T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAFİF SIKLET KRİPTOGRAFİ İÇİN İNVOLUTİF MDS MATRİS UYGULAMALARI

YÜKSEK LİSANS TEZİ

Tuğçe TUFANÇLI

Matematik Anabilim Dalı

Cebir ve Sayılar teorisi Bilim Dalı

OCAK 2024

T.C.
SAKARYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAFİF SIKLET KRİPTOGRAFİ İÇİN İNVOLUTİF MDS MATRİS UYGULAMALARI

YÜKSEK LİSANS TEZİ

Tuğçe TUFANÇLI

Matematik Anabilim Dalı

Cebir ve Sayılar teorisi Bilim Dalı

Tez Danışmanı: Prof. Dr. Mehmet ÖZEN

OCAK 2024

Tuğçe Tufançlı tarafından hazırlanan “Hafif Sıklet Kriptografi İçin İnvolutif MDS Matris Uygulamaları” adlı tez çalışması 25.01.2024 tarihinde aşağıdaki jüri tarafından oy birliği ile Sakarya Üniversitesi Fen Bilimleri Enstitüsü Matematik Anabilim Dalı **Cebir ve Sayılar teorisi** Bilim Dalı’nda Yüksek Lisans tezi olarak kabul edilmiştir.

Tez Jürisi

Jüri Başkanı :

Jüri Üyesi :

Jüri Üyesi :

ETİK İLKE VE KURALLARA UYGUNLUK BEYANNAMESİ

Sakarya Üniversitesi Fen Bilimleri Enstitüsü Lisansüstü Eğitim-Öğretim Yönetmeliğine ve Yükseköğretim Kurumları Bilimsel Araştırma ve Yayın Etiği Yönergesine uygun olarak hazırlamış olduğum "Hafif Sıklet Kriptografi İçin İnvolutif Mds Matrisin Bazı Uygulamaları" başlıklı tezin bana ait, özgün bir çalışma olduğunu; çalışmamın tüm aşamalarında yukarıda belirtilen yönetmelik ve yönergeye uygun davrandığımı, tezin içerdiği yenilik ve sonuçları başka bir yerden almadığımı, tezde kullandığım eserleri usulüne göre kaynak olarak gösterdiğimi, bu tezi başka bir bilim kuruluna akademik amaç ve unvan almak amacıyla vermediğimi ve 20.04.2016 tarihli Resmi Gazete'de yayımlanan Lisansüstü Eğitim ve Öğretim Yönetmeliğinin 9/2 ve 22/2 maddeleri gereğince Sakarya Üniversitesi'nin abonesi olduğu intihal yazılım programı kullanılarak Enstitü tarafından belirlenmiş ölçütlere uygun rapor alındığını, çalışmamla ilgili yaptığım bu beyana aykırı bir durumun ortaya çıkması halinde doğabilecek her türlü hukuki sorumluluğu kabul ettiğimi beyan ederim.

(25/01/2024)

Tuğçe TUFANÇLI

TEŞEKKÜR

Yüksek Lisans tez çalışmamda bilgisini ve tecrübesini esirgemeyip bana her zaman destek olan danışmanım sayın Prof. Dr. Mehmet ÖZEN'e teşekkürlerimi bir borç bilirim.

Her ihtiyacım olduğunda bana yardımcı olan, çalışmama yaptığı bilimsel katkı ve önerileri için Araş. Gör. Serra SAZOĞLU'na teşekkürlerimi sunarım.

Her zaman arkamda durup bana destek olan yol arkadaşım, canım eşim Sedat'a, üzerimde emeği çok olan aileme teşekkür ederim.

Tuğçe TUFANÇLI

İÇİNDEKİLER

Sayfa

KISALTMALAR

AES :Advanced Encryption Standart

GF :Galois Cismi

GH : Genelleştirilmiş Hadamard

MDS : Maximum Distances Seperable

XOR : Exclusive Or(Özel veya)

SİMGELER

C	: Kod
F	: Cisim
$\boldsymbol{F_{q^n}}$	: q bir asal sayı olmak üzere q^n elemanlı sonlu cisim
Circ()	: Dairesel Matris
Det()	: Determinant
d(C)	: C kodunun minimum uzaklığı
w(t)	: Hamming Ağırlık
⇨	: İse
∀	: Her
∃	:En az bir(bazı)

TABLO LİSTESİ

Sayfa

HAFİF SIKLET KRİPTOGRAFİ İÇİN İNVOLUTİF MDS MATRİS UYGULAMALARI

ÖZET

Kaynak kısıtlı cihazlar(akıllı kartlar, radyo frekansı, tanımlama etiketleri(RFD), kablosuz sensör düğümleri ve Nesnelerin İnterneti(IoT)) günlük hayatımızda önemli bir yer edinmektedir. Yani kaynak kasıtlı dediğimiz yüksek oranda en aza indirilmiş güç tüketimi, düşük işlem gücü ihtiyacı, düşük bellek kapasitesi tüketimi ve düşük güç kaynağı kullanımıdır. Bu teknolojiler bize kolaylık sağladığı gibi bazı riskleri de beraberinde getirmiştir. Bu riskleri ortadan kaldırmak için kriptografik algoritmaların hayatımıza girişi kaçınılmaz olmuştur. Oluşabilecek olumsuz durumları en aza indirebilmek için hafif sıklet(lightweight) şifreleme algoritmaları kullanılmaktadır.

Hafif sıklet blok şifrelerin yayılım tabakalarında maksimum uzaklığa ayrılabilen matrisler (MDS) kullanılır. MDS kodlarından türetilen MDS matrisleri kriptografik ilkelerin özelliklerini geliştirir, diferansiyel ve lineer kriptanalize karşı güvenlik sağlamaya yardımcı olur. Ayrıca minimum XOR sayısına sahip ,tersi kendine eşit yani involutif MDS matrisleri şifreleme ve şifre çözmede aynı matrisin kullanımına olanak sağladığı için hem daha düşük maliyete sahiptir hem de alan olarak daha az yer kaplamaktadır.

MDS matrislerini oluşturma yöntemleri iki gruba ayrılabilir. Bunlardan birincisi doğrudan oluşturma yöntemleri ve ikincisi ise arama tabanlı yöntemlerdir. İlk yöntem Cauchy matrisi, Vandermonde matrisi, tamamlayıcı matrisler ve kısaltılmış BCH kodlarına ve çarpık özyinelemeli yapılara dayanan yöntemdir. İkinci yöntem ise özyinelemeli yapılar, hibrit yapılar ve özel matris formlarıdır. Verimlilik sağlayan en kolay inşa yöntemlerinden biri için dairesel ve sonlu cisimde Hadamard matrisleri gibi özel matris formları kullanılır.

Bu çalışmada hafif sıklet blok şifreler de kullanılan MDS matrislerin üretilmesi için çalışmalar yapılmıştır. İnvolutif MDS matris,XOR sayısı, Genelleştirilmiş Hadamard (GHadamard) ve Cauchy tabanlı Hadamard (Hadamard-Cauchy) matris formları hakkında bilgi vererek ardından uygulamalara geçilmiştir. F_{2^4} sonlu cisminde $x^4 + x + 1$ indirgenemez polinomunu kullanarak Genelleştirilmiş Hadamard matris formu ile $4x4$ involutif MDS matris oluşturulmuştur. F_{2^6} sonlu cismi üzerinde $x^6 + x + 1$ ve $x^6 + x^3 + 1$ indirgenemez polinomları kullanılarak Genelleştirilmiş Hadamard matris formu ve Cauchy tabanlı Hadamard matris formu ile birlikte $4x4$ involutif MDS matrisler elde edilmiştir. F_{2^7} sonlu cisminde ise $x^7 + x + 1$ ve $x^7 + x^3 + 1$ indirgenemez polinomları ile Genelleştirilmiş Hadamard matris formu ve Cauchy tabanlı Hadamard matris formu kullanılarak $4x4$ involutif MDS matrsileri oluşturulmuştur. Daha sonra elde ettiğimiz bu matrislerin XOR sayılarını hesaplanmıştır. Böylece F_{2^4}, F_{2^6} ve F_{2^7} sonlu cisimleri üzerinde bazı özel matris formları yardımıyla $4x4$ involutif MDS matrisleri elde edilmiştir. Ayrıca elde ettiğimiz matrsilerin XOR sayıları da hesaplanmıştır. Bazı uygulamalarımızda oluşturuğumuz matrislerden izomorfizma yardımıyla yeni $4x4$ involutif MDS

matrisleri elde edilmiştir. Bu yeni oluşturduğumuz matrislerin de XOR sayıları hesaplanarak iki matrisin XOR sayısını kıyaslama şansı elde edilmiştir.

INVOLUTORY MDS MATRIX APPLICATIONS FOR LIGHTWEIGHT CRYPTOGRAPHY

SUMMARY

The use of resource-constrained devices (smart cards, radio frequency identification tags (RFD), wireless sensor nodes and the Internet of Things (IoT)) is increasing. So what we call resource-intentional is significantly reduced power consumption, less computational power requirements, less memory capacity consumption and less power supply utilization. While these technologies have brought us convenience, they have also brought some risks. To eliminate these risks, the use of cryptographic algorithms has become inevitable. Especially in resource-constrained devices such as IoT (Internet of Things) WSNs (Wireless Sensor Networks), RFID (Radio Frequency Identification) tags, lightweight encryption algorithms are used to minimize risks.

Today, billions of users communicate with each other over insecure communication media. sharing a myriad of information. In this insecure environment, cryptography ensures that information is complete, accurate and guarantees that the message is received in its entirety, because in practice it is not enough just to keep it confidential, it is also important to keep the content of the message it must be determined whether it has been modified.

To establish a secure communication channel between the transmitter and receiver channels security services are utilized, information security services are mathematical cryptographic algorithms. To establish a secure communication channel, four the basic information security services are confidentiality, integrity, authentication and is the inability to deny.

Today, many users share countless information with each other over insecure communication channel. In this insecure environment, it is cryptography that guarantees that the information reaches the other party completely and accurately. Security services are used for sender-receiver channels and information security services use mathematical cryptographic algorithms. There are four basic information security services for a secure communication channel. These are confidentiality, integrity, authentication and non-repudiation. [48]

Maximum distance separable matrices (MDS) are used in the diffusion layers of lightweight block ciphers. MDS matrices derived from mds codes improve the properties of cryptographic primitives and help provide security against differential and linear cryptanalysis. In addition, involutive MDS matrices, which have a minimum XOR number and whose inverse is equal to itself, allow the use of the same matrix in encryption and decryption, which is both less costly and less space consuming.

The main motivation for the use of MDS codes in cryptography is that these structures provide excellent propagation. In fact, as introduced by S. Vaudenayin, MDS matrices are isomorphic to multiple permutations over a Z-alphabet, which initially provides excellent propagation.

MDS matrices are generated from MDS codes. They have the maximum number of differential and linear branches, which helps to design block ciphers that are resistant to differential and linear cryptanalysis.[45]

MDS matrices have gained great importance since the use of MDS matrices in the diffusion layer is known to increase the encryption strength and make ciphers more resistant to linear and cryptanalysis attacks. For this reason, MDS matrix generation has become a field of great interest.[49]

Methods for constructing MDS matrices can be divided into two groups. The first one is direct generation methods and the second one is search-based methods. The first group is based on Cauchy matrix, Vandermonde matrix, complement matrices, abbreviated BCH codes and skew recursive structures. The second group includes recursive structures, hybrid structures and special matrix forms. Special matrix forms such as circular and Hadamard matrices over finite field are used for one of the easiest construction methods that provide efficiency.[27]

When the methods of creating MDS matrices are examined, it is checked that all square sub-matrices of the matrices created with the search-based method are also MDS, which increases the search cost. In addition, since the space to search for the elements of the created MDS matrix is very large, the applicability of this method in terms of space, speed, efficiency and performance is almost impossible under some conditions (limited system resources). In the direct generation method, on the other hand, since special matrix forms and codes are used to generate the matrix, the space to search for MDS matrices is minimized and thus no search cost is required. MDS matrices created using special matrix forms as Hadamard, Circulant, Toeplitz, Circulant-like require search costs because MDS matrices cannot be created directly with these structures.

One of the most important and most costly components in a lightweight cryptography is the diffusion layer. Therefore, the design of the diffusion layers to be formed with a minimum number of hardware elements, especially with low exclusive OR (XOR) count, is one of the open problems in the literature.

Generalized-Hadamard (GHadamard-Generalized Hadamard) matrix form is a hybrid method. It uses Hadamard matrices, one of the special matrix forms, in its substructure and generates new MDS matrices directly in Generalized Hadamard form without having to search. The main reason for using Hadamard matrices is that the Hadamard form plays an important role in the generation of involutive MDS matrices. The Hadamard matrix definition is generalized and improved by the generalized Hadamard matrix form [48].

In this paper, we study the generation of MDS matrices used in lightweight block ciphers. We give information about the involutive MDS matrix, XOR number, Generalized Hadamard (GHadamard) and Cauchy-based Hadamard (Hadamard-Cauchy) matrix forms and then proceed to applications. Using the irreducible polynomial $x^4 + x + 1$ in the finite field F_{2^4}, a 4x4 involutive MDS matrix was constructed with the Generalized Hadamard matrix form. Using the irreducible polynomials $x^6 + x + 1$ and $x^6 + x^3 + 1$ on the finite field F_{2^6}, 4x4 involutive MDS matrices are obtained with the Generalized Hadamard matrix form and the Cauchy-based Hadamard matrix form. In the finite field F_{2^7}, 4x4 involutive MDS matrices were constructed using the Generalized Hadamard matrix form and Cauchy-based Hadamard matrix form with the irreducible polynomials $x^7 + x + 1$ and $x^7 + x^3 + 1$. Then we computed the XOR numbers of these matrices. Thus, 4x4 involutive MDS

matrices were obtained on the finite fields F_{2^4}, F_{2^6} and F_{2^7} by using some special matrix forms. We also calculated the XOR numbers of the matrices we obtained. In some of our applications, we obtained new 4x4 involutive MDS matrices with the help of isomorphism from the matrices we created. By calculating the XOR numbers of these newly created matrices, we had the chance to compare the XOR numbers of two matrices.

1. GİRİŞ

1.1. Literatür Taraması ve Tezin Amacı

Günümüzde teknoloji hızla gelişmektedir. Teknoloji geliştikçe kullanımı da yaygınlaşmıştır. Güvenli bir iletişimin sağlanmasında ise kriptoloji önemli bir rolü üstlenmiştir. Yunanca gizli bilgi anlamına gelen kriptoloji, verilerin hem güvenli hem de gizli biçimde iletimini ve saklanmasını inceler [1]. Kriptolojide MDS matrisleri taşıdıkları özelliklerden dolayı vazgeçilmez bir matris türüdür. Oluşturulan MDS matrisin involutif olması bize birçok avantaj sağlar. Öyle ki hem şifrelemede hem de şifre çözmede aynı matris kullanılır. Böylece şifreleme ve şifre çözmede aynı uygulama maliyeti sağlanırken alan olarak daha az yer kaplamış olur. Bu çalışmada $F_{2^4}, F_{2^6}, F_{2^7}$ sonlu cisimleri üzerinde $4x4$ MDS matrisleri oluşturmayı ve bu matrislerin XOR sayılarını hesaplayarak karşılaştırma yapmayı amaçlanmıştır. Özel matris formları ile elde ettiğimiz bir matrise izomorfizma [2] uygulanarak başka bir matris oluşturuldu ve bu iki matrisin de XOR sayıları hesaplanarak karşılaştırma yapıldı. Ayrıca oluşturulan matrislerin involutif olması amaçlandı. Böylece bu üç cisim üzerinde uygulamalar yapılarak çeşitli örnekler elde edildi.

1.2. Tezin İçeriği

Bu çalışma dört bölümden oluşmaktadır. İlk kısımda matematiksel alt yapı ve kriptolojinin temel kavramlarına yer verilmiştir.

İkinci kısımda tezin uygulama çalışmasının yapıldığı involutif MDS matrisleri ile ilgili tanımlar ve teoremler verilmiştir.Bu bölümde tezde kullanılan bazı MDS matris formları tanımlanmıştır.Ayrıca bu matrislerin kapladıkları alanları belirlemede yararlanılan XOR sayısı hesaplama için gereken tanım verilmiştir.

Üçüncü bölümde ise $F_{2^4}, F_{2^6}, F_{2^7}$ sonlu cisimleri üzerinde Genelleştirilmiş Hadamard ve Cauchy tabanlı Hadamard matris formları kullanılarak $4x4$ involutif MDS matrsleri elde edilmiştir.Bölümün devamında gereken XOR sayıları hesaplanarak kapladıkları

alan bulunmuştur.Bazı uygulamalarda elde edilen $4x4$ involutif MDS matristen izormorfima yardımı ile yeni bir $4x4$ involutif MDS matris elde edilmiştir.

Dördüncü bölümde Sonuçlar ve Değerlendirme verilerek tez çalışması sonlandırılmıştır.

1.3. Temel Kavramlar

1.3.1. Matematiksel altyapı

Tanım 1.3.1.1 f, A kümesinden B kümesine fonksiyon olmak üzere $\forall x, y \in A$ için $f(x_1) = f(y_2) \Rightarrow x_1 = y_2$ ya da $x_1 \neq y_2 \Rightarrow f(x_1) \neq f(y_2)$ koşulları sağlanıyorsa f bire bir fonksiyondur.

f C dan D ye bir fonksiyon olsun. Eğer $\forall y_1 \in B$ elemanı için $f(x_1) = y_1$ sağlanacak şekilde en az bir $x_1 \in A$ elemanı bulunabiliyorsa f fonksiyonu örten fonksiyon olur [3].

Tanım 1.3.1.2 $A = \{1,2, \dots, n\}$, n elemanlı sonlu bir küme olsun. A dan A ya olan fonksiyon hem bire bir hem örten fonksiyon oluyorsa bu fonsiyona permütasyon adı verilir [3].

Tanım 1.3.1.3 a_1, b_1 herhangi bir tamsayı ve m_1 pozitif bir tam sayı olmak üzere eğer m_1, $b_1 - a_1$ sayısını bölüyorsa $a_1 \equiv b_1 \, mod m_1$ olarak ifade edilebilir. Burada $a_1, b_1{}' \, e \, (mod m_1)$'e göre denktir denir ve m_1 pozitif tam sayı ise modulo olarak adlandırılır [4].

Tanım 1.3.1.4 A sonlu bir küme olsun. A üzerinde tanımlanan $*$: $AxA \rightarrow A$ ikili işlemi bir fonksiyondur. Eğer $(a_1, a_2) \in AxA$ ise, A kümesinin tek bir elemanı (a_1, a_2) elemanının karşılığıdır ve $a_1 * a_1$ ile ifade edilir [5].

Tanım 1.3.1.5 $G \neq \emptyset$ ve $*$, G'de bir ikili işlem olsun. G kümesi $*$ işlem altında kapalı bir kümeyi belirtsin. Eğer;

$G1$: $*$ işlemi G de birleşme özelliğine sahip ise,

$G2$: $*$ işleminin G de birim elemana sahip ise,

$G3$: $*$ işlemine göre G deki her elemanın bir tersi mevcut ise

O zaman $(G,*)$ ikilisine bir grup adı verilir.

$(G,*)$ grubu $a * b = b * a$ değişme özelliğini sağlıyorsa G'ye değişmeli veya abelyen grup denir [6].

Tanım 1.3.1.6 $R \neq \emptyset$ olmak üzere bu kümede tanımlı iki ikili işlem $\oplus, \odot$ olsun. Aşağıdaki $H1, H2, H3$ aksiyomlarını sağlayan $(R, \oplus, \odot)$ cebirsel yapısına bir halka denir.

$H1$: $(R, \oplus)$ değişmeli bir gruptur. Yani $\forall \alpha, \beta \in R$ için $\alpha \oplus \beta = \beta \oplus \alpha$ dır.

$H2$: $\odot$ işlemi R de birleşme özelliğine sahiptir. Yani $\forall \varepsilon, \mu, \sigma \in R$ için $(\varepsilon \odot \mu) \odot \sigma = \varepsilon \odot (\mu \odot \sigma)$ dir.

$H3$:$\odot$Işleminin $\oplus$ işlemine hem sağdan hem soldan dağılma özelliği mevcuttur. Yani $\varepsilon \odot (\mu \oplus \sigma) = \varepsilon \odot \mu \oplus \varepsilon \odot \sigma \; ve \; (\varepsilon \oplus \mu) \odot \sigma = \varepsilon \odot \sigma \oplus \mu \odot \sigma$ dir.

Halkanın $\oplus$ işlemine göre etkisiz elemanı 0_R olur ve sıfır elemanı olarak adlandırılır. Eğer ikinci işleme göre de etkisiz eleman varsa bu eleman halkanın birim elemanı olur ve 1_R ile ifade edilir [6].

Tanım 1.3.1.7 $R_1 \; ve \; R_2$ iki halka ve $f: R_1 \to R_2$ bir fonksiyon olsun. Eğer aşağıdaki özellikleri sağlıyorsa $f \; ye \; R_1 \; den \; R_2 \; ye$ bir halka homomorfizması denir.

1) $\forall \theta_1, \alpha_1 \in R_1$ için $f(\theta_1 + \alpha_1) = f(\theta_1) + f(\alpha_1)$

2) $\forall \theta_1, \alpha_1 \in R_1$ için $f(\theta_1 \alpha_1) = f(\theta_1) f(\alpha_1)$ [6].

Tanım 1.3.1.8 R_1, R_2 iki halka olmak üzere $f: R_1 \to R_2$ homomorfizması bire bir ve örten ise f 'ye izomorfizma adı verilir ve $R_1 \cong R_2$ şeklinde gösterilir.

Tanım 1.3.1.9 Değişmeli ve birimli bir R halkası için $R - \{0_R\} = R^*$, ikinci işleme göre bir grup oluyorsa R halkasına cisim adı verilir [6].

Cisim sonlu sayıda elemana sahip ise sonlu cisim adı verilir.

Tanım 1.3.1.10 x bir bilinmeyen, R bir halka ve $a_0, a_1, \ldots, a_k$ lar R nin elemanı olmak üzere $a_0 + a_1 x + \cdots + a_k x^k$ yapısına katsıyıları R halkasından olan bir polinom adı verilir. Katsayıları R halkasından olan tüm polinomların kümesi $R[x]$ şeklinde ifade edilmektedir [6].

Tanım 1.3.1.11 $\theta \in R$ olsun. Eğer $x = \theta$ için $a_0 + a_1 \theta + \cdots + a_k \theta^k = 0$ oluyorsa θ' ya polinomun kökü denir. Polinom katsayıları aralarında asal ise bu polinoma monik polinom adı verilir.

Tanım 1.3.1.12 α elemanı $modp$'ye göre derecesi $(p-1)$ oluyorsa bu α elemanına ilkel (asal veya primitive) eleman adı verilir [4].

