W7 := HorizontalJoin(P7);
      P := [W1,W2,W3,W4,W5,W6,W7];
      W := VerticalJoin(P);
      if IsSingular(W) then  return false; end if;
   end for;
end for;
return true;
end function;
function BinFor(M,boy)
   S := {1..boy};
for s1 in Subsets(S,7) do
   i1 := Setseq(s1)[1];
   i2 := Setseq(s1)[2];
   i3 := Setseq(s1)[3];
   i4 := Setseq(s1)[4];
   i5 := Setseq(s1)[5];
   i6 := Setseq(s1)[6];
   i7 := Setseq(s1)[7];
   for s2 in Subsets(S,7) do
      j1 := Setseq(s2)[1];
      j2 := Setseq(s2)[2];
      j3 := Setseq(s2)[3];
      j4 := Setseq(s2)[4];
      j5 := Setseq(s2)[5];
      j6 := Setseq(s2)[6];
      j7 := Setseq(s2)[7];
      P1 := [M[i1][j1],M[i1][j2],M[i1][j3],M[i1][j4],M[i1][j5],M[i1][j6],M[i1][j7]];
      P2 := [M[i2][j1],M[i2][j2],M[i2][j3],M[i2][j4],M[i2][j5],M[i2][j6],M[i2][j7]];
      P3 := [M[i3][j1],M[i3][j2],M[i3][j3],M[i3][j4],M[i3][j5],M[i3][j6],M[i3][j7]];
      P4 := [M[i4][j1],M[i4][j2],M[i4][j3],M[i4][j4],M[i4][j5],M[i4][j6],M[i4][j7]];
      P5 := [M[i5][j1],M[i5][j2],M[i5][j3],M[i5][j4],M[i5][j5],M[i5][j6],M[i5][j7]];
      P6 := [M[i6][j1],M[i6][j2],M[i6][j3],M[i6][j4],M[i6][j5],M[i6][j6],M[i6][j7]];
      P7 := [M[i7][j1],M[i7][j2],M[i7][j3],M[i7][j4],M[i7][j5],M[i7][j6],M[i7][j7]];
```

```
        W1 := HorizontalJoin(P1);
        W2 := HorizontalJoin(P2);
        W3 := HorizontalJoin(P3);
        W4 := HorizontalJoin(P4);
        W5 := HorizontalJoin(P5);
        W6 := HorizontalJoin(P6);
        W7 := HorizontalJoin(P7);
        P := [W1,W2,W3,W4,W5,W6,W7];
        W := VerticalJoin(P);
    end for;
end for;
return W;
end function;
function xor_say(W)
        say := 0;
        satir := Nrows(W);
        sutun := Ncols(W);
        for i := 1 to satir do
            for j := 1 to sutun do
                if W[i][j] eq 1 then
                  say := say+1;
                end if;
            end for;
            say := say-1;
         end for;
         return say;
end function;
NonSing := [];
for M in MatrixRing(K, 4) do
    if not IsSingular(M) then
       Append(~NonSing,M);
    end if;
end for;
#NonSing;
Id := [[1,0,0,0],[0,1,0,0],[0,0,1,0],[0,0,0,1]];
I := MR1 ! Id;
counter := 0;
for W in NonSing do
    for Q in NonSing do
        for E in NonSing do
            if W^2 eq W*E + E*W + E*Q + Q*E and
              Q^2 eq W*Q + Q*W + W*E + E*W and
```

```
            E^2 eq W*Q + Q*W + Q*E + E*Q
            then
              block := [I,W,Q,E,E,Q,W];
              M := MR4 ! Circulant(block);
              BinFor(M,boy)^2 eq ScalarMatrix(K,28,1);
              if isMDS(M,boy) then
                 W,Q,E;
              end if;
          end if;
        end for;
    end for;
end for;
counter;
```

ÖZGEÇMİŞ

1990 yılında Karabük'te doğdu. İlk, orta ve lise eğitimini Karabük'te tamamladı. 2008 yılında Azerbaycan Bakü Devlet Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'nde lisans eğitimine başladı. 2010 yılında Sakarya Üniversitesi Fen Edebiyat Fakültesi Matematik Bölümü'ne yatay geçiş yaptı. 2013 yılı yaz döneminde Matematik Bölümü'nden mezuniyete hak kazandı. 2014 yılında Sakarya Üniversitesi'nde Matematik Anabilim Dalı'nda yüksek lisans eğitimine başlayıp eğitimine burada devam etti.