Tanım 1.3.1.13 F_1 bir cisim ve $F_1[x]$ bir polinom kümesi olarak verilsin. Pozitif dereceli $a \in F_1[x]$ polinomu ve $\beta, \gamma \in F_1[x]$ polinomları için $a = \beta . \gamma$ ise bu durumda β veya γ dan biri sabit polinom oluyorsa o zaman $a \in F_1[x]$ polinomuna F_1 üzerinde indirgenemez polinom denir [7].

1.4. Lineer Cebirsel Yapılar

Tanım 1.4.1 Bir K cismi verildiğinde, (veya bir K-vektör uzayı) V, değişmeli bir gruptur ve $KxV \to V$ aşağıdaki aksiyomları sağlayan bir işlemdir (skaler çarpma olarak da adlandırlır). $\forall \theta, \beta \in K \; ve \; \mu, \varepsilon \in V$ için

1) $\theta.(\beta.\mu) = (\theta.\beta).\mu$

2) $(\theta + \beta).\mu = \theta.\mu + \beta.\mu$

3) $1_K.\mu = \mu$

4) $\theta.(\mu + \varepsilon) = \theta.\mu + \theta.\varepsilon$

Burada $1_K, K$ 'nın çarpımsal birim elemanıdır [3].

Tanım 1.4.2 V bir vektör uzayı ve $V_1 \subset V$ olsun. Aşağıdaki iki şart sağlanıyorsa V_1 'e V uzayının alt vektör uzayı denir.

1) V_1, toplamaya göre V ' nin bir alt grubudur.

2) V_1, skaler çarpım altında kapalıdır [3].

Tanım 1.4.3 Vektörlerin lineer bağımsızlığı ile ilgili aşağıdaki tanımlar verilebilir.

- Eğer $x = \lambda_1 x_1 + \cdots + \lambda_n x_n$ olacak şekilde $\lambda_i \in K$ skalerleri bulunabiliyorsa x elemanı $x_1, x_2, \dots, x_n$ lineer kombinasyonu olur.
- $\lambda_1 x_1 + \cdots + \lambda_n x_n = 0$ iken $\lambda_1 = \cdots = \lambda_n = 0$ oluyorsa $x_1, \dots, x_n$ elemanları lineer bağımsızdır. Eğer $x_1, \dots, x_n$ lineer bağımsız değil ise lineer bağımlıdır denir.

V 'nin her elemanı A' nın sonlu sayıda elemanının lineer kombinasyonu olarak yazılabiliyorsa V vektör uzayının A alt kümesi V 'yi gerendir denir [3].

Tanım 1.4.4 P vektör uzayı ve $H = \{h_1, h_2, \dots, h_n\}$ olsun. Eğer H kümesi lineer bağımsız ve P 'yi geren bir küme oluyorsa H kümesi P uzayının tabanı veya bazı olarak adlandırılır [8].

Tanım 1.4.5 K cismi üzerinde $W_1 \; ve \; W_2$ vektör uzayları olsun. L , W_1 uzayından W_2 uzayına bir fonksiyon olmak üzere L fonksiyonu aşağıdaki özellikleri gerçekleştiriyorsa L'ye lineer dönüşüm denir.

I. $\forall \mu, \varepsilon \in V_1$ için $L(\mu + \varepsilon) = L(\mu) + L(\varepsilon)$

II. $\forall k \in K \; ve \; \forall \mu \in V_1$ için $L(k.\mu) = k.L(\mu)$ [9].

Tanım 1.4.6 F bir cisim ,$1 \leq i \leq m$, $1 \leq j \leq n$ ve $(A_{ij}) \in F$ olmak üzere aşağıda verilen tablo şeklinde ifadeye matris denir.

$$\begin{bmatrix} A_{11} & \cdots & A_{1n} \\ \vdots & \ddots & \vdots \\ A_{m1} & \cdots & A_{mn} \end{bmatrix}_{mxn}$$

Burada $i = 1,2, \dots, m$ ve $j = 1,2, \dots, n$ için $\beta_i = [A_{i1}, A_{i2}, \dots, A_{in}]$ ifadesine matrisin satırı ve $c_j = \begin{bmatrix} A_{1j} \\ \vdots \\ A_{mj} \end{bmatrix}$ ifadesine de matrisin sütunu denir. Dolayısıyla m satır sayısını ve n ise sütun sayısını vermektedir. Ayrıca m satırlı ve n sütunlu matrisi mxn matris olarak ifade edilir. Matrisin satır ve sütun sayısı birbirine eşit olduğunda matrise kare matris denir [10].

Tanım 1.4.7 $M = (m_{ij}) \in M_{m,n}(F)$ (burada $M_{m,n}(F)$, F cismine ait tüm matrislerin kümesi) olsun. M matrisinin satırlarının ve sütunlarının yer değiştirmesiyle oluşturulan yeni matris M matrisinin transpozu olarak adlandırılır ve M^T şeklinde gösterilir [11].

Tanım 1.4.8 M matrisinin sütun sayısının boyutuna M 'nin sütun rankı , satır sayısının boyutuna ise M 'nin satır rankı denir. M matrisinin rankı, satır ve sütun rankı olarak adlandırılır ve $r(M)$ ile ifade edilir [12].

Tanım 1.4.9 Bir M matrisinin çarpmaya göre tersi varsa M'ye tersinir (regüler) matris denir. Eğer M matrisinin çarpmaya göre tersi yok ise M matrisine tekil(singüler) matris denir [9].

Tanım 1.4.10 M , mxm biçiminde bir matris olmak üzere $f_A = \det(xI - A)$ polinomuna , M'nin karakteristik polinomu adı verilir [9].

Tanım 1.4.11 Bir M matrisinin minimal polinomunun bulunması için $m(A) = 0$ şartını sağlayan en küçük dereceye sahip monik polinomu bulunmalıdır. Bulunan bu polinom $m_M(x)$ şeklinde gösterilir [13].

Teorem 1.4.1 (Cayley-Hamilton) Tüm matrisler kendi karakteristik denklemini sağlar. Yani herhangi bir A matrisinin minimal polinomu , karakteristik polinomu böler [13].

Tanım 1.4.12 Bir $B = (b_{ij})_{mxn}$ matrisinde c adet satır ve k adet sütun çıkarıldığında $(m - c)x(n - k)$ biçiminde elde edilen matris B'nin alt matrisi olarak adlandırılır [14].

Tanım1.4.13 Bir $A = \begin{bmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{m1} & \cdots & a_{mn} \end{bmatrix}_{mxn}$ matrisinde

$r_1 + r_2 + \cdots + r_x = m$, $s_1 + s_2 + \cdots + s_y = n$ olsun ve

$(\varepsilon = 1,2, \dots, x\,; \sigma = 1,2, \dots, y)$ için $A_{\varepsilon\sigma} = (a_{ij})_{r_\varepsilon x s_\sigma}$ matrisleri A ' nın alt matrislerini ifade etmek üzere $\begin{pmatrix} A_{11} & \cdots & A_{1y} \\ \vdots & \ddots & \vdots \\ A_{x1} & \cdots & A_{xy} \end{pmatrix}$ biçiminde yazılabilir. Bu ifade A matrisinin bloklara ayrılması olarak adlandırılır [14].

Tanım 1.4.14 $C = (\gamma_{ij})$ $(\gamma_{ij} \in \mathbb{C})$ olmak üzere , elemanları $j - i \equiv m(mod n)$ şeklinde ifade edilen nxn tipindeki matris dairesel matris olarak adlandırılır ve $C = circ(\gamma_0, \gamma, \dots, \gamma_{n-1})$ şeklinde gösterilir.

Daha açık ifade edilecek olursa $C = \begin{pmatrix} \gamma_0 & \gamma_1 & \gamma_2 & & \gamma_{n-1} \\ \gamma_{n-1} & \gamma_0 & \gamma_1 & \cdots & \gamma_{n-2} \\ \gamma_{n-2} & \gamma_{n-1} & \gamma_0 & & \gamma_{n-3} \\ & \vdots & & \ddots & \vdots \\ \gamma_1 & \gamma_2 & \gamma_3 & \cdots & \gamma_0 \end{pmatrix}$ biçimindedir

[15].

Tanım 1.4.15 Bir Galois halkası sıfırın eklenmiş sıfır bölenleri ile birlikte bazı p asal sayıları için bir temel ideal $(p1)$ i oluşturuyorsa bu Galois halkası birimli sonlu bir halka olarak tanımlanır.

$p1 = \underbrace{1 + 1 + \cdots + 1}_{p}$ [16].

1.5. Lineer Kod

Tanım 1.5.1 $A = \{\theta_1, \theta_2, \dots, \theta_q\}$ sonlu bir küme olmak üzere A'ya alfabe veya q-lu alfabe denir. A^n ise A kümesinden alınan n-li elemanları temsil etmek üzere A^n kümesine sözler ailesi denir. A^n kümesinin bir C alt kümesi q −lu blok kodu , C'nin elemanları ise kodsöz olarak adlandırılır. $C \subset A^n$ nin M tane elemanı olduğunda C ye n uzunluğunda M elemana sahip bir kod adı verilir ve (n, M) ile ifade edilir[17].

Tanım 1.5.2 $p\ ve\ q$ aynı uzunlukta olup, aynı alfabe üzerinde tanımlı n-liler olarak verilsin. $p\ ve\ q$'nun farklı bileşenlerinin sayısı , $p\ ve\ q$ arasındaki Hamming uzaklık olarak adlandırılır. Hamming uzaklık $d(p, q)$ ile ifade edilir [17].

Tanım 1.5.3 C kodunun minimum uzaklığı $d(C) = \underbrace{\min d(x,y)}_{x,y\in C\,,x\neq y}$ sayısıdır. n uzunluğunda, M elemanlı ve d minimum uzaklığı olan kod (n,d,M) şeklinde gösterilir [17].

Tanım 1.5.4 Bir $y=(y_1,y_2,\dots,y_n)$ vektörünün sıfırdan farklı olan elemanlarının sayısına y vektörünün Hamming ağırlığı olarak adlandırılır ve $w(y)$ ile ifade edilir. Buradan $d(\mu,,\sigma)=w(\mu-\sigma)$ olduğu söylenebilir [17].

Tanım 1.5.1.5 Eğer $C\subset V(n,p)$ alt kümesi $V(n,p)$ uzayının bir alt uzayı olduğunda C lineer kod olarak adlandırılır. C kodunun boyutu q ise C'ye $[n,q]$ kodu denir. C kodunun minimum uzaklığı d oluyorsa C'ye $[n,q,d]$-kodu denir [17].

Teorem 1.5.1 $d(C)=w(C)$ ise C bir lineer kod olarak adlandırılır [17].

Tanım 1.5.5 C kodu $[n,k]$ olsun. Satırları C 'nin bazlarından oluşan kxn tipinde bir E matrisi C'nin bir üreteç matrisi olarak isimlendirilir [17].

Teorem 1.5.2 F_q cisminde bir $[n,k,d]$-kodu verilsin. Bu kod ilk k sütunu, k boyutlu I_k birim matrisi olan $D=[I_k|A]$ standart biçimdeki üreteç matrisine sahip bir koda denk olur [17].

Tanım 1.5.6 C lineer kodunun $[n,k,d]$ parametreleri olsun. Eğer $k+d=n+1$ şartını sağlıyorsa bu koda maksimum uzaklığa ayrılabilen (MDS) kod denir [18].

Tanım 1.5.1.7 $GF(2^n)$ sonlu cisminde $M=(I_k|A)$ matrisi ile oluşturulan bir C kodu MDS oluyorsa katsayıları $GF(2^n)$ den olan r-boyutlu bir A kare matrisi de MDS olur [19].

Teorem 1.5.3 N kxn biçiminde bir matris olmak üzere $K=[I|N]$ üreteç matrisine sahip C, $[n,k,d]$ kodu MDS dir ancak ve ancak N matrisinin her kare alt matrisi regülerdir [20].

Tanım 1.5.7 F , q elemanlı sonlu bir cisim ; $\exists a,n$ pozitif tamsayıları için $y\in F_q^{an}$ olsun. Burada y vektörü $k=1,\dots,m$ için $y_k=(y_{k,1},\dots,y_{k,a})$ olmak üzere $y=(y_1,\dots,y_m)$ olacak şekilde m tane parçaya ayrılabilir. Burada $\forall y_k$ değeri y vektörünün bir yığını(bundle) denir [21].

Tanım 1.5.8 F, q elemanlı sonlu bir cisim olmak üzere $y \in F_q^{bn}$ vektörünün yığın(bundle) ağırlığı sıfırdan farklı yığınlarının sayısı olarak adlandırılır ve $w_b(y)$ ile ifade edilir [21].

Örnek 1.5.1 $b = 3\ ve\ n = 4$ olmak üzere $y = (101000100111)$ vektörünü ele alalım. Bu vektör $y = (101{,}000{,}100{,}111)$ olacak şekilde 4 parçaya ayrılabilir. Burada uzunluğu 3 olan her parça y vektörünün bir yığınıdır ve yığın ağırlığı

$w_b(y) = 3$ tür.

Tanım 1.5.9 F_2_lineer dönüşümlere difüzyon tabakaları (difüzyon matris) denir [21].

Tanım 1.5.10 $(F_2^m)^n$ üzerinde bir nxn matrisinin maksimum dal sayısı $n + 1$ dir.O halde $K \in M_{bnxbn}(F_2)$ matrisi $\exists b, n$ pozitif tamsayıları için difüzyon matrisi olsun. Eğer $B_d(K) = n + 1$ olursa K matrisi MDS difüzyon matrisi olarak adlandırılır [21].

1.6. Kriptoloji

Kriptoloji; kriptografi veya şifreleme eski yunancada kryptos(gizli,saklı) ve grophein(yazma) kelimelerinden gelmiştir. Burada amaç bir verinin içerdiği bilginin istenmeyen kişilerce anlaşılmasının önüne geçmek olmuştur. Bunun için çeşitli yöntemler geliştirilmiştir.

Kriptoloji çok eski çağlardan beri insanların kullanımındadır. İlk olarak M.Ö.1900 yıllarında bir Mısırlı kâtipin yazdığı kitabelerde görülmüştür.M.Ö. 60-50 de Julius Ceasor alfabedeki harflerin yerlerini değiştirerek bir şifreleme yöntemi oluşturmuştur. 1623'te Sir Francis Bacon, 5 bitlik ikili kodlamayı kullanarak karakter türlerini değiştirme tabanlı bir kısayol sistemi üretmiştir. 1854 yılında ise Charles Wheatstone Playfair şifresini geliştirdi. 1790 yılında Thomas Jefferson şerit şifreleme makinesini icat etmiştir. Bu makine İkinci Dünya Savaşı'nda kullanıldı. 1917'de Joseph Mauborgne ve Gilbert Burnom "one-time pad"i oluşturmuşlardır.

William Frederick Friedman, İkinci Dünya Savaşı sırasında Japonların Purple Machine şifreleme sistemini kırmıştır. Ayrıca II. Dünya Savaşı sırasında Almanlar, Arthur Schelbius tarafından icat edilen Enigma makinesini kullanmışlardır. 1991 yılında Phil Zimmerman PGP sistemini geliştirdi. 2001 yılında Belçikalı Joan Daerman ve Vincent Rijmen tarafından geliştirilen Rijndael algoritması, AES (Gelişmiş Şifreleme Standardı) adı altında standartlaştırıldı [22].

1.6.1. Kriptografi

Bir veriye ait bilginin herkes tarafından anlaşılmasını engellemek amacıyla ortaya çıkan gizli yazma bilimidir. Ayrıca bilgilerin güvenliği için oluşturulan matematiksel yöntemlerdir. Burada amaç bilginin iletim esnasında karşılaşabileceği saldırılarda hem göndereni hem de alıcıyı korumaktır.

1.6.2. Kriptanaliz

Kriptolojinin önemli bir unsuru olan kriptanaliz kriptosistemlerin güvenliğinde etkin rol oynar. Blok şifrelerin bir çoğu kriptografik şemada geliştirilen en önemli yapı taşlarından biridir. Modern blok şifreler sıklıkla çeşitli döngüleri tekrarlar ve her döngü bir karıştırma tabakası ve bir yığılma tabakasından oluşur. Matematiksel olarak şöyle ifade edilebilir; yığılma tabakası doğrusal bir fonksiyon tarafından üretilirken, karıştırma tabakası genellikle doğrusal olmayan bir (S-kutusu) fonksiyon tarafından üretilir.

2. MDS MATRİSLER VE İNVOLUTİF(TERSİ KENDİSİ) MDS MATRİSLER

MDS(Maksimum uzaklığa ayrılabilen) kodlardan türetilen maksimum mesafeye ayrılabilir (MDS) matrisler , Gelişmiş Şifreleme Standardı (AES) [23] gibi blok şifrelerin çoğunda , Whirpool [24] , Photon ailesi [25] ve Whirlwind [26] gibi özet (hash) fonksiyonlarında kullanılır. MDS matrisler ayrıca diferansiyel ve lineer kriptanalizin güvenliğini ispatlar. Bu nedenle iyi uygulama özelliklerine sahip MDS matrisleri bulmak önemlidir [27].

Tersi kendisi olan (involutif) MDS matrisleri sayesinde şifrelemede ve şifre çözmede aynı matrisin kullanılmasıyla daha düşük maaliyetler elde edilir. Ayrıca involutif MDS matrisleri ile şifrelemede daha az yer kaplanır [28].

MDS matrisleri oluşturma yöntemleri ikiye ayrılabilir. Bunlar doğrudan oluşturma yöntemleri ve arama tabanlı yöntemlerdir. İlk grup Cauchy matrislerine [29], tamamlayıcı matrislere [25,30], Vandermonda matrislerlerine [31,32], kısaltılmış BCH kodlarına [33,34] ve çarpık özyinelemeli yapılara [35] dayanan yöntemleri içerir. İkinci grup ise bazı ilginç fikirlerden oluşur. Bunlar özyinelemeli yapılar [36,37] , hibrit yapılar [38] ve özel matris formları [30,39,40] kullanılarak yapılmaktadır. Doğrudan oluşturma yöntemleri ile aramaya dayalı yöntemleri birleştiren hibrit yöntemler (Genelleştirilmiş Hadamard Matrisler) vardır.Verimlilik sağlayan en kolay inşa yöntemlerinden biri için dairesel ve sonlu cisimde Hadamard matrisleri gibi matris formları kullanılır [27]. MDS matrislerinin bazı önemli özellikleri şu şekilde verilebilir:

1) A kare matrisi MDS dir ancak ve ancak A nın her alt kare matrisi regülerdir (tersinirdir).

2) Bir MDS matrisin özelliği satırların\sütunların permütasyonlarında korunur. Benzer şekilde bir satırın\sütunun sıfır olmayan bir c$\in F_{2^m}$ ile çarpılması , onun MDS olma özelliğini etkilemez. Genel olarak A ,kx(n-k) matrisi olmak üzere üreteç matrisi G=[I|A] olan bir [n,k,d] C kodunun minimum mesafesi d , yukarıdaki işlemler A ya uygulandıktan sonra korunur.

3) Bir MDS matrisin özelliği transpoze işleme altında korunur [41].

Tanım 2.2 K bir matris olmak üzere $K.K = I$ olan matrislere ya da tersi kendisine eşit olan matrislere involutif matris denir.

MDS matrisler oluşturulurken düşük XOR sayısına sahip olmasına dikkat edilir. Yukarıda saydığımız MDS matrisleri oluşturma yöntemleriyle birlikte MDS matris oluşturmak için farklı çalışmalar da bulunmaktadır. Sakallı, Akleylek, Akkanat ve Rijmen [27] çalışmalarında izomorfizma ve otomorfizmayı kullanmıştır; aynı ikili uzantı cisminde MDS matrislerinin otomorfizmasını açık bir şekilde tanımlamış ve bu fikri genişleterek F_{2^m} üzerinde MDS matrisleri ve $F_{2^{mt}}$ üzerinde MDS matrisleri arasında $(t \geq 1\,, m > 1\,)$ izomorfizmalar sunmuşlardır. Burada yapılan iş elimizdeki bir MDS matristen izomorfizma sayesinde yeni bir MDS matris üretmektir.

Büyüksaraçoğlu Sakallı, Aydın, Tuncay, Pehlivanoğlu, Güzel, ve Sakallı [42] çalışmalarında önce Hadamard ,Dairesel ve Toeplitz matris formlarını (H,C,T) arayarak ve bunları kullanarak $4x4$ involutif / involutif olmayan MDS matrislerini elde etmişlerdir. Ardından bu yeni formları (GH,CP,TP) kullanarak doğrudan yeni MDS matrisler üretmişlerdir. Ayrıca MDS matrislerini optimize etmek ve literatürde verilenlerle karşılaştırmak için Boyar-Peralta algoritmasını kullanarak XOR sayılarını değerlendirmişlerdir.

Yapılan bir başka çalışma ise Sim, Khoo, Oggier ve Peyrin [44] yaptığı çalışmadır. Bu çalışmada Hadamard ve Cauchy matrislerinin özelliklerini birleştirerek $2^s x 2^s$ lik bir matris yapısı önerilmiştir [44]. Bu matris bir Cauchy matrisi olduğu için MDS matrisidir. Hadamard matrisi ilk satırdaki elemanların kareleri toplamı 1'e eşit olduğunda involutif olacağından bir Hadamard-Cauchy matrisi oluşturmuşlardır. Böylece ilk satırın karelerinin toplamının 1'e eşit olup olmadığı kontrol edilerek bir MDS ve involutif matrisi elde etmişlerdir. Daha sonra oluşturulan matrisin hangi denklik sınıfına ait olduğunu belirlenmiştir. Bu çalışma aslında bir MDS matrisi ararken arama alanını büyük ölçüde azaltmayı planlamıştır. Bir denklik sınıfındaki bir Hadamard matrisi MDS değilse aynı denklik sınıfındaki matrisler de MDS olmayacaktır. Bu nedenle her şey Hadamard matrislerin kaç tane ve hangi permütasyonun aynı denklik sınıflarına ait olduğunu analiz etmeye indirgemiştir.

Teorem 2.1 $u\,, F_{2^{r_1+r_2+\cdots+r_s}}$ üzerinde sıfırdan farklı $kx1$ matrisi , u_i $F_{2^{r_i}}$ de bir $kx1$ matrisi olsun . $1 \leq i \leq s$ için $u = u_1||u_2|| \ldots ||u_s$ olarak alınsın. Ayrıca M_i $F_{2^{r_i}}$ de bir kxk MDS matrisi olsun o zaman

$1 \leq i \leq s$ olmak üzere $M_1u_1, M_2u_2, \dots, M_su_s$ $kx1$ matrislerinden

$v \coloneqq M_1u_1 \,||M_2u_2\,|| \dots ||M_su_s$ birleşmesi elde edilir. Böylece $u\ ve\ v$ nin sıfırdan farklı toplam girdi sayısı en az

$k + 1$ dir [28].

Teorem 2.2 Teorem 2.1 den yola çıkarak MDS fonksiyonu involutiftir ancak ve ancak her $1 \leq i \leq s$ için M_i MDS matrisi involutif olur.

Şimdi $k = 2,3,4$ için MDS matrislerini inceleyelim.

Teorem 2.3 Bazı **s**ıfırdan farklı $b, c \in F_{2^r}$ için F_{2^r} de herhangi bir $2x2$ involutif MDS matrisi aşağıdaki gibidir:

$$\begin{bmatrix} 1 + (bc)^{2^{r-1}} & b \\ c & 1 + (bc)^{2^{r-1}} \end{bmatrix}$$

Teorem 2.4 F_{2^r} üzerinde herhangi bir $3x3$ MDS matris formu şu şekildedir:

$$\begin{bmatrix} \sigma_1 & (\sigma_1 + 1)\mu_0 & (\sigma_1 + 1)\mu_1 \\ (\sigma_2 + 1){\mu_0}^{-1} & \sigma_2 & (\sigma_2 + 1){\mu_0}^{-1}\mu_1 \\ (\sigma_1 + \sigma_2){\mu_1}^{-1} & (\sigma_1 + \sigma_2){\mu_1}^{-1}\mu_0 & \sigma_1 + \sigma_2 + 1 \end{bmatrix}$$

Burada $\sigma_1, \sigma_2, \mu_0, \mu_1 \in F_{2^6} - \{0\}, \sigma_1 \neq \sigma_2, \sigma_1 + \sigma_2 \neq 1, \sigma_1 \neq 1\ ve\ \sigma_2 \neq 1$ i sağlar [45].

Tanım 2.3 Aşağıda verilen $4x4$ involutif MDS matris formuna Genelleştirilmiş Hadamard denir.

$$\begin{bmatrix} \alpha_0 & \alpha_1\beta_1 & \alpha_2\beta_2 & \alpha_3\beta_3 \\ \alpha_1{\beta_1}^{-1} & \alpha_0 & \alpha_3{\beta_1}^{-1}\beta_2 & \alpha_2{\beta_1}^{-1}\beta_3 \\ \alpha_2{\beta_2}^{-1} & \alpha_3{\beta_2}^{-1}\beta_1 & \alpha_0 & \alpha_1{\beta_2}^{-1}\beta_3 \\ \alpha_3{\beta_3}^{-1} & \alpha_2{\beta_3}^{-1}\beta_1 & \alpha_1{\beta_3}^{-1}\beta_2 & \alpha_0 \end{bmatrix}$$

Burada $\alpha_0, \alpha_1, \alpha_2, \alpha_3, \beta_1, \beta_2, \beta_3 \in F_{2^r}\backslash\{0\}$ dır [28].

Tanım 2.4 Bir $4x4$ Hadamard matris formu $H = had(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)$ aşağıdaki gibidir [43]:

$$\begin{bmatrix} \varepsilon_0 & \varepsilon_1 & \varepsilon_2 & \varepsilon_3 \\ \varepsilon_1 & \varepsilon_0 & \varepsilon_3 & \varepsilon_2 \\ \varepsilon_2 & \varepsilon_3 & \varepsilon_0 & \varepsilon_1 \\ \varepsilon_3 & \varepsilon_2 & \varepsilon_1 & \varepsilon_0 \end{bmatrix}$$

Tanım 2.5 Toeplitz MDS matrisinin genel formu aşağıdaki gibi tanımlanır [46]:

$$T = \begin{bmatrix} \theta_0 & \theta_1 & \theta_2 & \cdots & \theta_{n-2} & \theta_{n-1} \\ \theta_{-1} & \theta_0 & \theta_1 & & \theta_{n-3} & \theta_{n-2} \\ & \vdots & & \ddots & \vdots & \\ \theta_{-(n-1)} & \theta_{-(n-2)} & \theta_{-(n-3)} & \cdots & \theta_{-1} & \theta_0 \end{bmatrix}$$

Bir $4x4$ Toeplitz matris formu $T = Toep\ (\mu_0, \mu_1, \mu_2, \mu_3, \mu, \mu_5, \mu_6)$ aşağıdaki gibidir [42]:

$$T = \begin{bmatrix} \mu_0 & \mu_1 & \mu_2 & \mu_3 \\ \mu_4 & \mu_0 & \mu_1 & \mu_2 \\ \mu_5 & \mu_4 & \mu_0 & \mu_1 \\ \mu_6 & \mu_5 & \mu_3 & \mu_0 \end{bmatrix}$$

Tanım 2.6 Bir $4x4$ dairesel matris formu $C = cir(\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3)$ aşağıdaki gibi verilir [42]:

$$C = \begin{bmatrix} \varepsilon_0 & \varepsilon_1 & \varepsilon_2 & \varepsilon_3 \\ \varepsilon_3 & \varepsilon_0 & \varepsilon_1 & \varepsilon_2 \\ \varepsilon_2 & \varepsilon_3 & \varepsilon_0 & \varepsilon_1 \\ \varepsilon_1 & \varepsilon_2 & \varepsilon_3 & \varepsilon_0 \end{bmatrix}$$

Tanım 2.7 Bir Cauchy matrisi C , $C[m,n] = \frac{1}{\mu_m + \varepsilon_n}$ olacak şekilde $GF(2^r)$, $\{\mu_0, \mu_1, \dots, \mu_{k-1}\}$ ve $\{\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{k-1}\}$ den gelen iki ayrık eleman kümesiyle oluşturulan bir kxk matrisidir [43].

Tanım 2.8 $\{\varphi_0, \varphi_1, \dots, \varphi_{n-1}\} \subseteq F_{2^r}$ ve $\{\tau_0, \tau_1, \dots, \tau_{n-1}\} \subseteq F_{2^r}$ verilsin öyle ki tüm $0 \le i, j \le n-1$ $için$ $\varphi_i + \tau_j \neq 0$ dır. O zaman $a_{i,j} = \frac{1}{\varphi_i + \tau_j}$ olmak üzere $A = (a_{i,j})$ Cauchy matrisi olarak adlandırılır [43].

Önerme 2.1 $G = \{x_0, x_1, \dots, x_{n-1}\}$ F_{2^r} de toplamsal alt grup olsun. $y_j = I + x_j$, burada $j = 0,1, \dots, n-1$, G nin elemanları olmak üzere, $I + G$, $I \notin G$ kosetini ele alalım. O zaman $a_{i,j} = \frac{1}{x_i + y_j}$ olmak üzere nxn $A = \left(a_{i,j}\right)$ matrisi tüm $0 \le i, j \le n-1$ için MDS matris olur [47].

Önerme 2.2 A matrisi Önerme 2.1.1.1 de belirtilen formda bir matris ise o zaman $A^2 = c^2.I$ olur, burada $c = \sum_{j=0}^{n-1} \frac{1}{I + x_j}$ dir [47].

Sonuç 2.1 Eğer A matrisi Önerme 2.1.1.1 de belirtilen formda bir nxn matrisi ise $c^{-1}A$ matrisi involutif MDS matrisi olur öyle ki c burada herhangi bir satırdaki elemanların toplamıdır [47].

Önerme 2.3 $H = \left(h_{i,j}\right)$ $2^n x 2^n$ matrisi olsun ve ilk satırı $(h_0, h_1, \dots, h_{2^n-1})$ dir. Bu durumda H Hadamard olur ancak ve ancak $h_{i,j} = h_{i\oplus j}$ dir , burada $i \oplus j$, $i \; ve \; j$ nin n-bitlik ikilisine eşittir ve sırasıyla $i \; ve \; j$ nin temsilidir [47].

Sonuç 2.2 $G = \{\varphi_0, \varphi_1, \dots, \varphi_{2^n-1}\}$ F_{2^r} nin toplamsal alt grubu olsun ve $\varphi_i + \varphi_j = \varphi_{i\oplus j}$ burada $i \oplus j$, $i \; ve \; j$ nin n-bitlik ikilisine eşittir ve sırasıyla $i \; ve \; j$ nin temsilidir. O zaman $I \in F_{2^r}/G$ için , $H' = \left(h'_{i,j}\right) = \left(\frac{1}{I+\varphi_{i\oplus j}}\right)$ Hadamard olur [47].

Önerme 2.4 $(i_{n-1}, \dots, i_1, i_0)$, i 'nin ikili temsili olmak üzere $x_i = \sum_{k=0}^{n-1} i_k x_{2^k}$ olacak şekilde n lineer bağımsız $\{x_0, x_1, \dots, x_{2^n-1}\}$ elemanlarının bir lineer gereni olan

F_{2^r} 'nin bir toplamsal altgrubu $G = \{x_0, x_1, \dots, x_{2^n-1}\}$ olsun. $l \in F_{2^r}/G$ olmak üzere $0 \le i \le 2^n - 1$ için $y_i = l + x_i$ olsun. $a_{i,j} = \frac{1}{(x_i+y_j)}$ olmak üzere $A = (a_{i,j})$ matrisi bir Hadamard MDS matristir [47].

İspat : $H = \left(h_{i,j}\right) = (x_i + x_j)$ matrisini düşünelim. O zaman $h_{i,j} = x_{i\oplus j}$ dir. Önerme 2.3 ten H Hadamard olur. Şimdi $a_{i,j} = \frac{1}{(x_i+y_j)} = \frac{1}{(I+x_i+x_j)} = \frac{1}{I+x_{i\oplus j}}$ dir.Ayrıca Sonuç 2.2 den A Hadamard olur. Tekrar Önerme 2.1 den A MDS olur.Yani A Hadamard MDS matrisidir [47].

Sonuç 2.3 $\frac{1}{c}A$ matrisi Hadamard involutif MDS matrisidir , burada c herhangi satırdaki elemanların toplamıdır [47].

Önerme 2.5 A , F_{2^m} sonlu cismi üzerinde bir kxk matrisi olsun.

$0 \le i \le m-1 \; ve \; b \in F_{2^{m^*}}$ olmak üzere A' , A nın elemanlarına $f: b \to b^{2^i}$ otomorfizması uygulanarak üretilir. O zaman A' nün determinantı sıfıra eşit olur ancak ve ancak A nın determinantı sıfıra eşittir [27].

Teorem 2.5 β , F_{2^m} de ilkel eleman , $c \in F_{2^m}{}^*$ olsun. $0 \le i \le m-1$ olmak üzere $f_{i,c}: \beta \to \left(\beta^{2^i}\right)c$ formunda $m.(2^m - 1)$ tane farklı ve bijektif fonksiyon vardır. Bu fonksiyonlar aynı ikili uzantı cismi üzerinde bir kare matrisinin MDS özelliğini korur, yani yeni MDS matrisleri mevcut olanlardan üretilitir [27].

Önerme 2.6 A $F_{2^m}/p_1(x)$ in herhangi ilkel elemanı olsun. A' A nın elemanlarına $F_{2^m}/p_2(x)$ sonlu cisminde $f_{s_u}: \beta_1 \to \beta_2{}^{s_u}$ otomorfizminin uygulamasıyla

oluşturulsun ; burada β_2 $F_{2^m}/p_2(x)$ in herhangi ilkel elemanı , $s_u = e.2^i$, $1 \leq e \leq 2^m - 2$ için $ebob(e, 2^m - 1) = 1$, $p_1(\beta_2{}^{s_u}) = 0$ ve

$0 \leq u$, $i \leq m - 1$. O zaman $detA' = 0 \Leftrightarrow detA = 0$ [27].

Teorem 2.6 $f_{s_{u,c}}: \beta_1 \rightarrow (\beta_2^{s_u})c$ formunda izomorfizmler kullanılarak elde edilen $m.(2^m - 1)$ farklı fonksiyon vardır , burada β_1 ve β_2 sırasıyla $F_{2^m}/p_1(x)$ ve F_{2^m} / $p_2(x)$ in herhangi ilkel elemanı , $c \in F_{2^m}{}^*$, $s_u = e.2^i$, $1 \leq e \leq 2^m - 2$ için $ebob(e, 2^m - 1) = 1$, $p_1(\beta_2^{s_u}) = 0$ ve $0 \leq u$, $i \leq m - 1$. Bu fonksiyonlar $F_{2^m}/p_1(x)$ üzerindeki MDS matrislerinden F_{2^m} / $p_2(x)$ üzerinde bir kare matrisin MDS özelliğini koruyan yeni MDS matrisler üretilmesinde kullanılabilir [27].

Tanım 2.9 $GF(2^r)/p(X)$ cismindeki α elemanının XOR sayısı α nın $GF(2^r)/p(X)$ üzerindeki herhangi bir β elemanı ile çarpımını uygulamak için gereken XOR sayısıdır [43].

Örneğin; $GF(2^4)/Ox13$ üzerindeki $\alpha = 3$ ün XOR sayısını hesaplayalım.

$(\varphi_3, \varphi_2, \varphi_1, \varphi_0)$ cismin herhangi bir φ elemanının gösterimi olsun. $GF(2^4)/Ox13$ için,

$(0,0,1,1).(\varphi_3, \varphi_2, \varphi_1, \varphi_0) = (\varphi_2, \varphi_1, \varphi_0 \oplus \varphi_3, \varphi_3) \oplus (\varphi_3, \varphi_2, \varphi_1, \varphi_0)$

$= (\varphi_2 \oplus \varphi_3, \varphi_1 \oplus \varphi_2, \varphi_0 \oplus \varphi_1 \oplus \varphi_3, \varphi_0 \oplus \varphi_3)$

olur ki bu da 5 XORs a karşılık gelir(Artıların sayısı kadar) [43].

3. $F_{2^7}, F_{2^6}, F_{2^4}$ SONLU CİSİMLERİ ÜZERİNDE $4x4$ İNVOLUTİF MDS MATRİS UYGULAMALARI

Bu bölümde F_{2^6} cisminde x^6+x+1 ve x^6+x^3+1 indirgenemez polinomlarına göre cismin elemanları bulunarak tablo oluşturuldu. Aynı şekilde F_{2^7} cisminde x^7+x+1 ve x^7+x^3+1 indirgenemez polimomlarına göre bu cismin elemalarını elde edildi. Tablo oluşturmada son olarak F_{2^4} cisminin x^4+x+1 indirgenemez polinomuna göre elemanları bulundu. Oluşturulan bu tablolar sayesinde F_{2^7}, F_{2^6}, F_{2^4} cisimleri üzerinde Genelleştrilmiş Hadamard ve Hadamard-Cauchy tipinde $4x4$ involutif MDS matrisler elde edildi. Bazı uygulamalarda elde edilen matristen izomorfizma yardımıyla yeni bir $4x4$ involutif MDS matris oluşturuldu. Böylece oluşturulan matrislerin XOR sayıları da hesaplayarak iki matristen hangisinin daha iyi XOR sayısına sahip olduğunu incelenmiş oldu.

Tablolarımızı aşağıdaki gibi oluşturabiliriz.

$F_{2^6} = F_2(\delta)\ ,\ \delta\ , p(x) = x^6+x+1$ in kökü olsun.

Tablo 3.1. $F_{2^6}/p(x)$ sonlu cismin elemanları

$\delta^6 = \delta + 1$	$\delta^{18} = \delta^3 + \delta^2 + \delta + 1$	$\delta^{30} = \delta^5 + \delta^4 + \delta + 1$
$\delta^7 = \delta^2 + \delta$	$\delta^{19} = \delta^4 + \delta^3 + \delta^2 + \delta$	$\delta^{31} = \delta^5 + \delta^2 + 1$
$\delta^8 = \delta^3 + \delta^2$	$\delta^{20} = \delta^5 + \delta^4 + \delta^3 + \delta^2$	$\delta^{32} = \delta^3 + 1$
$\delta^9 = \delta^4 + \delta^3$	$\delta^{21} = \delta^5 + \delta^4 + \delta^3 + \delta + 1$	$\delta^{33} = \delta^4 + \delta$
$\delta^{10} = \delta^5 + \delta^4$	$\delta^{22} = \delta^5 + \delta^4 + \delta^2 + 1$	$\delta^{34} = \delta^5 + \delta^2$
$\delta^{11} = \delta^5 + \delta + 1$	$\delta^{23} = \delta^5 + \delta^3 + 1$	$\delta^{35} = \delta^3 + \delta + 1$
$\delta^{12} = \delta^2 + 1$	$\delta^{24} = \delta^4 + 1$	$\delta^{36} = \delta^4 + \delta^2 + \delta$
$\delta^{13} = \delta^3 + \delta$	$\delta^{25} = \delta^5 + \delta$	$\delta^{37} = \delta^5 + \delta^3 + \delta^2$
$\delta^{14} = \delta^4 + \delta^2$	$\delta^{26} = \delta^2 + \delta + 1$	$\delta^{38} = \delta^4 + \delta^3 + \delta + 1$

$F_{2^7} = F_2(\mu)\ ,\ burada\ \mu\ , q(x) = x^7+x+1$ in kökü olsun.

Tablo 3.2. (Devamı) $F_{2^6}/p(x)$ sonlu cismin elemanları

$\delta^{15} = \delta^5 + \delta^3$	$\delta^{27} = \delta^3 + \delta^2 + \delta$	$\delta^{39} = \delta^5 + \delta^4 + \delta^2 + \delta$
$\delta^{16} = \delta^4 + \delta + 1$	$\delta^{28} = \delta^4 + \delta^3 + \delta^2$	$\delta^{40} = \delta^5 + \delta^3 + \delta^2 + \delta + 1$
$\delta^{17} = \delta^5 + \delta^2 + \delta$	$\delta^{29} = \delta^5 + \delta^4 + \delta^3$	$\delta^{41} = \delta^4 + \delta^3 + \delta^2 + 1$
$\delta^{42} = \delta^5 + \delta^4 + \delta^3 + \delta$	$\delta^{50} = \delta^5 + \delta^4 + \delta^2$	$\delta^{58} = \delta^5 + \delta^4 + \delta^3 + \delta^2 + \delta + 1$
$\delta^{43} = \delta^5 + \delta^4 + \delta^2 + \delta + 1$	$\delta^{51} = \delta^5 + \delta^3 + \delta + 1$	$\delta^{59} = \delta^5 + \delta^4 + \delta^3 + \delta^2 + 1$
$\delta^{44} = \delta^5 + \delta^3 + \delta^2 + 1$	$\delta^{52} = \delta^4 + \delta^2 + 1$	$\delta^{60} = \delta^5 + \delta^4 + \delta^3 + 1$
$\delta^{45} = \delta^4 + \delta^3 + 1$	$\delta^{53} = \delta^5 + \delta^3 + \delta$	$\delta^{61} = \delta^5 + \delta^4 + 1$
$\delta^{46} = \delta^5 + \delta^4 + \delta$	$\delta^{54} = \delta^4 + \delta^2 + \delta + 1$	$\delta^{62} = \delta^5 + 1$
$\delta^{47} = \delta^5 + \delta^2 + \delta + 1$	$\delta^{55} = \delta^5 + \delta^3 + \delta^2 + \delta$	$\delta^{63} = 1$
$\delta^{48} = \delta^3 + \delta^2 + 1$	$\delta^{56} = \delta^4 + \delta^3 + \delta^2 + \delta + 1$	
$\delta^{49} = \delta^4 + \delta^3 + \delta$	$\delta^{57} = \delta^5 + \delta^4 + \delta^3 + \delta^2 + \delta$	

$F_{2^7} = F_2(\mu)$, $burada\ \mu$, $q(x) = x^7 + x + 1$ in kökü olsun.

Tablo 3.3. $F_{2^7}/q(x)$ sonlu cisminin elemanları

$\mu^7 = \mu + 1$	$\mu^{21} = \mu^3 + \mu^2 + \mu + 1$	$\mu^{35} = \mu^5 + \mu^4 + \mu + 1$
$\mu^8 = \mu^2 + \mu$	$\mu^{22} = \mu^4 + \mu^3 + \mu^2 + \mu$	$\mu^{36} = \mu^6 + \mu^5 + \mu^2 + \mu$
$\mu^9 = \mu^3 + \mu^2$	$\mu^{23} = \mu^5 + \mu^4 + \mu^3 + \mu^2$	$\mu^{37} = \mu^6 + \mu^3 + \mu^2 + \mu + 1$
$\mu^{10} = \mu^4 + \alpha^3$	$\mu^{24} = \mu^6 + \mu^5 + \mu^4 + \mu^3$	$\mu^{38} = \mu^4 + \mu^3 + \mu^2 + 1$
$\mu^{11} = \mu^5 + \mu^4$	$\mu^{25} = \mu^6 + \mu^5 + \mu^4 + \mu + 1$	$\mu^{39} = \mu^5 + \mu^4 + \mu^3 + \mu$
$\mu^{12} = \mu^6 + \mu^5$	$\mu^{26} = \mu^6 + \mu^5 + \mu^2 + 1$	$\mu^{40} = \mu^6 + \mu^5 + \mu^4 + \mu^2$

Tablo 3.4. (Devamı) $F_{2^7}/q(x)$ sonlu cisminin elemanları

$\mu^{13} = \mu^6 + \mu + 1$	$\mu^{27} = \mu^6 + \mu^3 + 1$	$\mu^{41} = \mu^6 + \mu^5 + \mu^3 + \mu + 1$
$\mu^{14} = \mu^2 + 1$	$\mu^{28} = \mu^4 + 1$	$\mu^{42} = \mu^6 + \mu^4 + \mu^2 + 1$
$\mu^{15} = \mu^3 + \mu$	$\mu^{29} = \mu^5 + \mu$	$\mu^{43} = \mu^5 + \mu^3 + 1$
$\mu^{16} = \mu^4 + \mu^2$	$\mu^{30} = \mu^6 + \mu^2$	$\mu^{44} = \mu^6 + \mu^4 + \mu$
$\mu^{17} = \mu^5 + \mu^3$	$\mu^{31} = \mu^3 + \mu + 1$	$\mu^{45} = \mu^5 + \mu^2 + \mu + 1$
$\mu^{18} = \mu^6 + \mu^4$	$\mu^{32} = \mu^4 + \mu^2 + \mu$	$\mu^{46} = \mu^6 + \mu^3 + \mu^2 + \mu$
$\mu^{19} = \mu^5 + \mu + 1$	$\mu^{33} = \mu^5 + \mu^3 + \mu^2$	$\mu^{47} = \mu^4 + \mu^3 + \mu^2 + \mu + 1$
$\mu^{20} = \mu^6 + \mu^2 + \mu$	$\mu^{34} = \mu^6 + \mu^4 + \mu^3$	$\mu^{48} = \mu^5 + \mu^4 + \mu^3 + \mu^2 + \mu$
$\mu^{49} = \mu^6 + \mu^5 + \mu^4 + \mu^3 + \mu^2$	$\mu^{64} = \mu^4 + \mu$	$\mu^{79} = \mu^5 + \mu^4 + \mu^2 + \mu + 1$
$\mu^{50} = \mu^6 + \mu^5 + \mu^4 + \mu^3 + \mu + 1$	$\mu^{65} = \mu^5 + \mu^2$	$\mu^{80} = \mu^6 + \mu^5 + \mu^3 + \mu^2 + \mu$
$\mu^{51} = \mu^6 + \mu^5 + \mu^4 + \mu^2 + 1$	$\mu^{66} = \mu^6 + \mu^3$	$\mu^{81} = \mu^6 + \mu^4 + \mu^3 + \mu^2 + \mu + 1$
$\mu^{52} = \mu^6 + \mu^5 + \mu^3 + 1$	$\mu^{67} = \mu^4 + \mu + 1$	$\mu^{82} = \mu^5 + \mu^4 + \mu^3 + \mu^2 + 1$
$\mu^{53} = \mu^6 + \mu + 1$	$\mu^{68} = \mu^5 + \mu^2 + \mu$	$\mu^{83} = \mu^6 + \mu^5 + \mu^4 + \mu^3 + \mu$
$\mu^{54} = \mu^5 + 1$	$\mu^{69} = \mu^6 + \mu^3 + \mu^2$	$\mu^{84} = \mu^6 + \mu^5 + \mu^4 + \mu^2 + 1$
$\mu^{55} = \mu^6 + \mu$	$\mu^{70} = \mu^4 + \mu^3 + \mu + 1$	$\mu^{85} = \mu^6 + \mu^5 + \mu^3 + \mu^2 + 1$
$\mu^{56} = \mu^2 + \mu + 1$	$\mu^{71} = \mu^5 + \mu^4 + \mu^2 + \mu$	$\mu^{86} = \mu^6 + \mu^4 + \mu^3 + 1$
$\mu^{57} = \mu^3 + \mu^2 + \mu$	$\mu^{72} = \mu^6 + \mu^5 + \mu^3 + \mu^2$	$\mu^{87} = \mu^5 + \mu^4 + 1$
$\mu^{58} = \mu^4 + \mu^3 + \mu^2$	$\mu^{73} = \mu^6 + \mu^4 + \mu^3 + \mu + 1$	$\mu^{88} = \mu^6 + \mu^5 + \mu$
$\mu^{59} = \mu^5 + \mu^4 + \mu^3$	$\mu^{74} = \mu^5 + \mu^4 + \mu^2 + 1$	$\mu^{89} = \mu^6 + \mu^2 + \mu + 1$

Tablo 3.5. (Devamı) $F_{2^7}/q(x)$ sonlu cisminin elemanları

$\mu^{60} = \mu^6 + \mu^5 + \mu^4$	$\mu^{75} = \mu^6 + \mu^5 + \mu^3 + \mu$	$\mu^{90} = \mu^3 + \mu^2 + 1$
$\mu^{61} = \mu^6 + \mu^5 + \mu + 1$	$\mu^{76} = \mu^6 + \mu^4 + \mu^2 + \mu + 1$	$\mu^{91} = \mu^4 + \mu^3 + \mu$
$\mu^{62} = \mu^6 + \mu^2 + 1$	$\mu^{77} = \mu^5 + \mu^3 + \mu^2 + 1$	$\mu^{92} = \mu^5 + \mu^4 + \mu^2$
$\mu^{63} = \mu^3 + 1$	$\mu^{78} = \mu^6 + \mu^4 + \mu^3 + \mu$	$\mu^{93} = \mu^6 + \mu^5 + \mu^3$
$\mu^{94} = \mu^6 + \mu^4 + \mu + 1$	$\mu^{106} = \mu^6 + \mu^5 + \mu^2 + \mu + 1$	$\mu^{118} = \mu^6 + \mu^4 + \mu^3 + \mu^2 + \mu$
$\mu^{95} = \mu^5 + \mu^2 + 1$	$\mu^{107} = \mu^6 + \mu^3 + \mu^2 + 1$	$\mu^{119} = \mu^5 + \mu^4 + \mu^3 + \mu^2 + \mu + 1$
$\mu^{96} = \mu^6 + \mu^3 + \mu$	$\mu^{108} = \mu^4 + \mu^3 + 1$	$\mu^{120} = \mu^6 + \mu^5 + \mu^4 + \mu^3 + \mu^2 + \mu$
$\mu^{97} = \mu^4 + \mu^2 + \mu + 1$	$\mu^{109} = \mu^5 + \mu^4 + \mu$	$\mu^{121} = \mu^6 + \mu^5 + \mu^4 + \mu^3 + \mu^2 + \mu + 1$
$\mu^{98} = \mu^5 + \mu^3 + \mu^2 + \mu$	$\mu^{110} = \mu^6 + \mu^5 + \mu^2$	$\mu^{122} = \mu^6 + \mu^5 + \mu^4 + \mu^3 + \mu^2 + 1$
$\mu^{99} = \mu^6 + \mu^4 + \mu^3 + \mu^2$	$\mu^{111} = \mu^6 + \mu^3 + \mu + 1$	$\mu^{123} = \mu^6 + \mu^5 + \mu^4 + \mu^3 + 1$
$\mu^{100} = \mu^5 + \mu^4 + \mu^3 + \mu + 1$	$\mu^{112} = \mu^4 + \mu^2 + 1$	$\mu^{124} = \mu^6 + \mu^5 + \mu^4 + 1$
$\mu^{101} = \mu^6 + \mu^5 + \mu^4 + \mu^2 + \mu$	$\mu^{113} = \mu^5 + \mu^3 + \mu$	$\mu^{125} = \mu^6 + \mu^5 + 1$
$\mu^{102} = \mu^6 + \mu^5 + \mu^3 + \mu^2 + \mu + 1$	$\mu^{114} = \mu^6 + \mu^4 + \mu^2$	$\mu^{126} = \mu^6 + 1$
$\mu^{103} = \mu^6 + \mu^4 + \mu^3 + \mu + 1$	$\mu^{115} = \mu^5 + \mu^3 + \mu + 1$	$\mu^{127} = 1$
$\mu^{104} = \mu^5 + \mu^4 + \mu^3 + 1$	$\mu^{116} = \mu^6 + \mu^4 + \mu^2 + \mu$	
$\mu^{105} = \mu^6 + \mu^5 + \mu^4 + \mu$	$\mu^{117} = \mu^5 + \mu^3 + \mu^2 + \mu + 1$	

$F_{2^7} = F(\sigma)\,,\ burada\ \sigma\,, r(x) = x^7 + x^3 + 1$ in kökü olsun.

Şimdi $F_{2^7}/r(x)$ sonlu cisminin elemanlarını tablo yardımı ile gösterelim.

Tablo 3.6. $F_{2^7}/r(x)$ sonlu cisminin elemanları

$\sigma^7 = \sigma^3 + 1$	$\sigma^{19} = \sigma^5 + \sigma^4 + \sigma^3 + 1$	$\sigma^{31} = \sigma + 1$
$\sigma^8 = \sigma^4 + \sigma$	$\sigma^{20} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma$	$\sigma^{32} = \sigma^2 + \sigma$
$\sigma^9 = \sigma^5 + \sigma^2$	$\sigma^{21} = \sigma^6 + \sigma^5 + \sigma^3 + \sigma^2 + 1$	$\sigma^{33} = \sigma^3 + \sigma^2$
$\sigma^{10} = \sigma^6 + \sigma^3$	$\sigma^{22} = \sigma^6 + \sigma^4 + \sigma + 1$	$\sigma^{34} = \sigma^4 + \sigma^3$
$\sigma^{11} = \sigma^4 + \sigma^3 + 1$	$\sigma^{23} = \sigma^5 + \sigma^3 + \sigma^2 + \sigma + 1$	$\sigma^{35} = \sigma^5 + \sigma^4$
$\sigma^{12} = \sigma^5 + \sigma^4 + \sigma$	$\sigma^{24} = \sigma^6 + \sigma^4 + \sigma^3 + \sigma^2 + \sigma$	$\sigma^{36} = \sigma^6 + \sigma^5$
$\sigma^{13} = \sigma^6 + \sigma^5 + \sigma^2$	$\sigma^{25} = \sigma^5 + \sigma^4 + \sigma^2 + 1$	$\sigma^{37} = \sigma^6 + \sigma^3 + 1$
$\sigma^{14} = \sigma^6 + 1$	$\sigma^{26} = \sigma^6 + \sigma^5 + \sigma^3 + \sigma$	$\sigma^{38} = \sigma^4 + \sigma^3 + \sigma + 1$
$\sigma^{15} = \sigma^3 + \sigma + 1$	$\sigma^{27} = \sigma^6 + \sigma^4 + \sigma^3 + \sigma^2 + 1$	$\sigma^{39} = \sigma^5 + \sigma^4 + \sigma^2 + \sigma$
$\sigma^{16} = \sigma^4 + \sigma^2 + \sigma$	$\sigma^{28} = \sigma^5 + \sigma^4 + \sigma + 1$	$\sigma^{40} = \sigma^6 + \sigma^5 + \sigma^3 + \sigma^2$
$\sigma^{17} = \sigma^5 + \sigma^3 + \sigma^2$	$\sigma^{29} = \sigma^6 + \sigma^5 + \sigma^2 + \sigma$	$\sigma^{41} = \sigma^6 + \sigma^4 + 1$
$\sigma^{18} = \sigma^6 + \sigma^4 + \sigma^3$	$\sigma^{30} = \sigma^6 + \sigma^2 + 1$	$\sigma^{42} = \sigma^5 + \sigma^3 + \sigma + 1$
$\sigma^{43} = \sigma^6 + \sigma^4 + \sigma^2 + \sigma$	$\sigma^{57} = \sigma^5 + \sigma^4 + \sigma^2 + \sigma + 1$	$\sigma^{71} = \sigma^5 + \sigma^4 + \sigma^3 + \sigma^2 + 1$
$\sigma^{44} = \sigma^5 + \sigma^2 + 1$	$\sigma^{58} = \sigma^6 + \sigma^5 + \sigma^3 + \sigma^2 + \sigma$	$\sigma^{72} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^3 + \sigma$
$\sigma^{45} = \sigma^6 + \sigma^3 + \sigma$	$\sigma^{59} = \sigma^6 + \sigma^4 + \sigma^2 + 1$	$\sigma^{73} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^3 + \sigma^2 + 1$
$\sigma^{46} = \sigma^4 + \sigma^3 + \sigma^2 + 1$	$\sigma^{60} = \sigma^5 + \sigma + 1$	$\sigma^{74} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma + 1$
$\sigma^{47} = \sigma^5 + \sigma^4 + \sigma^3 + \sigma$	$\sigma^{61} = \sigma^6 + \sigma^2 + \sigma$	$\sigma^{75} = \sigma^6 + \sigma^5 + \sigma^3 + \sigma^2 + \sigma + 1$
$\sigma^{48} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^2$	$\sigma^{62} = \sigma^2 + 1$	$\sigma^{76} = \sigma^6 + \sigma^4 + \sigma^2 + \sigma + 1$
$\sigma^{49} = \sigma^6 + \sigma^5 + 1$	$\sigma^{63} = \sigma^3 + \sigma$	$\sigma^{77} = \sigma^5 + \sigma^2 + \sigma + 1$

Tablo 3.7.(Devamı) $F_{2^7}/r(x)$ sonlu cisminin elemanları

$\sigma^{50} = \sigma^6 + \sigma^3 + \sigma + 1$	$\sigma^{64} = \sigma^4 + \sigma^2$	$\sigma^{78} = \sigma^6 + \sigma^3 + \sigma^2 + \sigma$
$\sigma^{51} = \sigma^4 + \sigma^3 + \sigma^2 + \sigma + 1$	$\sigma^{65} = \sigma^5 + \sigma^3$	$\sigma^{79} = \sigma^4 + \sigma^2 + 1$
$\sigma^{52} = \sigma^5 + \sigma^4 + \sigma^3 + \sigma^2 + \sigma$	$\sigma^{66} = \sigma^6 + \sigma^4$	$\sigma^{80} = \sigma^5 + \sigma^3 + \sigma$
$\sigma^{53} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^3 + \sigma^2$	$\sigma^{67} = \sigma^5 + \sigma^3 + 1$	$\sigma^{81} = \sigma^6 + \sigma^4 + \sigma^2$
$\sigma^{54} = \sigma^6 + \sigma^5 + \sigma^4 + 1$	$\sigma^{68} = \sigma^6 + \sigma^4 + \sigma$	$\sigma^{82} = \sigma^5 + 1$
$\sigma^{55} = \sigma^6 + \sigma^5 + \sigma^3 + \sigma + 1$	$\sigma^{69} = \sigma^5 + \sigma^3 + \sigma^2 + 1$	$\sigma^{83} = \sigma^6 + \sigma$
$\sigma^{56} = \sigma^6 + \sigma^4 + \sigma^3 + \sigma^2 + \sigma + 1$	$\sigma^{70} = \sigma^6 + \sigma^4 + \sigma^3 + \sigma$	$\sigma^{84} = \sigma^3 + \sigma^2 + 1$
$\sigma^{85} = \sigma^4 + \sigma^3 + \sigma$	$\sigma^{99} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^3 + \sigma^2 + \sigma + 1$	$\sigma^{113} = \sigma^6 + \sigma^5 + \sigma + 1$
$\sigma^{86} = \sigma^5 + \sigma^4 + \sigma^2$	$\sigma^{100} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^2 + \sigma + 1$	$\sigma^{114} = \sigma^6 + \sigma^3 + \sigma^2 + \sigma + 1$
$\sigma^{87} = \sigma^6 + \sigma^5 + \sigma^3$	$\sigma^{101} = \sigma^6 + \sigma^5 + \sigma^2 + \sigma + 1$	$\sigma^{115} = \sigma^4 + \sigma^2 + \sigma + 1$
$\sigma^{88} = \sigma^6 + \sigma^4 + \sigma^3 + 1$	$\sigma^{102} = \sigma^6 + \sigma^2 + \sigma + 1$	$\sigma^{116} = \sigma^5 + \sigma^3 + \sigma^2 + \sigma$
$\sigma^{89} = \sigma^5 + \sigma^4 + \sigma^3 + \sigma + 1$	$\sigma^{103} = \sigma^2 + \sigma + 1$	$\sigma^{117} = \sigma^6 + \sigma^4 + \sigma^3 + \sigma^2$
$\sigma^{90} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^2 + \sigma$	$\sigma^{104} = \sigma^3 + \sigma^2 + \sigma$	$\sigma^{118} = \sigma^5 + \sigma^4 + 1$
$\sigma^{91} = \sigma^6 + \sigma^5 + \sigma^2 + 1$	$\sigma^{105} = \sigma^4 + \sigma^3 + \sigma^2$	$\sigma^{119} = \sigma^6 + \sigma^5 + \sigma$
$\sigma^{92} = \sigma^6 + \sigma + 1$	$\sigma^{106} = \sigma^5 + \sigma^4 + \sigma^3$	$\sigma^{120} = \sigma^6 + \sigma^3 + \sigma^2 + 1$
$\sigma^{93} = \sigma^3 + \sigma^2 + \sigma + 1$	$\sigma^{107} = \sigma^6 + \sigma^5 + \sigma^4$	$\sigma^{121} = \sigma^4 + \sigma + 1$
$\sigma^{94} = \sigma^4 + \sigma^3 + \sigma^2 + \sigma$	$\sigma^{108} = \sigma^6 + \sigma^5 + \sigma^3 + 1$	$\sigma^{122} = \sigma^5 + \sigma^2 + \sigma$
$\sigma^{95} = \sigma^5 + \sigma^4 + \sigma^3 + \sigma^2$	$\sigma^{109} = \sigma^6 + \sigma^4 + \sigma^3 + \sigma + 1$	$\sigma^{123} = \sigma^6 + \sigma^3 + \sigma^2$

Tablo 3.8.(Devamı) $F_{2^7}/r(x)$ sonlu cisminin elemanları

$\sigma^{96} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^3$	$\sigma^{110} = \sigma^5 + \sigma^4 + \sigma^3 + \sigma^2 + \sigma + 1$	$\sigma^{124} = \sigma^4 + 1$
$\sigma^{97} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^3 + 1$	$\sigma^{111} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^3 + \sigma^2 + \sigma$	$\sigma^{125} = \sigma^5 + \sigma$
$\sigma^{98} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^3 + \sigma + 1$	$\sigma^{112} = \sigma^6 + \sigma^5 + \sigma^4 + \sigma^2 + 1$	$\sigma^{126} = \sigma^6 + \sigma^2$
$\sigma^{127} = 1$		

F_{2^6} , $p_2(x) = x^6 + x^3 + 1$ indirgenemez polinomu tarafından tanımlansın. $\delta + 1$, $p_2(x)$ in kökü olsun.

Tablo 3.9. $F_{2^6}/p_2(x)$ sonlu cisminin elemanları

$(\delta+1)^1 = \delta + 1$	$(\delta+1)^{12} = \delta^5 + \delta^4 + \delta^3 + \delta^2 + 1$	$(\delta+1)^{23} = \delta^5 + \delta^3 + \delta^2 + 1$
$(\delta+1)^2 = \delta^2 + 1$	$(\delta+1)^{13} = \delta^3 + \delta^2 + \delta$	$(\delta+1)^{24} = \delta^5 + \delta^4 + \delta^3 + \delta^2 + \delta$
$(\delta+1)^3 = \delta^2 + \delta^2 + \delta + 1$	$(\delta+1)^{14} = \delta^4 + \delta$	$(\delta+1)^{25} = \delta^3 + \delta + 1$
$(\delta+1)^4 = \delta^4 + 1$	$(\delta+1)^{15} = \delta^5 + \delta^4 + \delta^2 + \delta$	$(\delta+1)^{26} = \delta^4 + \delta^3 + \delta^2 + 1$
$(\delta+1)^5 = \delta^5 + \delta^4 + \delta + 1$	$(\delta+1)^{16} = \delta^4 + \delta + 1$	$(\delta+1)^{27} = \delta^5 + \delta^2 + \delta + 1$
$(\delta+1)^6 = \delta^4 + \delta^3 + \delta^2$	$(\delta+1)^{17} = \delta^5 + \delta^4 + \delta^2 + 1$	$(\delta+1)^{28} = \delta^5$
$(\delta+1)^7 = \delta^5 + \delta^2$	$(\delta+1)^{18} = \delta^4 + \delta^2 + \delta$	$(\delta+1)^{29} = \delta^5 + \delta^3 + 1$
$(\delta+1)^8 = \delta^5 + \delta^2 + 1$	$(\delta+1)^{19} = \delta^5 + \delta^4 + \delta^3 + \delta$	$(\delta+1)^{30} = \delta^5 + \delta^4 + \delta$
$(\delta+1)^9 = \delta^5 + \delta^2 + \delta$	$(\delta+1)^{20} = \delta^2 + \delta + 1$	$(\delta+1)^{31} = \delta^4 + \delta^3 + \delta^2 + \delta + 1$
$(\delta+1)^{10} = \delta^5 + \delta + 1$	$(\delta+1)^{21} = \delta^3 + 1$	$(\delta+1)^{32} = \delta^5 + 1$

Tablo 3.10.(Devamı) $F_{2^6}/p_2(x)$ sonlu cisminin elemanları

$(\delta+1)^{11}=\delta^5+\delta^3+\delta^2$	$(\delta+1)^{22}=\delta^4+\delta^3+\delta+1$	$(\delta+1)^{33}=\delta^5+\delta^3+\delta$
$(\delta+1)^{34}=\delta^5+\delta^4+\delta^2+\delta+1$	$(\delta+1)^{46}=\delta^4+\delta^3+\delta$	$(\delta+1)^{58}=\delta^3+\delta$
$(\delta+1)^{35}=\delta^4$	$(\delta+1)^{47}=\delta^5+\delta^3+\delta^2+\delta$	$(\delta+1)^{59}=\delta^4+\delta^3+\delta^2+\delta$
$(\delta+1)^{36}=\delta^5+\delta^4$	$(\delta+1)^{48}=\delta^5+\delta^4+\delta^3+\delta+1$	$(\delta+1)^{60}=\delta^5+\delta$
$(\delta+1)^{37}=\delta^4+\delta^3+1$	$(\delta+1)^{49}=\delta^2$	$(\delta+1)^{61}=\delta^5+\delta^3+\delta^2+\delta+1$
$(\delta+1)^{38}=\delta^5+\delta^3+\delta+1$	$(\delta+1)^{50}=\delta^3+\delta^2$	$(\delta+1)^{62}=\delta^5+\delta^4+\delta^3$
$(\delta+1)^{39}=\delta^5+\delta^4+\delta^2$	$(\delta+1)^{51}=\delta^4+\delta^2$	$(\delta+1)^{63}=1$
$(\delta+1)^{40}=\delta^4+\delta^2+1$	$(\delta+1)^{52}=\delta^5+\delta^4+\delta^3+\delta^2$	
$(\delta+1)^{41}=\delta^5+\delta^4+\delta^3+\delta^2+\delta+1$	$(\delta+1)^{53}=\delta^3+\delta^2+1$	
$(\delta+1)^{42}=\delta^3$	$(\delta+1)^{54}=\delta^4+\delta^2+\delta+1$	
$(\delta+1)^{43}=\delta^4+\delta^3$	$(\delta+1)^{55}=\delta^5+\delta^4+\delta^3+1$	
$(\delta+1)^{44}=\delta^5+\delta^3$	$(\delta+1)^{56}=\delta$	
$(\delta+1)^{45}=\delta^5+\delta^4+1$	$(\delta+1)^{57}=\delta^2+\delta$	

Örnek 3.1 x^6+x+1 indirgenemez polinomu ve F_{2^6} cismini ele alalım.

$G=\{x_0=\alpha^2, x_1=\alpha, x_2=\alpha^3, x_3=\alpha^3+\alpha^2+\alpha\}$ toplamsal alt grup *ve*

$I=\alpha^5+\alpha^4$ olsun. $y_i=I+x_i$ olmak üzere

$y_0=\alpha^5+\alpha^4+\alpha^2, y_1=\alpha^5+\alpha^4+\alpha, y_2=\alpha^5+\alpha^4+\alpha^3$ ve

$y_3=\alpha^5+\alpha^4+\alpha^3+\alpha^2+\alpha$ olarak bulunur.

$$A = \begin{bmatrix} \frac{1}{x_0+y_0} & \frac{1}{x_0+y_1} & \frac{1}{x_0+y_2} & \frac{1}{x_0+y_3} \\ \frac{1}{x_1+y_0} & \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & \frac{1}{x_1+y_3} \\ \frac{1}{x_2+y_0} & \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & \frac{1}{x_2+y_3} \\ \frac{1}{x_3+y_0} & \frac{1}{x_3+y_1} & \frac{1}{x_3+y_2} & \frac{1}{x_3+y_3} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{\alpha^5+\alpha^4} & \frac{1}{\alpha^5+\alpha^4+\alpha^2+\alpha} & \frac{1}{\alpha^5+\alpha^4+\alpha^3+\alpha^2} & \frac{1}{\alpha^5+\alpha^4+\alpha^3+\alpha} \\ \frac{1}{\alpha^5+\alpha^4+\alpha^2+\alpha} & \frac{1}{\alpha^5+\alpha^4} & \frac{1}{\alpha^5+\alpha^4+\alpha^3+\alpha} & \frac{1}{\alpha^5+\alpha^4+\alpha^3+\alpha^2} \\ \frac{1}{\alpha^5+\alpha^4+\alpha^3+\alpha^2} & \frac{1}{\alpha^5+\alpha^4+\alpha^3+\alpha} & \frac{1}{\alpha^5+\alpha^4} & \frac{1}{\alpha^5+\alpha^4+\alpha^2+\alpha} \\ \frac{1}{\alpha^5+\alpha^4+\alpha^3+\alpha} & \frac{1}{\alpha^5+\alpha^4+\alpha^3+\alpha^2} & \frac{1}{\alpha^5+\alpha^4+\alpha^2+\alpha} & \frac{1}{\alpha^5+\alpha^4} \end{bmatrix}$$

$\frac{1}{\alpha^5+\alpha^4} = \frac{\alpha^{63}}{\alpha^{10}} = \alpha^{53}$, $\frac{1}{\alpha^5+\alpha^4+\alpha^2+\alpha} = \frac{\alpha^{63}}{\alpha^{39}} = \alpha^{24}$, $\frac{1}{\alpha^5+\alpha^4+\alpha^3+\alpha^2} = \frac{\alpha^{63}}{\alpha^{20}} = \alpha^{43}$,

$\frac{1}{\alpha^5+\alpha^4+\alpha^3+\alpha} = \frac{\alpha^{63}}{\alpha^{42}} = \alpha^{21}$ olmak üzere matrisimiz en son aşağıdaki gibi bulunur:

$$A = \begin{bmatrix} \alpha^{53} & \alpha^{24} & \alpha^{43} & \alpha^{21} \\ \alpha^{24} & \alpha^{53} & \alpha^{21} & \alpha^{43} \\ \alpha^{43} & \alpha^{21} & \alpha^{53} & \alpha^{24} \\ \alpha^{21} & \alpha^{43} & \alpha^{24} & \alpha^{53} \end{bmatrix}$$

Burada A matrisimiz Cauchy tabanlı Hadamard matrisidir (Hadamard-Cauchy) fakat involutif değildir.A matrisinin involutif olması için matrisi $c = \sum_{j=0}^{n-1} \frac{1}{I+x_i}$ ile ya da herhangi bir satırdaki elemanların toplamı ile çarpmamız gerekiyor. Şimdi bu c yi bulalım.

$$c = \alpha^5 + \alpha^3 + \alpha + \alpha^4 + 1 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + 1$$

$$= \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1 = \alpha^{43}$$

$$A_1 = \frac{1}{c}.A = \begin{bmatrix} \alpha^{10} & \alpha^{44} & 1 & \alpha^{41} \\ \alpha^{44} & \alpha^{10} & \alpha^{41} & 1 \\ 1 & \alpha^{41} & \alpha^{10} & \alpha^{44} \\ \alpha^{41} & 1 & \alpha^{44} & \alpha^{10} \end{bmatrix}$$

involutif Hadamard Cauchy MDS matrisini elde ettik.

Bu matris için gereken XOR sayısı 38+4.3.6=110 dur.

F_{2^6} cismi p(x)=$x^6 + x + 1$ polinomu tarafından tanımlansın.α , $p(x)$ in kökü olsun ve A_1 matrisi $F_{2^6}/p(x)$ üzerinde $4x4$ involutif Hadamard-Cauchy MDS matrisidir.

$F_{2^6}/p_2(x)$ sonlu cismini ele alalım. Burada $p_2(x) = x^6 + x^3 + 1$ olsun. $p_2(x)$ in bir kökü $\beta = \alpha + 1$ olsun. Buna göre $p(\beta^{s_1}) = p((\alpha+1)^{s_1}) = 0$ olacak şekilde $(\alpha+1)^{s_1}$ elemanı nedir? Bu eleman bulunabilirse $F_{2^2}/p(x)$ ile $F_{2^6}/p_2(x)$ arasında izomorfizma kurulabilir. Böylece var olan MDS matris sayesinde yeni bir MDS matris elde edilir.

$$p((\alpha+1)^5) = ((\alpha+1)^5)^6 + (\alpha+1)^5 + 1 = (\alpha+1)^{30} + (\alpha+1)^5 + 1$$

$$= \alpha^5 + \alpha^4 + \alpha + \alpha^5 + \alpha^4 + \alpha + 1 + 1 = 0$$

O halde $f_{5,1}: \alpha \to (\alpha+1)^5$ izomorfizmasını kullanarak $F_{2^6}/p(x)$ üzerindeki A_1 matrisinden $F_{2^6}/p_2(x)$ üzerine A_1' $4x4$ Hadamard-Cauchy MDS matrisi aşağıdaki gibi oluşturulabilir:

$$A_1 = \begin{bmatrix} \alpha^{10} & \alpha^{44} & 1 & \alpha^{41} \\ \alpha^{44} & \alpha^{10} & \alpha^{41} & 1 \\ 1 & \alpha^{41} & \alpha^{10} & \alpha^{44} \\ \alpha^{41} & 1 & \alpha^{44} & \alpha^{10} \end{bmatrix} \xrightarrow{\alpha \to (\alpha+1)^5} \begin{bmatrix} (\alpha+1)^{50} & (\alpha+1)^{220} & 1 & (\alpha+1)^{205} \\ (\alpha+1)^{220} & (\alpha+1)^{50} & (\alpha+1)^{205} & 1 \\ 1 & (\alpha+1)^{205} & (\alpha+1)^{50} & (\alpha+1)^{220} \\ (\alpha+1)^{205} & 1 & (\alpha+1)^{220} & (\alpha+1)^{50} \end{bmatrix}$$

$$A_1' = \begin{bmatrix} (\alpha+1)^{50} & (\alpha+1)^{31} & 1 & (\alpha+1)^{16} \\ (\alpha+1)^{31} & (\alpha+1)^{50} & (\alpha+1)^{16} & 1 \\ 1 & (\alpha+1)^{16} & (\alpha+1)^{50} & (\alpha+1)^{31} \\ (\alpha+1)^{16} & 1 & (\alpha+1)^{31} & (\alpha+1)^{50} \end{bmatrix} =$$

$$\begin{bmatrix} \alpha^3+\alpha^2 & \alpha^4+\alpha^3+\alpha^2+\alpha+1 & 1 & \alpha^4+\alpha+1 \\ \alpha^4+\alpha^3+\alpha^2+\alpha+1 & \alpha^3+\alpha^2 & \alpha^4+\alpha+1 & 1 \\ 1 & \alpha^4+\alpha+1 & \alpha^3+\alpha^2 & \alpha^4+\alpha^3+\alpha^2+\alpha+1 \\ \alpha^4+\alpha+1 & 1 & \alpha^4+\alpha^3+\alpha^2+\alpha+1 & \alpha^3+\alpha^2 \end{bmatrix}$$

Toplam gereken XOR sayısı 38+4.3.6=110

Örnek 3.2 F_{2^6}, $p_2(x) = x^6 + x^3 + 1$ indirgenemez polinomu tarafından tanımlansın. $\alpha + 1$, $p_2(x)$ polinomunun bir kökü olsun.

$$G = \{x_0 = (\alpha+1)^2 = \alpha^2 + 1, x_1 = \alpha + 1, x_2 = (\alpha+1)^3 = \alpha^3 + \alpha^2 + \alpha + 1, \\ x_3 = (\alpha+1)^3 + (\alpha+1)^2 + \alpha + 1 = \alpha^3 + 1\}$$

toplamsal alt grup ve $y_i = I + x_i$ olmak üzere

$y_0 = \alpha^5 + \alpha^2 + \alpha + 1$, $y_1 = \alpha^5 + 1$, $y_2 = \alpha^5 + \alpha^3 + \alpha^2 + 1$,

$y_3 = \alpha^5 + \alpha^3 + \alpha + 1$ olarak y_i elemanları bulunur.

Buna göre Hadamard-Cauchy matrisi aşağıdaki gibi oluşturulabilir:

$$M_1 = \begin{bmatrix} \frac{1}{x_0+y_0} & \frac{1}{x_0+y_1} & \frac{1}{x_0+y_2} & \frac{1}{x_0+y_3} \\ \frac{1}{x_1+y_0} & \frac{1}{x_1+y_1} & \frac{1}{x_1+y_2} & \frac{1}{x_1+y_3} \\ \frac{1}{x_2+y_0} & \frac{1}{x_2+y_1} & \frac{1}{x_2+y_2} & \frac{1}{x_2+y_3} \\ \frac{1}{x_3+y_0} & \frac{1}{x_3+y_1} & \frac{1}{x_3+y_2} & \frac{1}{x_3+y_3} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{\alpha^5+\alpha} & \frac{1}{\alpha^5+\alpha^2} & \frac{1}{\alpha^5+\alpha^3} & \frac{1}{\alpha^5+\alpha^3+\alpha^2+\alpha} \\ \frac{1}{\alpha^5+\alpha^2} & \frac{1}{\alpha^5+\alpha} & \frac{1}{\alpha^5+\alpha^3+\alpha^2+\alpha} & \frac{1}{\alpha^5+\alpha^3} \\ \frac{1}{\alpha^5+\alpha^3} & \frac{1}{\alpha^5+\alpha^3+\alpha^2+\alpha} & \frac{1}{\alpha^5+\alpha} & \frac{1}{\alpha^5+\alpha^2} \\ \frac{1}{\alpha^5+\alpha^3+\alpha^2+\alpha} & \frac{1}{\alpha^5+\alpha^3} & \frac{1}{\alpha^5+\alpha^2} & \frac{1}{\alpha^5+\alpha} \end{bmatrix}$$

$\frac{1}{\alpha^5+\alpha} = \frac{(\alpha+1)^{63}}{(\alpha+1)^{60}} = (\alpha+1)^3$, $\frac{1}{\alpha^5+\alpha^2} = \frac{(\alpha+1)^{63}}{(\alpha+1)^7} = (\alpha+1)^{56}$

$\frac{1}{\alpha^5+\alpha^3} = \frac{(\alpha+1)^{63}}{(\alpha+1)^{44}} = (\alpha+1)^{19}$, $\frac{1}{\alpha^5+\alpha^3+\alpha^2+\alpha} = \frac{(\alpha+1)^{63}}{(\alpha+1)^{47}} = (\alpha+1)^{16}$

Yukarıda bulunan ifadeler *M* matrisinde yerine yazılınca matrisin yeni hali

$$\begin{bmatrix} (\alpha+1)^3 & (\alpha+1)^{56} & (\alpha+1)^{19} & (\alpha+1)^{16} \\ (\alpha+1)^{56} & (\alpha+1)^3 & (\alpha+1)^{16} & (\alpha+1)^{19} \\ (\alpha+1)^{19} & (\alpha+1)^{16} & (\alpha+1)^3 & (\alpha+1)^{56} \\ (\alpha+1)^{16} & (\alpha+1)^{19} & (\alpha+1)^{56} & (\alpha+1)^3 \end{bmatrix}$$ şeklinde elde edilir. Fakat bu matris involutif değildir. Matrisi involutif yapmak için $c = \sum_{j=0}^{n-1} \frac{1}{I+x_i}$(ya da c, matrisin herhangi bir satırının elemanları toplamı) elemanını bulmalıyız.

$c = \alpha^3 + \alpha^2 + \alpha + 1 + \alpha + \alpha^5 + \alpha^4 + \alpha^3 + \alpha + \alpha^4 + \alpha + 1$

$= \alpha^5 + \alpha^2 = (\alpha+1)^7$

$$\frac{1}{c}.M_1 = \begin{bmatrix} (\alpha+1)^{59} & (\alpha+1)^{49} & (\alpha+1)^{12} & (\alpha+1)^9 \\ (\alpha+1)^{49} & (\alpha+1)^{59} & (\alpha+1)^9 & (\alpha+1)^{12} \\ (\alpha+1)^{12} & (\alpha+1)^9 & (\alpha+1)^{59} & (\alpha+1)^{49} \\ (\alpha+1)^9 & (\alpha+1)^{12} & (\alpha+1)^{49} & (\alpha+1)^{59} \end{bmatrix}$$

$\frac{1}{c}.M_1$ matrisi $F_{2^6}/(x^6+x^3+1)$ üzerinde $4x4$ involutif Hadamard-Cauchy matrisidir.

Bu matris için gereken XOR sayısı 49+4.4.6=145

$F_{2^6}/p(x)$,burada $p(x) = (x^6 + x + 1)$ olmak üzere , sonlu cismini ele alalım.

$\alpha_1 = \beta + 1$, $p(x)$ in bir kökü olsun.

$p({\alpha_1}^{s_1}) = 0$ olacak şekilde ${\alpha_1}^{s_1} = (\beta + 1)^{s_1}$ var mıdır?

$p_2(x) = x^6 + x^3 + 1$ olmak üzere

$((\beta + 1)^7)^6 + (\beta + 1)^7)^3 + 1 = (\beta + 1)^{42} + (\beta + 1)^{21} + 1 =$

$\beta^3 + \beta^3 + 1 + 1 = 0$

$f_{7,1}: \alpha \to (\beta + 1)^7$ izomorfizmasını kullanarak $F_{2^6}/p_2(x)$ cismi üzerindeki $\frac{1}{c}.M_1$ matrisinden $F_{2^6}/p(x)$ cismi üzerine M_1' matrisi aşağıdaki gibi oluşturulabilir:

$$\frac{1}{c}.M_1 = \begin{bmatrix} (\alpha+1)^{59} & (\alpha+1)^{49} & (\alpha+1)^{12} & (\alpha+1)^{9} \\ (\alpha+1)^{49} & (\alpha+1)^{59} & (\alpha+1)^{9} & (\alpha+1)^{12} \\ (\alpha+1)^{12} & (\alpha+1)^{9} & (\alpha+1)^{59} & (\alpha+1)^{49} \\ (\alpha+1)^{9} & (\alpha+1)^{12} & (\alpha+1)^{49} & (\alpha+1)^{59} \end{bmatrix} \xrightarrow{\alpha \to (\beta+1)^7} \begin{bmatrix} \beta^{35} & \beta^{28} & \beta^{21} & 1 \\ \beta^{28} & \beta^{35} & 1 & \beta^{21} \\ \beta^{21} & 1 & \beta^{35} & \beta^{28} \\ 1 & \beta^{21} & \beta^{28} & \beta^{35} \end{bmatrix} =$$

$$\begin{bmatrix} \beta^3+\beta+1 & \beta^4+\beta^3+\beta^2 & \beta^5+\beta^4+\beta^3+\beta+1 & 1 \\ \beta^4+\beta^3+\beta^2 & \beta^3+\beta+1 & 1 & \beta^5+\beta^4+\beta^3+\beta+1 \\ \beta^5+\beta^4+\beta^3+\beta+1 & 1 & \beta^3+\beta+1 & \beta^4+\beta^3+\beta^2 \\ 1 & \beta^5+\beta^4+\beta^3+\beta+1 & \beta^4+\beta^3+\beta^2 & \beta^3+\beta+1 \end{bmatrix}$$

Bu matris için gereken XOR sayısı 39+4.3.6=111

Örnek 3.3 F_{2^6} , $p(x) = x^6 + x + 1$ polinomu tarafından tanımlansın. α , $p(x)$ in bir kökü olsun. $M_2 = Ghad(a_0, a_1, b_1, a_2, b_2, a_3, b_3) =$
$Ghad(1, \alpha^{32}, \alpha^{32}, \alpha, \alpha, \alpha^{35}, \alpha^{34})$ matrisi $F_{2^6}/p(x)$ üzerinde $4x4$ involutif MDS matrisidir.

${b_1}^{-1} = \alpha^{31}$, ${b_2}^{-1} = \alpha^{62}$, ${b_3}^{-1} = \alpha^{29}$ olmak üzere;

$$M_2 = \begin{bmatrix} a_0 & a_1b_1 & a_2b_2 & a_3b_3 \\ a_1{b_1}^{-1} & a_0 & a_3{b_1}^{-1}b_2 & a_2{b_1}^{-1}b_3 \\ a_2{b_2}^{-1} & a_3{b_2}^{-1}b_1 & a_0 & a_1{b_2}^{-1}b_3 \\ a_3{b_3}^{-1} & a_2{b_3}^{-1}b_1 & a_1{b_3}^{-1}b_2 & a_0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^{32}.\alpha^{32} & \alpha.\alpha. & \alpha^{35}.\alpha^{34} \\ \alpha^{32}.\alpha^{31} & 1 & \alpha^{35}.\alpha^{31}.\alpha & \alpha.\alpha^{31}.\alpha^{34} \\ \alpha.\alpha^{62} & \alpha^{35}.\alpha^{62}.\alpha^{32} & 1 & \alpha^{32}.\alpha^{62}.\alpha^{34} \\ \alpha^{35}.\alpha^{29} & \alpha.\alpha^{29}.\alpha^{32} & \alpha^{32}.\alpha^{29}.\alpha & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^{64} & \alpha^{2} & \alpha^{69} \\ \alpha^{63} & 1 & \alpha^{67} & \alpha^{66} \\ \alpha^{63} & \alpha^{129} & 1 & \alpha^{128} \\ \alpha^{64} & \alpha^{62} & \alpha^{62} & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha & \alpha^{2} & \alpha^{6} \\ 1 & 1 & \alpha^{4} & \alpha^{3} \\ 1 & \alpha^{3} & 1 & \alpha^{2} \\ \alpha & \alpha^{62} & \alpha^{62} & 1 \end{bmatrix}$$

Toplam gereken XOR sayısı=24+4.3.6=96.

Örnek 3.4 F_{2^7} , $r(x) = x^7 + x^3 + 1$ indirgenemez polinomu tarafından tanımlansın. α , $r(x)$ in bir kökü olsun.

$G = \{x_0 = \alpha^2 + \alpha\, , x_1 = \alpha^3\, , x_2 = \alpha^4\, , x_3 = \alpha^4 + \alpha^3 + \alpha^2 + \alpha\}$ toplamsal alt grup olmak üzere $I = \alpha^6 + \alpha^5$ olsun. $y_i = I + x_i$ olmak üzere y_i ler

$y_0 = \alpha^6 + \alpha^5 + \alpha^2 + \alpha$, $y_1 = \alpha^6 + \alpha^5 + \alpha^3$, $y_2 = \alpha^6 + \alpha^5 + \alpha^4$

$y_3 = \alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha$ olarak bulunur.

$$M_3 = \begin{bmatrix} \frac{1}{x_0 + y_0} & \frac{1}{x_0 + y_1} & \frac{1}{x_0 + y_2} & \frac{1}{x_0 + y_3} \\ \frac{1}{x_1 + y_0} & \frac{1}{x_1 + y_1} & \frac{1}{x_1 + y_2} & \frac{1}{x_1 + y_3} \\ \frac{1}{x_2 + y_0} & \frac{1}{x_2 + y_1} & \frac{1}{x_2 + y_2} & \frac{1}{x_2 + y_3} \\ \frac{1}{x_3 + y_0} & \frac{1}{x_3 + y_1} & \frac{1}{x_3 + y_2} & \frac{1}{x_3 + y_3} \end{bmatrix}$$

$$= \begin{bmatrix} \frac{1}{\alpha^6 + \alpha^5} & \frac{1}{\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha} & \frac{1}{\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha} & \frac{1}{\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3} \\ \frac{1}{\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha} & \frac{1}{\alpha^6 + \alpha^5} & \frac{1}{\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3} & \frac{1}{\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha} \\ \frac{1}{\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha} & \frac{1}{\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3} & \frac{1}{\alpha^6 + \alpha^5} & \frac{1}{\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha} \\ \frac{1}{\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3} & \frac{1}{\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha} & \frac{1}{\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha} & \frac{1}{\alpha^6 + \alpha^5} \end{bmatrix}$$

$\frac{1}{\alpha^6+\alpha^5} = \frac{\alpha^{127}}{\alpha^{36}} = \alpha^{91}$, $\frac{1}{\alpha^6+\alpha^5+\alpha^3+\alpha^2+\alpha} = \frac{\alpha^{127}}{\alpha^{58}} = \alpha^{69}$, $\frac{1}{\alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha} = \frac{\alpha^{127}}{\alpha^{90}} = \alpha^{37}$,

$\frac{1}{\alpha^6+\alpha^5+\alpha^4+\alpha^3} = \frac{\alpha^{127}}{\alpha^{96}} = \alpha^{31}$

$M_3 = \begin{bmatrix} \alpha^{91} & \alpha^{69} & \alpha^{37} & \alpha^{31} \\ \alpha^{69} & \alpha^{91} & \alpha^{31} & \alpha^{37} \\ \alpha^{37} & \alpha^{31} & \alpha^{91} & \alpha^{69} \\ \alpha^{31} & \alpha^{37} & \alpha^{69} & \alpha^{91} \end{bmatrix}$ matrisi Cauchy tabanlı Hadamard MDS matrisidir fakat involutif değildir.

İnvolutif yapmak için matrisi $c = \sum_{j=0}^{n-1} \frac{1}{I + x_i}$ değerine veya matrisin herhangi satırındaki elemanları toplayarak elde edilen c değerine bölerek M_3 matrisi involutif yapılabilir.

$c = \alpha^5 + \alpha^2 + \alpha^6 + 1 + \alpha^5 + \alpha^2 + \alpha^3 + 1 + \alpha^6 + \alpha^3 + 1 + \alpha + 1 = \alpha$

$$\frac{1}{c}M_3 = \begin{bmatrix} \alpha^{90} & \alpha^{68} & \alpha^{36} & \alpha^{30} \\ \alpha^{68} & \alpha^{90} & \alpha^{30} & \alpha^{36} \\ \alpha^{36} & \alpha^{30} & \alpha^{90} & \alpha^{68} \\ \alpha^{30} & \alpha^{36} & \alpha^{68} & \alpha^{90} \end{bmatrix}$$

Matrisi artık involutif MDS matristir.

Bu matris için gereken XOR sayısı 284+4.4.7=396

$q(x) = x^7 + x + 1$ olmak üzere $F_{2^7}/q(x)$ sonlu cismini ele alalım. Burada β , $q(x)$ in bir kökü olsun. $r(\beta^{s_u}) = 0$ olacak şekilde β^{s_u} var mıdır?

$r(\beta^{11}) = (\beta^{11})^7 + (\beta^{11})^3 + 1 = \beta^{77} + \beta^{33} + 1$

$= \beta^5 + \beta^3 + \beta^2 + 1 + \beta^5 + \beta^3 + \beta^2 + 1 = 0$

$f_{11,1}: \alpha \to \beta^{11}$ izomorfizmasını kullanarak $F_{2^7}/r(x)$ üzerindeki $\frac{1}{c}M_3$ matrisinden $F_{2^7}/q(x)$ üzerine M_3' $4x4$ involutif Hadamard-Cauchy MDS matrisi aşağıdaki gibi oluşturulabilir.

$$\frac{1}{c}M_3 = \begin{bmatrix} \alpha^{90} & \alpha^{68} & \alpha^{36} & \alpha^{30} \\ \alpha^{68} & \alpha^{90} & \alpha^{30} & \alpha^{36} \\ \alpha^{36} & \alpha^{30} & \alpha^{90} & \alpha^{68} \\ \alpha^{30} & \alpha^{36} & \alpha^{68} & \alpha^{90} \end{bmatrix} \xrightarrow{\alpha \to \beta^{11}} \begin{bmatrix} (\beta^{11})^{90} & (\beta^{11})^{68} & (\beta^{11})^{36} & (\beta^{11})^{30} \\ (\beta^{11})^{68} & (\beta^{11})^{90} & (\beta^{11})^{30} & (\beta^{11})^{36} \\ (\beta^{11})^{36} & (\beta^{11})^{30} & (\beta^{11})^{90} & (\beta^{11})^{68} \\ (\beta^{11})^{30} & (\beta^{11})^{36} & (\beta^{11})^{68} & (\beta^{11})^{90} \end{bmatrix}$$

$$= \begin{bmatrix} \beta^{101} & \beta^{113} & \beta^{15} & \beta^{76} \\ \beta^{113} & \beta^{101} & \beta^{76} & \beta^{15} \\ \beta^{15} & \beta^{76} & \beta^{101} & \beta^{113} \\ \beta^{76} & \beta^{15} & \beta^{113} & \beta^{101} \end{bmatrix} = M_3'$$

$$M_3' = \begin{bmatrix} \beta^6 + \beta^5 + \beta^4 + \beta^2 + \beta & \beta^5 + \beta^3 + \beta & \beta^3 + \beta & \beta^6 + \beta^4 + \beta^2 + \beta + 1 \\ \beta^5 + \beta^3 + \beta & \beta^6 + \beta^5 + \beta^4 + \beta^2 + \beta & \beta^6 + \beta^4 + \beta^2 + \beta + 1 & \beta^3 + \beta \\ \beta^3 + \beta & \beta^6 + \beta^4 + \beta^2 + \beta + 1 & \beta^6 + \beta^5 + \beta^4 + \beta^2 + \beta & \beta^5 + \beta^3 + \beta \\ \beta^6 + \beta^4 + \beta^2 + \beta + 1 & \beta^3 + \beta & \beta^5 + \beta^3 + \beta & \beta^6 + \beta^5 + \beta^4 + \beta^2 + \beta \end{bmatrix}$$

Bu matris için gereken XOR sayısı 87+4.4.7=199

Örnek 3.5 Genelleştirilmiş Hadamard matris formuna göre F_{2^7} da $4x4$ involutif MDS matris oluşturalım.

$a_0 = 1, a_1 = \alpha + 1, a_2 = \alpha^2 + \alpha$, $a_3 = \alpha^2 + 1$,

$b_1 = \alpha$, $b_2 = \alpha^4 + \alpha$, $b_3 = \alpha^3 + \alpha + 1$ olsun ve $b_1^{-1} = \alpha^{126} = \alpha^6 + 1$,

$b_2^{-1} = \alpha^{63} = \alpha^3 + 1$, $b_3^{-1} = \alpha^{96} = \alpha^6 + \alpha^3 + \alpha$ olur.

Ayrıca $a_0 + a_1 + a_2 + a_3 = 1$ olursa matris involutif olacaktır.

$1 + \alpha + 1 + \alpha^2 + \alpha + \alpha^2 + 1 = 1$ olduğundan oluşturulan matris involutif olacaktır.

$$M_4 = \begin{bmatrix} a_0 & a_1b_1 & a_2b_2 & a_3b_3 \\ a_1{b_1}^{-1} & a_0 & a_3{b_1}^{-1}b_2 & a_2{b_1}^{-1}b_3 \\ a_2{b_2}^{-1} & a_3{b_2}^{-1}b_1 & a_0 & a_1{b_2}^{-1}b_3 \\ a_3{b_3}^{-1} & a_2{b_3}^{-1}b_1 & a_1{b_3}^{-1}b_2 & a_0 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^7.\alpha & \alpha^8.\alpha^{64} & \alpha^{14}.\alpha^{31} \\ \alpha^7.\alpha^{126} & 1 & \alpha^{14}.\alpha^{126}.\alpha^{64} & \alpha^8.\alpha^{126}.\alpha^{31} \\ \alpha^8.\alpha^{63} & \alpha^{14}.\alpha^{63}.\alpha & 1 & \alpha^7.\alpha^{63}.\alpha^{31} \\ \alpha^{14}.\alpha^{96} & \alpha^8.\alpha^{96}.\alpha & \alpha^7.\alpha^{96}.\alpha^{64} & 1 \end{bmatrix} = \begin{bmatrix} 1 & \alpha^8 & \alpha^{72} & \alpha^{45} \\ \alpha^6 & 1 & \alpha^{77} & \alpha^{38} \\ \alpha^{71} & \alpha^{78} & 1 & \alpha^{101} \\ \alpha^{110} & \alpha^{105} & \alpha^{40} & 1 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & \alpha^2+\alpha & \alpha^6+\alpha^5+\alpha^3+\alpha^2 & \alpha^5+\alpha^2+\alpha+1 \\ \alpha^6 & 1 & \alpha^5+\alpha^3+\alpha^2+1 & \alpha^4+\alpha^3+\alpha^2+1 \\ \alpha^5+\alpha^4+\alpha^2+\alpha & \alpha^6+\alpha^4+\alpha^3+\alpha & 1 & \alpha^6+\alpha^5+\alpha^4+\alpha^2+\alpha \\ \alpha^6+\alpha^5+\alpha^2 & \alpha^6+\alpha^5+\alpha^4+\alpha & \alpha^6+\alpha^5+\alpha^4+\alpha^2 & 1 \end{bmatrix}$$

Şimdi bu matrisin XOR sayısını bulalım.

$$\alpha^8(a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$$

$$= a_6\alpha^{14} + a_5\alpha^{13} + a_4\alpha^{12} + a_3\alpha^{11} + a_2\alpha^{10} + a_1\alpha^9 + a_0\alpha^8$$

$$= a_6(\alpha^2+1) + a_5(\alpha^6+\alpha+1) + a_4(\alpha^6+\alpha^5) + a_3(\alpha^5+\alpha^4) + a_2(\alpha^4+\alpha^3)$$

$$+a_1(\alpha^3+\alpha^2) + a_0(\alpha^2+\alpha)$$

$$= \alpha^6(a_5+a_4) + \alpha^5(a_4+a_3) + \alpha^4(a_3+a_2) + \alpha^3(a_2+a_1) + \alpha^2(a_6+a_1+a_0)$$

$$+\alpha(a_5+a_0) + a_6 + a_5$$

$$= (a_5 \oplus a_4, a_4 \oplus a_3, a_3 \oplus a_2, a_2 \oplus a_1, a_6 \oplus a_1 \oplus a_0, a_5 \oplus a_0, a_6 \oplus a_5)$$

Toplam artıların sayısı=8 dir.

$$\alpha^{72}(a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$$
$$= a_6\alpha^{78} + a_5\alpha^{77} + a_4\alpha^{76} + a_3\alpha^{75} + a_2\alpha^{74} + a_1\alpha^{73} + a_0\alpha^{72}$$
$$= a_6(\alpha^6+\alpha^4+\alpha^3+\alpha) + a_5(\alpha^5+\alpha^3+\alpha^2+1) + a_4(\alpha^6+\alpha^4+\alpha^2+\alpha+1)$$
$$+ a_3(\alpha^6+\alpha^5+\alpha^3+\alpha) + a_2(\alpha^5+\alpha^4+\alpha^2+1) + a_1(\alpha^6+\alpha^4+\alpha^3+\alpha+1)$$
$$+ a_0(\alpha^6+\alpha^5+\alpha^3+\alpha^2) =$$
$$= \alpha^6(a_6+a_4+a_3+a_1+a_0) + \alpha^5(a_5+a_3+a_2+a_0) + \alpha^4(a_6+a_4+a_2+a_1)$$
$$+ \alpha^3(a_6+a_5+a_3+a_1+a_0) + \alpha^2(a_5+a_4+a_2+a_0) + \alpha(a_6+a_4+a_3+a_1)$$
$$+ a_5 + a_4 + a_2 + a_1$$
$$= \begin{pmatrix} a_6 \oplus a_4 \oplus a_3 \oplus a_1 \oplus a_0, a_5 \oplus a_3 \oplus a_2 \oplus a_0, a_6 \oplus a_4 \oplus a_2 \oplus a_1, a_6 \oplus a_5 \oplus a_3 \oplus a_1 \oplus a_0, \\ a_5 \oplus a_4 \oplus a_2 \oplus a_0, a_6 \oplus a_4 \oplus a_3 \oplus a_1, a_5 \oplus a_4 \oplus a_2 \oplus a_1 \end{pmatrix}$$

Toplam artı sayısı =23

$$\alpha^{45}(a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$$

$= a_6\alpha^{51} + a_5\alpha^{50} + a_4\alpha^{49} + a_3\alpha^{48} + a_2\alpha^{47} + a_1\alpha^{46} + a_0\alpha^{45}$

$= a_6(\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + 1) + a_5(\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha$+1)+$a_4(\alpha^6 + \alpha^5 +$
$\alpha^4 + \alpha^3 + \alpha^2) + a_3(\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha) + a_2(\alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) +$
$a_1(\alpha^6 + \alpha^3 + \alpha^2 + \alpha) + a_0(\alpha^5 + \alpha^2 + \alpha + 1)$

$= \alpha^6(a_6 + a_5 + a_4 + a_1) + \alpha^5(a_6 + a_5 + a_4 + a_3 + a_0)$

$+\alpha^4(a_6 + a_5 + a_4 + a_3 + a_2) + \alpha^3(a_5 + a_4 + a_3 + a_2 + a_1)$

$+\alpha^2(a_6 + a_4 + a_3 + a_2 + a_1 + a_0) + \alpha(a_5 + a_3 + a_2 + a_1 + a_0) + a_6 + a_5 + a_2$

$+a_0 = (a_6 \oplus a_5 \oplus a_4 \oplus a_1, a_6 \oplus a_5 \oplus a_4 \oplus a_3 \oplus a_0, a_6 \oplus a_5 \oplus a_4 \oplus a_3$

$\oplus a_2, a_5 \oplus a_4 \oplus a_3 \oplus a_2 \oplus a_1, a_6 \oplus a_4 \oplus a_3 \oplus a_2 \oplus a_1 \oplus a_0, a_5 \oplus a_3 \oplus a_2$

$\oplus a_1 \oplus a_0, a_6 \oplus a_5 \oplus a_2 \oplus a_0)$

Toplam artı sayısı =27

$\alpha^6(a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$

$= a_6\alpha^{12} + a_5\alpha^{11} + a_4\alpha^{10} + a_3\alpha^9 + a_2\alpha^8 + a_1\alpha^7 + a_0\alpha^6$

$= a_6(\alpha^6 + \alpha^5) + a_5(\alpha^5 + \alpha^4) + a_4(\alpha^4 + \alpha^3) + a_3(\alpha^3 + \alpha^2) + a_2(\alpha^2 + \alpha)$

$+a_1(\alpha + 1) + a_0\alpha^6$

$= \alpha^6(a_6 + a_0) + \alpha^5(a_6 + a_5) + \alpha^4(a_5 + a_4)$

$+\alpha^3(a_4 + a_3) + \alpha^2(a_3 + a_2)$

$+\alpha(a_2 + a_1) + a_1 = (a_6 \oplus a_0, a_6 \oplus a_5, a_5 \oplus a_4, a_4 \oplus a_3, a_3 \oplus a_2, a_2 \oplus a_1, a_1)$

Topma artı sayısı=6

$\alpha^{77}(a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$

$= a_6\alpha^{83} + a_5\alpha^{82} + a_4\alpha^{81} + a_3\alpha^{80} + a_2\alpha^{79} + a_1\alpha^{78} + a_0\alpha^{77}$

$= a_6(\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha) + a_5(\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1)$

$+a_4(\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1) +$

$a_3(\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha) + a_2(\alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1)$

$+a_1(\alpha^6 + \alpha^4 + \alpha^3 + \alpha)$

$+a_0(\alpha^5 + \alpha^3 + \alpha^2 + 1)$

$= \alpha^6(a_6 + a_4 + a_3 + a_1) + \alpha^5(a_6 + a_5 + a_3 + a_2 + a_0)$

$$+\alpha^4(a_6+a_5+a_4+a_2+a_1)$$

$$+\alpha^3(a_6+a_5+a_4+a_3+a_1+a_0)+\alpha^2(a_5+a_4+a_3+a_2+a_0)$$

$$+\alpha(a_6+a_4+a_3+a_2+a_1)+a_5+a_4+a_2+a_0)$$

$$=\begin{matrix}(a_6\oplus a_4\oplus a_3\oplus a_1, a_6\oplus a_5\oplus a_3\oplus a_2\oplus a_0, a_6\oplus a_5\oplus a_4\oplus a_2\oplus a_1,\\ a_6\oplus a_5\oplus a_4\oplus a_3\oplus a_1\oplus a_0,\\ a_5\oplus a_4\oplus a_3\oplus a_2\oplus a_0, a_6\oplus a_4\oplus a_3\oplus a_2\oplus a_1, a_5\oplus a_4\oplus a_2\oplus a_0)\end{matrix}$$

Toplam artı sayısı=27

$$\alpha^{38}(a_6\alpha^6+a_5\alpha^5+a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0)$$

$$=a_6\alpha^{44}+a_5\alpha^{43}+a_4\alpha^{42}+a_3\alpha^{41}+a_2\alpha^{40}+a_1\alpha^{39}+a_0\alpha^{38}$$

$$=a_6(\alpha^6+\alpha^4+\alpha)+a_5(\alpha^5+\alpha^3+1)+a_4(\alpha^6+\alpha^4+\alpha^2+1)$$

$$+a_3(\alpha^6+\alpha^5+\alpha^3+\alpha+1)+a_2(\alpha^6+\alpha^5+\alpha^4+\alpha^2)$$

$$+a_1(\alpha^5+\alpha^4+\alpha^3+\alpha)+a_0(\alpha^4+\alpha^3+\alpha^2+1)$$

$$=\alpha^6(a_6+a_4+a_3+a_2)+\alpha^5(a_5+a_3+a_2+a_1)+\alpha^4(a_6+a_4+a_2+a_1+a_0)$$

$$+\alpha^3(a_5+a_3+a_1+a_0)+\alpha^2(a_4+a_2+a_0)$$

$$+\alpha(a_6+a_3+a_1)+a_5+a_4+a_3+a_0$$

$$=\begin{pmatrix}a_6\oplus a_4\oplus a_3\oplus a_2, a_5\oplus a_3\oplus a_2\oplus a_1, a_6\oplus a_4\oplus a_2\oplus a_1\oplus a_0, a_6,\\ a_5\oplus a_3\oplus a_1\oplus a_0, a_4\oplus a_2\oplus a_0,\\ a_6\oplus a_3\oplus a_1, a_5\oplus a_4\oplus a_3\oplus a_0\end{pmatrix}$$

Toplam artı sayısı=20

$$\alpha^{71}\left(a_6\alpha^6+a_5\alpha^5+a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0\right)$$
$$=a_6\alpha^{77}+a_5\alpha^{76}+a_4\alpha^{75}+a_3\alpha^{74}+a_2\alpha^{73}+a_1\alpha^{72}+a_0\alpha^{71}$$
$$=a_6\left(\alpha^5+\alpha^3+\alpha^2+1\right)+a_5\left(\alpha^6+\alpha^4+\alpha^2+\alpha+1\right)+a_4\left(\alpha^6+\alpha^5+\alpha^3+\alpha\right)$$
$$+a_3\left(\alpha^5+\alpha^4+\alpha^2+1\right)+a_2\left(\alpha^6+\alpha^4+\alpha^3+\alpha+1\right)+a_1\left(\alpha^6+\alpha^5+\alpha^3+\alpha^2\right)$$
$$+a_0\left(\alpha^5+\alpha^4+\alpha^2+\alpha\right)$$
$$=\alpha^6(a_5+a_4+a_2+a_1)+\alpha^5(a_6+a_4+a_3+a_1+a_0)+\alpha^4(a_5+a_3+a_2+a_0)$$
$$+\alpha^3(a_6+a_4+a_2+a_1)+\alpha^2(a_6+a_5+a_3+a_1+a_0)+\alpha(a_5+a_4+a_2+a_0)$$
$$+a_6+a_5+a_3+a_2$$
$$=\begin{pmatrix}a_5\oplus a_4\oplus a_2\oplus a_1, a_6\oplus a_4\oplus a_3\oplus a_1\oplus a_0, a_5\oplus a_3\oplus a_2\oplus a_0, a_6\oplus a_4\oplus a_2\oplus a_1,\\ a_6\oplus a_5\oplus a_3\oplus a_1\oplus a_0,\\ a_5\oplus a_4\oplus a_2\oplus a_0, a_6\oplus a_5\oplus a_3\oplus a_2\end{pmatrix}$$

Toplam artı sayısı=23

$$\alpha^{78}\left(a_6\alpha^6+a_5\alpha^5+a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0\right)$$

$$= a_6\alpha^{84} + a_5\alpha^{83} + a_4\alpha^{82} + a_3\alpha^{81} + a_2\alpha^{80} + a_1\alpha^{79} + a_0\alpha^{78}$$

$$= a_6(\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1) + a_5(\alpha^6 + \alpha^5 + \alpha^4 + \alpha^3 + \alpha)$$

$$+a_4(\alpha^5 + \alpha^4 + \alpha^3 + \alpha^2 + 1) + a_3(\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + \alpha + 1)$$

$$+a_2(\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha) + a_1(\alpha^5 + \alpha^4 + \alpha^2 + \alpha + 1)$$

$$+a_0(\alpha^6 + \alpha^4 + \alpha^3 + \alpha)$$

$$= \alpha^6(a_6 + a_5 + a_3 + a_2 + a_0) + \alpha^5(a_6 + a_5 + a_4 + a_2 + a_1)$$

$$+\alpha^4(a_6 + a_5 + a_4 + a_3 + a_1 + a_0) + \alpha^3(a_5 + a_4 + a_3 + a_2 + a_0)$$

$$+\alpha^2(a_6 + a_4 + a_3 + a_2 + a_1) + \alpha(a_6 + a_5 + a_4 + a_3 + a_2 + a_1) + a_6 + a_4 + a_3$$

$$+a_1 = \begin{pmatrix} a_6 + a_5 + a_3 + a_2 + a_0, a_6 + a_5 + a_4 + a_2 + a_1, a_6 + a_5 + a_4 + a_3 + a_1 \\ +a_0, a_6 + a_5 + a_4 + a_3 + a_1 + a_0, a_5 + a_4 + a_3 + a_2 + a_0, a_6 \\ +a_4 + a_3 + a_2 + a_1, a_6 + a_4 + a_3 + a_1 \end{pmatrix}$$

Toplam artı sayısı=29

$$\alpha^{101}(a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$$

$$= a_6\alpha^{107} + a_5\alpha^{106} + a_4\alpha^{105} + a_3\alpha^{104} + a_2\alpha^{103} + a_1\alpha^{102} + a_0\alpha^{101}$$

$$= a_6(\alpha^6 + \alpha^3 + \alpha^2 + 1) + a_5(\alpha^6 + \alpha^5 + \alpha^2 + \alpha + 1) + a_4(\alpha^6 + \alpha^5 + \alpha^4 + \alpha)$$

$$+a_3(\alpha^5 + \alpha^4 + \alpha^3 + 1) + a_2(\alpha^6 + \alpha^4 + \alpha^3 + \alpha^2 + 1)$$

$$+a_1(\alpha^6 + \alpha^5 + \alpha^3 + \alpha^2 + \alpha + 1) + a_0(\alpha^6 + \alpha^5 + \alpha^4 + \alpha^2 + \alpha)$$

$$= \alpha^6(a_6 + a_5 + a_4 + a_2 + a_1 + a_0) + \alpha^5(a_5 + a_4 + a_3 + a_1 + a_0)$$

$$+\alpha^4(a_4 + a_3 + a_2 + a_0) + \alpha^3(a_6 + a_3 + a_2 + a_1) + \alpha^2(a_6 + a_5 + a_2 + a_1 + a_0)$$

$$+\alpha(a_5 + a_4 + a_1 + a_0) + a_6 + a_5 + a_3 + a_2 + a_1$$

$$= \begin{pmatrix} a_6 + a_5 + a_4 + a_2 + a_1 + a_0, a_5 + a_4 + a_3 + a_1 + a_0, a_4 + a_3 + a_2 + a_0, a_6 \\ +a_3 + a_2 + a_1, a_6 + a_5 + a_2 + a_1 + a_0, a_5 + a_4 + a_1 + a_0, \\ a_6 + a_5 + a_3 + a_2 + a_1 \end{pmatrix}$$

Toplam artı sayısı=26

$$\alpha^{110}(a_6\alpha^6 + a_5\alpha^5 + a_4\alpha^4 + a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$$

$$= a_6\alpha^{116} + a_5\alpha^{115} + a_4\alpha^{114} + a_3\alpha^{113} + a_2\alpha^{112} + a_1\alpha^{111} + a_0\alpha^{110}$$

$$= a_6(\alpha^6 + \alpha^4 + \alpha^2 + \alpha) + a_5(\alpha^5 + \alpha^3 + \alpha + 1) + a_4(\alpha^6 + \alpha^4 + \alpha^2)$$

$$+a_3(\alpha^5 + \alpha^3 + \alpha) + a_2(\alpha^4 + \alpha^2 + 1) + a_1(\alpha^6 + \alpha^3 + \alpha + 1)$$

$$+a_0(\alpha^6+\alpha^5+\alpha^2)$$

$$=\alpha^6(a_6+a_4+a_1+a_0)+\alpha^5(a_5+a_3+a_0)+\alpha^4(a_6+a_4+a_2)$$

$$+\alpha^3(a_5+a_3+a_1)+\alpha^2(a_6+a_4+a_2+a_0)+\alpha(a_6+a_5+a_3+a_1)+a_5+a_2$$

$$+a_1$$

$$=\begin{pmatrix}a_6+a_4+a_1+a_0, a_5+a_3+a_0, a_6+a_4+a_2, a_5+a_3+a_1, a_6+a_4+a_2\\ +a_0, a_6+a_5+a_3+a_1, a_5+a_2+a_1\end{pmatrix}$$

Toplam artı sayısı=17

$$\alpha^{105}(a_6\alpha^6+a_5\alpha^5+a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0)$$

$$=a_6\alpha^{111}+a_5\alpha^{110}+a_4\alpha^{109}+a_3\alpha^{108}+a_2\alpha^{107}+a_1\alpha^{106}+a_0\alpha^{105}$$

$$=a_6(\alpha^6+\alpha^3+\alpha+1)+a_5(\alpha^6+\alpha^5+\alpha^2)+a_4(\alpha^5+\alpha^4+\alpha)$$

$$+a_3(\alpha^4+\alpha^3+1)+a_2(\alpha^6+\alpha^3+\alpha^2+1)+a_1(\alpha^6+\alpha^5+\alpha^2+\alpha+1)$$

$$+a_0(\alpha^6+\alpha^5+\alpha^4+\alpha)7$$

$$=\alpha^6(a_6+a_5+a_2+a_1+a_0)+\alpha^5(a_5+a_4+a_1+a_0)+\alpha^4(a_4+a_3+a_0)$$

$$+\alpha^3(a_6+a_3+a_2)+\alpha^2(a_5+a_2+a_1)+\alpha(a_6+a_4+a_1+a_0)+a_6+a_3+a_2$$

$$+a_1$$

$$=\begin{pmatrix}a_6+a_5+a_2+a_1+a_0, a_5+a_4+a_1+a_0, a_4+a_3+a_0, a_6+a_3+a_2, a_5\\ +a_2+a_1, a_6+a_4+a_1+a_0, a_6+a_3+a_2+a_1\end{pmatrix}$$

Toplam artı sayısı=19

$$\alpha^{40}=(a_6\alpha^6+a_5\alpha^5+a_4\alpha^4+a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0)$$

$$=a_6\alpha^{46}+a_5\alpha^{45}+a_4\alpha^{44}+a_3\alpha^{43}+a_2\alpha^{42}+a_1\alpha^{41}+a_0\alpha^{40}$$

$$=a_6(\alpha^6+\alpha^3+\alpha^2+\alpha)+a_5(\alpha^5+\alpha^2+\alpha+1)+a_4(\alpha^6+\alpha^4+\alpha)$$

$$+a_3(\alpha^5+\alpha^3+1)+a_2(\alpha^6+\alpha^4+\alpha^2+1)+a_1(\alpha^6+\alpha^5+\alpha^3+\alpha+1)$$

$$+a_0(\alpha^6+\alpha^5+\alpha^4+\alpha^2)$$

$$=\alpha^6(a_6+a_4+a_2+a_1+a_0)+\alpha^5(a_5+a_3+a_1+a_0)+\alpha^4(a_4+a_2+a_0)$$

$$+\alpha^3(a_6+a_3+a_1)+\alpha^2(a_6+a_5+a_2+a_0)+\alpha(a_6+a_5+a_4+a_1)+a_5+a_3$$

$$+a_2+a_1=\begin{pmatrix}a_6+a_4+a_2+a_1+a_0, a_5+a_3+a_1+a_0, a_4+a_2+a_0, a_6+a_3\\ +a_1, a_6+a_5+a_2+a_0, a_6+a_5+a_4+a_1, a_5+a_3+a_2+a_1\end{pmatrix}$$

Toplam artı sayısı=20

Bütün artıların toplam sayısı 245 dir. Toplam gereken XOR sayısı ise 245+84=329
Şimdi matrisin involutif olduğunu gösterelim.

$$\begin{bmatrix} 1 & \alpha^8 & \alpha^{72} & \alpha^{45} \\ \alpha^6 & 1 & \alpha^{77} & \alpha^{38} \\ \alpha^{71} & \alpha^{78} & 1 & \alpha^{101} \\ \alpha^{110} & \alpha^{105} & \alpha^{40} & 1 \end{bmatrix} \cdot \begin{bmatrix} 1 & \alpha^8 & \alpha^{72} & \alpha^{45} \\ \alpha^6 & 1 & \alpha^{77} & \alpha^{38} \\ \alpha^{71} & \alpha^{78} & 1 & \alpha^{101} \\ \alpha^{110} & \alpha^{105} & \alpha^{40} & 1 \end{bmatrix} =$$

$$\begin{bmatrix} 1+\alpha^{14}+\alpha^{143}+\alpha^{155} & \alpha^8+\alpha^8+\alpha^{150}+\alpha^{150} & \alpha^{72}+\alpha^{85}+\alpha^{72}+\alpha^{85} & \alpha^{45}+\alpha^{46}+\alpha^{173}+\alpha^{45} \\ \alpha^6+\alpha^6+\alpha^{148}+\alpha^{148} & \alpha^{14}+1+\alpha^{155}+\alpha^{143} & \alpha^{78}+\alpha^{77}+\alpha^{77}+\alpha^{78} & \alpha^{51}+\alpha^{38}+\alpha^{178}+\alpha^{38} \\ \alpha^{71}+\alpha^{84}+\alpha^{71}+\alpha^{211} & \alpha^{79}+\alpha^{78}+\alpha^{78}+\alpha^{206} & \alpha^{143}+\alpha^{155}+1+\alpha^{151} & \alpha^{116}+\alpha^{116}+\alpha^{101}+\alpha^{101} \\ \alpha^{110}+\alpha^{111}+\alpha^{111}+\alpha^{110} & \alpha^{118}+\alpha^{105}+\alpha^{118}+\alpha^{105} & \alpha^{182}+\alpha^{182}+\alpha^{40}+\alpha^{40} & \alpha^{155}+\alpha^{143}+\alpha^{141}+1 \end{bmatrix} =$$

$$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Örnek 3.6 F_{2^6}/x^6+x+1 cisminde bir$4x4$ involutif MDS matris oluşturalım.

$M_5 = Ghad(a_0, a_1, b_1, a_2, b_2, a_3, b_3) = Ghad(\beta, 1, \beta^5+\beta^3, \beta+1, \beta, 1, \beta^3+1)$

ve $b_1^{-1}.(\beta^5+\beta^3) = 1 \Rightarrow b_1^{-1} = \beta^{48} = 1+\beta^3+\beta^2$

$b_2^{-1}.\beta = 1 \Rightarrow\ b_2^{-1} = \beta^{62} = 1+\beta^5$

$b_3^{-1}.\left(\beta^3+1\right) = 1 \Rightarrow b_3^{-1} = \beta^{31} = 1+\beta^5+\beta^2$

$a_0^2+a_1^2+a_2^2+a_3^2 = 1$ olmak üzere

$$M_5 = \begin{bmatrix} a_0 & a_1b_1 & a_2b_2 & a_3b_3 \\ a_1{b_1}^{-1} & a_0 & a_3{b_1}^{-1}b_2 & a_2{b_1}^{-1}b_3 \\ a_2{b_2}^{-1} & a_3{b_2}^{-1}b_1 & a_0 & a_1{b_2}^{-1}b_3 \\ a_3{b_3}^{-1} & a_2{b_3}^{-1}b_1 & a_1{b_3}^{-1}b_2 & a_0 \end{bmatrix} =$$

$$\begin{bmatrix} \beta & 1.(\beta^5+\beta^3) & (\beta+1).\beta & 1.(\beta^3+1) \\ 1.(1+\beta^3+\beta^2) & \beta & 1.(1+\beta^3+\beta^2).\beta & (\beta+1).(\beta^{48}).(\beta^3+1) \\ (\beta+1).(1+\beta^5) & 1.(1+\beta^5).(\beta^5+\beta^3) & \beta & 1.(1+\beta^5).(\beta^3+1) \\ 1.(1+\beta^5+\beta^2) & (\beta+1).(1+\beta^5+\beta^2).(\beta^5+\beta^3) & 1.(1+\beta^5+\beta^2).\beta & \beta \end{bmatrix}$$

$\rightarrow (\beta+1).(1+\beta^3+\beta^2).(\beta^3+1) = \beta^6.\beta^{48}.\beta^{32} = \beta^{86} = \beta^5+\beta^3+1$

$\rightarrow (\beta+1).(1+\beta^5) = \beta^6.\beta^{62} = \beta^5$

$\rightarrow (1+\beta^5).(\beta^5+\beta^3) = \beta^{62}.\beta^{15} = \beta^{14} = \beta^4+\beta^2$

$\rightarrow (1+\beta^5).(\beta^3+1) = \beta^{62}.\beta^{32} = \beta^{31} = \beta^5+\beta^2+1$

$\rightarrow (\beta+1).(1+\beta^5+\beta^2).(\beta^5+\beta^3) = \beta^6.\beta^{31}.\beta^{15} = \beta^{52} = \beta^4+\beta^2+1$

$\rightarrow (1+\beta^5+\beta^2).\beta = \beta+1+\beta+\beta^3 = \beta^3+1$

Yukarıda bulduğumuz denklemlere göre matrisimizi bir daha düzenleyelim.

$$M_5 = \begin{bmatrix} \beta & \beta^5+\beta^3 & \beta^2+\beta & \beta^3+1 \\ \beta^3+\beta^2+1 & \beta & \beta^4+\beta^3+\beta & \beta^5+\beta^3+1 \\ \beta^5 & \beta^4+\beta^2 & \beta & \beta^5+\beta^2+1 \\ \beta^5+\beta^2+1 & \beta^4+\beta^2+1 & \beta^3+1 & \beta \end{bmatrix}$$

Şimdi oluşturduğumuz bu matrisin XOR sayısını hesaplayalım.

$\beta.(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0)$

$= b_5\beta^6 + b_4\beta^5 + b_3\beta^4 + b_2\beta^3 + b_1\beta^2 + b_0\beta$

$= b_4\beta^5 + b_3\beta^4 + b_2\beta^3 + b_1\beta^2 + (b_5 + b_0)\beta + b_5$

$= (b_4, b_3, b_2, b_1, b_5 \oplus b_0, b_5)$

Toplam artı sayısı=1

$\beta^5 + \beta^3 = \beta^{15}$ olmak üzere

$\beta^{15}.(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0)$
$= b_5\beta^{20} + b_4\beta^{19} + b_3\beta^{18} + b_2\beta^{17} + b_1\beta^{16} + b_0\beta^{15}$
$= b_5(\beta^5 + \beta^4 + \beta^3 + \beta^2) + b_4(\beta^4 + \beta^3 + \beta^2 + \beta) + b_3(\beta^3 + \beta^2 + \beta + 1)$
$+ b_2(\beta^5 + \beta^2 + \beta) + b_1(\beta^4 + \beta + 1) + b_0(\beta^5 + \beta^3)$
$= \beta^5(b_5 + b_2 + b_0) + \beta^4(b_5 + b_4 + b_1) + \beta^3(b_5 + b_4 + b_3 + b_0)$
$+ \beta^2(b_5 + b_4 + b_3 + b_2) + \beta(b_4 + b_3 + b_2 + b_1) + b_3 + b_1$
$= (b_5 \oplus b_2 \oplus b_0, b_5 \oplus b_4 \oplus b_1, b_5 \oplus b_4 \oplus b_3 \oplus b_0, b_5 \oplus b_4 \oplus b_3 \oplus b_2, b_4 \oplus b_3 \oplus b_2 \oplus b_1, b_3 \oplus b_1)$

Toplam artı sayısı=14

$\beta^2 + \beta = \beta^7$ olmak üzere

$\beta^7.(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0)$

$= b_5\beta^{12} + b_4\beta^{11} + b_3\beta^{10} + b_2\beta^9 + b_1\beta^8 + b_0\beta^7$

$= b_5(\beta^2 + 1) + b_4(\beta^5 + \beta + 1) + b_3(\beta^5 + \beta^4) + b_2(\beta^4 + \beta^3) + b_1(\beta^3 + \beta^2)$

$+ b_0(\beta^2 + \beta) = \beta^5(b_4 + b_3) + \beta^4(b_3 + b_2) + \beta^3(b_2 + b_1) + \beta^2(b_5 + b_1 + b_0)$

$+ \beta(b_4 + b_0) + b_5 + b_4 = (b_4 \oplus b_3, b_3 \oplus b_2, b_2 \oplus b_1, b_5 \oplus b_1 \oplus b_0, b_4 \oplus b_0, b_5 \oplus b_4)$

Toplam artı sayısı=7

$\beta^3 + 1 = \beta^{32}$ olmak üzere

$\beta^{32}.(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0)$

$= b_5\beta^{37} + b_4\beta^{36} + b_3\beta^{35} + b_2\beta^{34} + b_1\beta^{33} + b_0\beta^{32}$

$= b_5(\beta^5 + \beta^3 + \beta^2) + b_4(\beta^4 + \beta^2 + \beta) + b_3(\beta^3 + \beta + 1) + b_2(\beta^5 + \beta^2)$

$+b_1(\beta^4 + \beta) + b_0(\beta^3 + 1)$

$= \beta^5(b_5 + b_2) + \beta^4(b_4 + b_1) + \beta^3(b_5 + b_3 + b_0) + \beta^2(b_5 + b_4 + b_2)$

$+\beta(b_4 + b_3 + b_1) + b_3 + b_0$

$= (b_5 \oplus b_2, b_4 \oplus b_1, b_5 \oplus b_3 \oplus b_0, b_5 \oplus b_4 \oplus b_2, b_4 \oplus b_3 \oplus b_1, b_3 \oplus b_0)$

Toplam artı sayısı=9

$\beta^3 + \beta^2 + 1 = \beta^{48}$ olmak üzere

$\beta^{48}.\left(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0\right)$

$= b_5\beta^{53} + b_4\beta^{52} + b_3\beta^{51} + b_2\beta^{50} + b_1\beta^{49} + b_0\beta^{48}$

$= b_5\left(\beta^5 + \beta^3 + \beta\right) + b_4\left(\beta^4 + \beta^2 + 1\right) + b_3\left(\beta^5 + \beta^3 + \beta + 1\right)$

$+ b_2\left(\beta^5 + \beta^4 + \beta^2\right) + b_1\left(\beta^4 + \beta^3 + \beta\right) + b_0\left(\beta^3 + \beta^2 + 1\right)$

$= \beta^5(b_5 + b_3 + b_2) + \beta^4(b_4 + b_2 + b_1) + \beta^3(b_5 + b_3 + b_1 + b_0)$

$+ \beta^2(b_4 + b_2 + b_0) + \beta(b_5 + b_3 + b_1) + b_4 + b_3 + b_0$

$= (b_5 \oplus b_3 \oplus b_2, b_4 \oplus b_2 \oplus b_1, b_5 \oplus b_3 \oplus b_1 \oplus b_0, b_4 \oplus b_2 \oplus b_0, b_5 \oplus b_3 \oplus b_1, b_4 \oplus b_3 \oplus b_0)$

Toplam artı sayısı=13

$\beta^4 + \beta^3 + \beta = \beta^{49}$ olmak üzere

$\beta^{49}.\left(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0\right)$

$= b_5\beta^{54} + b_4\beta^{53} + b_3\beta^{52} + b_2\beta^{51} + b_1\beta^{50} + b_0\beta^{49}$

$= b_5\left(\beta^4 + \beta^2 + \beta + 1\right) + b_4\left(\beta^5 + \beta^3 + \beta\right) + b_3\left(\beta^4 + \beta^2 + 1\right)$

$+ b_2\left(\beta^5 + \beta^3 + \beta + 1\right) + b_1\left(\beta^5 + \beta^4 + \beta^2\right) + b_0\left(\beta^4 + \beta^3 + \beta\right)$

$= \beta^5(b_4 + b_2 + b_1) + \beta^4(b_5 + b_3 + b_1 + b_0) + \beta^3(b_4 + b_2 + b_0)$

$+ \beta^2(b_5 + b_3 + b_1) + \beta(b_5 + b_4 + b_2 + b_0) + b_5 + b_3 + b_2$

$= (b_4 \oplus b_2 \oplus b_1, b_5 \oplus b_3 \oplus b_1 \oplus b_0, b_4 \oplus b_2 \oplus b_0, b_5 \oplus b_3 \oplus b_1, b_5 \oplus b_4 \oplus b_2 \oplus b_0, b_5 \oplus b_3 \oplus b_2)$

Toplam artı sayısı=14

$\beta^5 + \beta^3 + 1 = \beta^{23}$ olmak üzere

$\beta^{23}.(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0)$

$= b_5\beta^{28} + b_4\beta^{27} + b_3\beta^{26} + b_2\beta^{25} + b_1\beta^{24} + b_0\beta^{23}$

$= b_5(\beta^4 + \beta^3 + \beta^2) + b_4(\beta^3 + \beta^2 + \beta) + b_3(\beta^2 + \beta + 1) + b_2(\beta^5 + \beta)$

$+b_1(\beta^4 + 1) + b_0(\beta^5 + \beta^3 + 1)$

$= \beta^5(b_2 + b_0) + \beta^4(b_5 + b_1) + \beta^3(b_5 + b_4 + b_0) + \beta^2(b_5 + b_4 + b_3)$

$+\beta(b_4 + b_3 + b_2) + b_3 + b_1 + b_0$

$= (b_2 \oplus b_0, b_5 \oplus b_1, b_5 \oplus b_4 \oplus b_0, b_5 \oplus b_4 \oplus b_3, b_4 \oplus b_3 \oplus b_2, b_3 \oplus b_1 \oplus b_0)$

Toplam artı sayısı=10

$\beta^5.\left(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0\right)$

$= b_5\beta^{10} + b_4\beta^9 + b_3\beta^8 + b_2\beta^7 + b_1\beta^6 + b_0\beta^5$

$= b_5(\beta^5 + \beta^4) + b_4(\beta^4 + \beta^3) + b_3(\beta^3 + \beta^2) + b_2(\beta^2 + \beta) + b_1(\beta + 1) + b_0\beta^5$

$= \beta^5(b_5 + b_0) + \beta^4(b_5 + b_4) + \beta^3(b_4 + b_3) + \beta^2(b_3 + b_2) + \beta(b_2 + b_1) + b_2$

$= (b_5 \oplus b_0, b_5 \oplus b_4, b_4 \oplus b_3, b_3 \oplus b_2, b_2 \oplus b_1, b_2)$

Toplam artı sayısı=5

$\beta^4 + \beta^2 = \beta^{14}$ olmak üzere

$\beta^{14}.(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0)$

$= b_5\beta^{19} + b_4\beta^{18} + b_3\beta^{17} + b_2\beta^{16} + b_1\beta^{15} + b_0\beta^{14}$

$= b_5(\beta^4 + \beta^3 + \beta^2 + \beta) + b_4(\beta^3 + \beta^2 + \beta + 1) + b_3(\beta^5 + \beta^2 + \beta)$

$+ b_2(\beta^4 + \beta + 1) + b_1(\beta^5 + \beta^3) + b_0(\beta^4 + \beta^2)$

$= (\beta^4 \oplus \beta^3 \oplus \beta^2 \oplus \beta, \beta^3 \oplus \beta^2 \oplus \beta \oplus 1, \beta^5 \oplus \beta^2 \oplus \beta, \beta^4 \oplus \beta \oplus 1, \beta^5 \oplus \beta^3, \beta^4 \oplus \beta^2)$

Toplam artı sayısı=12

$\beta^5 + \beta^2 + 1 = \beta^{31}$ olmak üzere

$\beta^{31}.(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0)$

$= b_5\beta^{36} + b_4\beta^{35} + b_3\beta^{34} + b_2\beta^{33} + b_1\beta^{32} + b_0\beta^{31}$

$= b_5(\beta^4 + \beta^2 + \beta) + b_4(\beta^3 + \beta + 1) + b_3(\beta^5 + \beta^2) + b_2(\beta^4 + \beta) + b_1(\beta^3 + 1)$

$+b_0(\beta^5 + \beta^2 + 1)$

$= \beta^5(b_3 + b_0) + \beta^4(b_5 + b_2) + \beta^3(b_4 + b_1) + \beta^2(b_5 + b_3 + b_0)$

$+\beta(b_5 + b_4 + b_2) + b_4 + b_1 + b_0$

$= (b_3 \oplus b_0, b_5 \oplus b_2, b_4 \oplus b_1, b_5 \oplus b_3 \oplus b_0, b_5 \oplus b_4 \oplus b_2, b_4 \oplus b_1 \oplus b_0)$

Toplam artı sayısı=9

$\beta^4 + \beta^2 + 1 = \beta^{52}$ olmak üzere

$\beta^{52}.(b_5\beta^5 + b_4\beta^4 + b_3\beta^3 + b_2\beta^2 + b_1\beta + b_0)$

$= b_5\beta^{57} + b_4\beta^{56} + b_3\beta^{55} + b_2\beta^{54} + b_1\beta^{53} + b_0\beta^{52}$

$= b_5(\beta^5 + \beta^4 + \beta^3 + \beta^2 + \beta) + b_4(\beta^4 + \beta^3 + \beta^2 + \beta + 1) + b_3(\beta^5 + \beta^3 + \beta^2 + \beta)$

$+b_2(\beta^4 + \beta^2 + \beta + 1) + b_1(\beta^5 + \beta^3 + \beta) + b_0(\beta^4 + \beta^2 + 1)$

$= \beta^5(b_5 + b_3 + b_1) + \beta^4(b_5 + b_4 + b_2 + b_0) + \beta^3(b_5 + b_4 + b_3 + b_1)$

$+\beta^2(b_5 + b_4 + b_3 + b_2 + b_0) + \beta(b_5 + b_4 + b_3 + b_2 + b_1) + b_4 + b_2 + b_0$

$$= \begin{pmatrix} b_5 \oplus b_3 \oplus b_1, b_5 \oplus b_4 \oplus b_2 \oplus b_0, b_5 \oplus b_4 \oplus b_3 \oplus b_1, b_5 \oplus b_4 \oplus b_3 \oplus b_2 \oplus b_0, \\ b_5 \oplus b_4 \oplus b_3 \oplus b_2 \oplus b_1, b_4 \oplus b_2 \oplus b_0 \end{pmatrix}$$

Toplam artı sayısı=18

Toplam XOR sayısı=133+4.4.6=229

Şimdi matrisin involutif olduğunu gösterelim.

$M_5.M_5 =$

$$\begin{bmatrix} \beta^2 + \beta^{63} + \beta^{12} & \beta^{21} + \beta^{84} & \beta^3 + \beta^2 + \beta^{64} + \beta^8 + \beta^{64} & \beta^4 + \beta + \beta^{33} \\ \beta^{49} + \beta^{49} + \beta^{54} + \beta^{54} & \beta^{63} + \beta^2 + \beta^{75} & \beta^{55} + \beta^{55} & \beta^{80} + \beta^{80} \\ \beta^{62} + \beta^{62} & \beta^{20} + \beta^{83} & \beta^{12} + \beta^{63} + \beta^2 + \beta^{63} & \beta^{37} + \beta^{37} \\ \beta^{100} + \beta^{37} & \beta^{46} + \beta^{46} & \beta^{38} + \beta^{101} & \beta^{75} + \beta^2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$$

Örnek 3.6 $F_{2^4}/x^4 + x + 1$ sonlu cismini ele alalım. ε , $x^4 + x + 1$ in bir kökü olsun.

Tablo 3.11. $F_{2^4}/x^4 + x + 1$ sonu cisminin elemanları

$\varepsilon^4 = \varepsilon + 1$	$\varepsilon^{10} = \varepsilon^2 + \varepsilon + 1$
$\varepsilon^5 = \varepsilon^2 + \varepsilon$	$\varepsilon^{11} = \varepsilon^3 + \varepsilon^2 + \varepsilon$
$\varepsilon^6 = \varepsilon^3 + \varepsilon^2$	$\varepsilon^{12} = \varepsilon^3 + \varepsilon^2 + \varepsilon + 1$

Tablo 3.12. (Devamı) F_{2^4}/x^4+x+1 sonu cisminin elemanları

$\varepsilon^7=\varepsilon^3+\varepsilon+1$	$\varepsilon^{13}=\varepsilon^3+\varepsilon^2+1$
$\varepsilon^8=\varepsilon^2+1$	$\varepsilon^{14}=\varepsilon^3+1$
$\varepsilon^9=\varepsilon^3+\varepsilon$	$\varepsilon^{15}=1$

$M_6=Ghad(a_0,a_1,b_1,a_2,b_2,a_3,b_3)=Ghad(1,\alpha,\alpha^3+\alpha,\alpha+1,\alpha,1,\alpha^2+\alpha)$

$4x4$ involutif MDS matrisi oluşturalım.

$b_1^{-1}.(\alpha^3+\alpha)=1 \Rightarrow b_1^{-1}=\alpha^6$

$b_2^{-1}.\alpha=1 \Rightarrow b_2^{-1}=\alpha^{14}$

$b_3^{-1}.(\alpha^2+\alpha)=1 \Rightarrow b_3^{-1}=\alpha^{10}$ olmak üzere

$$M_6=\begin{bmatrix} a_0 & a_1b_1 & a_2b_2 & a_3b_3 \\ a_1{b_1}^{-1} & a_0 & a_3{b_1}^{-1}b_2 & a_2{b_1}^{-1}b_3 \\ a_2{b_2}^{-1} & a_3{b_2}^{-1}b_1 & a_0 & a_1{b_2}^{-1}b_3 \\ a_3{b_3}^{-1} & a_2{b_3}^{-1}b_1 & a_1{b_3}^{-1}b_2 & a_0 \end{bmatrix}$$

$$=\begin{bmatrix} 1 & \alpha.(\alpha^3+\alpha) & (\alpha+1).\alpha & 1.(\alpha^2+\alpha) \\ \alpha.\alpha^7 & 1 & 1.\alpha^6.\alpha & (\alpha+1).\alpha^6.(\alpha^2+\alpha) \\ (\alpha+1).\alpha^{14} & 1.\alpha^{14}.(\alpha^3+\alpha) & 1 & \alpha.\alpha^{14}.(\alpha^2+\alpha) \\ 1.\alpha^{10} & (\alpha+1).\alpha^{10}.(\alpha^3+\alpha) & \alpha.\alpha^{10}.\alpha & 1 \end{bmatrix}$$

$$=\begin{bmatrix} 1 & \alpha^{10}=\alpha^2+\alpha+1 & \alpha^2+\alpha & \alpha^2+\alpha \\ \alpha^7=\alpha^3+\alpha+1 & 1 & \alpha^7=\alpha^3+\alpha+1 & 1 \\ \alpha^{18}=\alpha^3 & \alpha^{23}=\alpha^8=\alpha^2+1 & 1 & \alpha^{20}=\alpha^5=\alpha^2+\alpha \\ \alpha^{10}=\alpha^2+\alpha+1 & \alpha^{23}=\alpha^8=\alpha^2+1 & \alpha^{12}=\alpha^3+\alpha^2+\alpha & 1 \end{bmatrix}$$

Şimdi oluşturduğumuz matrisin XOR sayısını hesaplayalım.

$(\alpha^2+\alpha+1).(a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0)=\alpha^{10}.(a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0)$

$=a_3\alpha^{13}+a_2\alpha^{12}+a_1\alpha^{11}+a_0\alpha^{10}$

$=a_3(\alpha^3+\alpha^2+1)+a_2(\alpha^3+\alpha^2+\alpha+1)+a_1(\alpha^3+\alpha^2+\alpha)+a_0(\alpha^2+\alpha+1)$

$=\alpha^3(a_3+a_2+a_1)+\alpha^2(a_3+a_2+a_1+a_0)+\alpha(a_2+a_1+a_0)+a_3+a_2+a_0$

$=(a_3\oplus a_2\oplus a_1, a_3\oplus a_2\oplus a_1\oplus a_0, a_2\oplus a_1\oplus a_0, a_3\oplus a_2\oplus a_0)$

Toplam artı sayısı=9

$(\alpha^2+\alpha).(a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0)=\alpha^5.(a_3\alpha^3+a_2\alpha^2+a_1\alpha+a_0)$

$= a_3\alpha^8 + a_2\alpha^7 + a_1\alpha^6 + a_0\alpha^5$

$= a_3(\alpha^2 + 1) + a_2(\alpha^3 + \alpha + 1) + a_1(\alpha^3 + \alpha) + a_0(\alpha^2 + \alpha)$

$= \alpha^3(a_2 + a_1) + \alpha^2(a_3 + a_0) + \alpha(a_2 + a_1 + a_0) + a_3 + a_2$

$= (a_2 \oplus a_1, a_3 \oplus a_0, a_2 \oplus a_1 \oplus a_0, a_3 \oplus a_2)$

Toplam artı sayısı=5

$(\alpha^3 + \alpha + 1).(a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0) = \alpha^7.(a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$

$= a_3\alpha^{10} + a_2\alpha^9 + a_1\alpha^8 + a_0\alpha^7$

$= a_3(\alpha^2 + \alpha + 1) + a_2(\alpha^3 + \alpha) + a_1(\alpha^2 + 1) + a_0(\alpha^3 + \alpha + 1)$

$= \alpha^3(a_2 + a_0) + \alpha^2(a_3 + a_1) + \alpha(a_3 + a_2 + a_0) + a_3 + a_1 + a_0$

$= (a_2 \oplus a_0, a_3 \oplus a_1, a_3 \oplus a_2 \oplus a_0, a_3 \oplus a_1 \oplus a_0)$

Toplam artı sayısı=6

$\alpha^3.(a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0) = a_3\alpha^6 + a_2\alpha^5 + a_1\alpha^4 + a_0\alpha^3$

$= a_3(\alpha^3 + \alpha^2) + a_2(\alpha^2 + \alpha) + a_1(\alpha + 1) + a_0\alpha^3$

$= \alpha^3(a_3 + a_0) + \alpha^2(a_3 + a_2) + \alpha(a_2 + a_1) + a_1$

$= (a_3 \oplus a_0, a_3 \oplus a_2, a_2 \oplus a_1, a_1)$

Toplam artı sayısı=3

$(\alpha^2 + 1).(a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0) = \alpha^8.(a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$

$= a_3\alpha^{11} + a_2\alpha^{10} + a_1\alpha^9 + a_0\alpha^8$

$= a_3(\alpha^3 + \alpha^2 + \alpha) + a_2(\alpha^2 + \alpha + 1) + a_1(\alpha^3 + \alpha) + a_0(\alpha^2 + 1)$

$= \alpha^3(a_3 + a_1) + \alpha^2(a_3 + a_2 + a_0) + \alpha(a_3 + a_2 + a_1) + a_2 + a_0$

$= (a_3 \oplus a_1, a_3 \oplus a_2 \oplus a_0, a_3 \oplus a_2 \oplus a_1, a_2 \oplus a_0)$

Toplam artı sayısı=6

$(\alpha^3 + \alpha^2 + \alpha + 1).(a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0) = \alpha^{12}.(a_3\alpha^3 + a_2\alpha^2 + a_1\alpha + a_0)$

$= a_3\alpha^{15} + a_2\alpha^{14} + a_1\alpha^{13} + a_0\alpha^{12}$

$= a_3.1 + a_2(\alpha^3 + 1) + a_1(\alpha^3 + \alpha^2 + 1) + a_0(\alpha^3 + \alpha^2 + \alpha + 1)$

$= \alpha^3(a_2 + a_1 + a_0) + \alpha^2(a_1 + a_0) + \alpha.a_0 + a_3 + a_2 + a_1 + a_0$

$= (a_2 \oplus a_1 \oplus a_0, a_1 \oplus a_0, a_0, a_3 \oplus a_2 \oplus a_1 \oplus a_0)$

Toplam artı sayısı=6

Toplam XOR sayısı=66+4.4.3=114

4. SONUÇ VE DEĞERLENDİRME

Bu bölümde elde dilen sonuçlar ve yazılan sözde kodlar Magma Programlama Dili kullanılarak elde edilmiştir.

$F_{2^6}[X]/\left(x^6+x^3+1\right)$ için Sözde (pseudo) kod:

- **XOR Sayısı Düşük Olan MDS Matris Bulma Algoritması**

Halka tanımlanır:

```
P < v >:= PolynomialRing(GF(2));
f:= v^6 + v^3 + 1;
R < v >:= qou < P|f >;
```

Halkanın elemanları tanımlanır:

```
Elemanlar := [[0]];
for α in R do
  if α ne 0 then
     Append(~Elemanlar,α);
  end if;
end for;
```

Terslenebilir elemanların tersleri tanımlanır:

```
function FindElementsInverse()
element_inv := [0];
elements := [0];
for u in R do
  if IsInverstible(u) then
    inverse := u^-1;
    Append(~elements,u);
    Append(~element_inv,inverse);
  end if;
end for;
return element_inv;
return elements
```

$end\ function;$

R'deki elemanlarla MDS matris oluşturulur:

$function\ Find\_ai()$

$for\ i\ in\ [1..4]\ do$

$a_i := [\ ];$

$for\ ai\ in\ R\ do$

$sonuc := (a0)^2 + (a1)^2 + (a2)^2 + (a3)^2;$

$if\ sonuc\ eq\ 1\ then$

$Append(\sim a_i, ai);$

$end\ if;$

$end\ for;$

$end\ for;$

$return\ a_i;$

$end\ function;$

$xy1 := x1 * y1;$

$xy2 := x2 * y2;$

$xy3 := x3 * y3;$

$xy11 := x1 * (y1)^{-1};$

$x3y12 := x3 * (y1)^{-1} * y2;$

$x2y13 := x2 * (y1)^{-1} * y3;$

$x2y21 := x2 * (y2)^{-1};$

$x3y211 := x3 * (y2)^{-1} * y1;$

$x1y213 := x1 * (y2)^{-1} * y3;$

$x3y31 := x3 * (y3)^{-1};$

$x3y311 := x3 * (y3)^{-1} * y1;$

$x1y312 := x1 * (y3)^{-1} * y2;$

$A := Matrix(R, 4, 4, [[x0, xy1, xy2, xy3], [xy11, x0, x3y12, x2y13],$

$[x2y21, x3y211, x0, x1y213], [x3y31, x3y311, x1y312, x0]];$

Matrisin XOR sayısı hesaplanır:

$R < a, b, c, d, e, f >:= PolynomialRing(R, 6);$

$f := a * v^5 + b * v^4 + c * v^3 + d * v^2 + e * v + f;$

$S1 := [[\ ]];$

$for\ i\ in\ [1..4]\ do$

```
  for j in [1..4] do
    result := A[i][j] * f;
    Append(~S1,result);
  end for;
end for;
```

XOR sayısı en düşük olan MDS matrisler

$$\begin{bmatrix} v & v^5+v^4+v^2+v+1 & v^4+v^2 & v^5+v^4+v^3+v^2+v+1 \\ v^5+v^4+v^3+v+1 & v & v^5+v^4+v^3+v^2+v+1 & v^2+1 \\ v^4+v^3+v^2+v+1 & v^5+v^2 & v & v^5+v^4+v^3+v+1 \\ v^5+v^2 & 1 & v^5+v^4+v^2+v+1 & v \end{bmatrix}$$

XOR sayısı: 154

$$\begin{bmatrix} 1 & v^5+v^3 & v^5 & v^5+v^4+v^3+v \\ v^4+v^3+v+1 & 1 & v^5+v^2+v+1 & v^5+v^3+1 \\ v^3+v^2+1 & v^4 & 1 & v^4+v \\ v^4+v^3 & v^5+v^4+v^3 & v^5+v^4+v^3+v^2 & 1 \end{bmatrix}$$

XOR sayısı: 140

$F_{2^7}[X]/\left(x^7+x^3+1\right)$ için Sözde (pseudo) kod:

- **XOR Sayısı Düşük Olan MDS Matris Bulma Algoritması**

Halka tanımlanır:

```
P < v >:= PolynomialRing(GF(2));
f:= v^7 + v^3 + 1;
R < v >:= qou < P|f >;
```

Halkanın elemanları tanımlanır:

```
Elemanlar := [[0]];
for α in R do
  if α ne 0 then
     Append(~Elemanlar,α);
  end if;
end for;
```

Terslenebilir elemanların tersleri tanımlanır:

```
function FindElementsInverse()
element_inv := [0];
elements := [0];
for u in R do
  if IsInverstible(u) then
    inverse := u^-1;
    Append(~elements,u);
    Append(~element_inv,inverse);
  end if;
end for;
return element_inv;
return elements
end function;
```

R'deki elemanlarla MDS matris oluşturulur:

```
function Find_ai()
for i in [1..4] do
  a_i := [ ];
  for ai in R do
    sonuc := (a0)^2 + (a1)^2 + (a2)^2 + (a3)^2;
    if sonuc eq 1 then
      Append(~a_i,ai);
    end if;
  end for;
end for;
return a_i;
end function;
xy1 := x1 * y1;
xy2 := x2 * y2;
xy3 := x3 * y3;
xy11 := x1 * (y1)^-1;
x3y12 := x3 * (y1)^-1 * y2;
x2y13 := x2 * (y1)^-1 * y3;
x2y21 := x2 * (y2)^-1;
```

$x3y211 := x3 * (y2)^{-1} * y1;$

$x1y213 := x1 * (y2)^{-1} * y3;$

$x3y31 := x3 * (y3)^{-1};$

$x3y311 := x3 * (y3)^{-1} * y1;$

$x1y312 := x1 * (y3)^{-1} * y2;$

$A := Matrix(R, 4, 4, [[x0, xy1, xy2, xy3], [xy11, x0, x3y12, x2y13],$

$[x2y21, x3y211, x0, x1y213], [x3y31, x3y311, x1y312, x0]];$

Matrisin XOR sayısı hesaplanır:

$R < a, b, c, d, e, f, g >:= PolynomialRing(R, 7);$

$f := a * v^6 + b * v^5 + c * v^4 + d * v^3 + e * v^2 + f * v + g;$

$S1 := [[\ ]];$

$for\ i\ in\ [1..4]\ do$

  $for\ j\ in\ [1..4]\ do$

    $result := A[i][j] * f;$

    $Append(\sim S1, result);$

  $end\ for;$

$end\ for;$

XOR sayısı en düşük olan MDS matrisler

$$\begin{bmatrix} v & v^6+v^4+1 & v^4+v^2+v+1 & v^6+v^3+v^2+v \\ v^6+v^2+1 & v & v^6+v^5+v^3+v^2+v & v^4+1 \\ v^6+v & v^6+v^3+1 & v & v^6+v^3+v+1 \\ v^5+v^3+v^2 & v^5+v^4+v^2 & v^6+v^5+v^3+v^2+1 & v \end{bmatrix}$$

XOR sayısı: 206

$$\begin{bmatrix} 1 & v^5+v^3+v^2 & v^5+v^4+v+1 & v^6+v \\ v^6+v^5+v^4+1 & 1 & v^5+v^2+v & v^6+v^5+v^3+v \\ v^6+v^4+v^2+v & v^6+v^5+v^4+v^2+v+1 & 1 & v^3+v+1 \\ v^5+v^4+v & v^5+v^4+v^2+v+1 & v^6+v^4+v^3+v^2+v+1 & 1 \end{bmatrix}$$

XOR sayısı: 205

KAYNAKLAR

[1] Aslan B., Blok Şifreler İçin Cebirsel İkili Doğrusal Dönüşüm Tasarımı ve Modern Bir Blok Şifreye Uygulanması, Doktora Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne, 2013, 307650.

[2] Sakallı, M. T., Akleylek, S., Akkanat, K., Rıjmen, V. On The Automorphisms And İsomorphisms Of MDS Matrices And Their Efficient İmplementations, in Turkish Journal of Electrical Engineering and Computer Sciences: Vol. 28: No. 1, Article 20, 2020.

[3] Smart, N. P., Cryptography Made Simple, Springer International Publishing, Switzerland, 2016.

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

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

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

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

[10] Taşcı, D., Lineer Cebir. Selçuk Üniversitesi Vakfı Yayınları, Konya, 2001.

[11] Horn, R.A., Johnson, C.R.,. Matrix Analysis. Cambridge University Press, Cambridge, 1990.

[12] Venit, S., Bishop, W., Elementary linear algebra, PWS publishers, Massachusetts, 1985.

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

[14] Çetin, N., Orhun, N., Lineer Cebir, Anadolu Üniversitesi Yayınları No:1074, Açıköğretim Fakültesi Yayınları No:589, 1998.

[15] Uslu A., Dairesel Matrisler Ve Uygulaması, Yüksek Lisans Tezi, Sakarya Üniversitesi, Fen Bilimleri Enstitüsü, Sakarya, 2008, T03787.

[16] Wan, Z. C, Fınıte Fields And Galois Rings, World Scientific Publishing, 2003.

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

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

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

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

[21] 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.

[22] https://tr.wikipedia.org/wiki/Kriptografi internet sitesinden alındı. Erişim tarihi: 11.11.2023

[23] Daemen J, Rijmen V. The Design of Rijndael, AES - The Advanced Encryption Standard. Berlin, Germany: Springer-Verlag, 2002.

[24] Barreto PSLM, Rijmen V. Whirlpool. In: van Tilborg HCA, Jajodia S. (editors). Encyclopedia of Cryptography and Security. 2nd ed. Boston, MA, USA: Springer, 2011, pp. 1384-1385.

[25] Guo J, Peyrin T, Poschmann A. The PHOTON family of lightweight hash functions. In: Proceedings of CRYPTO; Santa Barbara, CA, USA; 2011. pp. 222-239.

[26] Barreto PSLM, Nikov V, Nikova S, Rijmen V, Tischhauser E. Whirlwind: A new cryptographic hash function. Design, Codes and Cryptography 2010; 56: 141–162. doi: 10.1007/s10623-010-9391-y

[27] Sakallı M. T., Akleylek S, Akkanat K and Rıjmen V (2020) "On the automorphisms and isomorphisms of MDS matrices and their efficient implementations," Turkish Journal of Electrical Engineering and Computer Sciences: Vol. 28: No. 1, Article 20. https://doi.org/ 10.3906/elk-1906-151

[28] Otal K., "A Generalization of the Subfield Construction", IJISS, vol. 11, no. 2, pp. 1–11, 2022.

[29] Youssef AM, Mister S, Tavares SE. On the design of linear transformation for substitution permutation encryption networks. In: Proceedings of SAC; Ottowa, Canada; 1997. pp. 40-48.

[30] Gupta KC, Ray IG. On constructions of circulant MDS matrices for lightweight cryptography. In: Proceedings of ISPEC; Fuzhou, China; 2014. pp. 564-576.

[31] Lacan J, Fimes J. Systematic MDS erasure codes based on Vandermonde matrices. IEEE Transactions on Communications Letters 2004; 8 (9): 570-572. doi: 10.1109/LCOMM.2004.833807

[32] Sajadieh M, Dakhilalian M, Mala H, Omoomi B. On construction of involutory MDS matrices from Vandermonde matrices in GF(2q) . Design, Codes and Cryptography 2012; 64 (3): 287-308. doi: 10.1007/s10623-011-9578-x

[33] Augot D, Finiasz M. Direct construction of recursive MDS diffusion layers using shortened BCH codes. In: Proceedings of FSE; London, UK; 2014. pp. 3-17.

[34] Berger TP. Construction of recursive MDS diffusion layers from Gabidulin codes. In: Proceedings of INDOCRYPT; Mumbai, India; 2013. pp. 274-285.

[35] Cauchois V, Loidreau P, Merkiche N. Direct construction of quasi-involutory recursive-like MDS matrices from 2- cyclic codes. IACR Transactions on Symmetric Cryptology 2016; 2016 (2): 80-98. doi: 10.13154/tosc.v2016.i2.80-98

[36] Sajadieh M, Dakhilalian M, Mala H, Sepehrdad P. Recursive diffusion layers for block ciphers and hash functions. In: Proceedings of FSE; Washington, DC, USA; 2012. pp. 385-401.

[37] Wu S, Wang M, Wu W. Recursive diffusion layers for (lightweight) block ciphers and hash functions. In: Proceedings of SAC; Windsor, Canada; 2012. pp. 355-371.

[38] Sim SM, Khoo K, Oggier F, Peyrin T. Lightweight MDS involution matrices. In: Proceedings of FSE; İstanbul, Turkey; 2015. pp. 471-493.

[39] Li Y, Wang M. On the construction of lightweight circulant involutory MDS matrices. In: Proceedings of FSE; Bochum, Germany; 2016. pp. 121-139.

[40] Liu M, Siu SM. Lightweight MDS generalized circulant matrices. In: Proceedings of FSE; Bochum, Germany; 2016. pp. 101-120.

[41] MacWilliams FJ, Sloane NJA. The Theory of Error Correcting Codes. Amsterdam, the Netherlands: North Holland, 1986.

[42] Büyüksaraçoğlu Sakallı F., Aydın Ö., Tuncay G., Pehlivanoğlu M. K., Güzel G. G., and Sakallı M. T., "On Lightweight 4x4 MDS Matrices over Binary Field Extensions", IJISS, vol. 9, no. 2, pp. 94–103, 2020.

[43] Sim, S.M., Khoo, K., Oggier, F., Peyrin, T. (2015). Lightweight MDS Involution Matrices. In: Leander, G. (eds) Fast Software Encryption. FSE 2015. Lecture Notes in Computer Science(), vol 9054. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-662-48116-5_23

[44] Chand Gupta, K., Ghosh Ray, I.: On constructions of involutory MDS matrices. In: Youssef, A., Nitaj, A., Hassanien, A.E. (eds.) AFRICACRYPT 2013. LNCS, vol. 7918, pp. 43–60. Springer, Heidelberg (2013)

[45] Güzel G. G, Sakallı M. T, Akleylek S, Rijmen V and Çengellenmiş Y., "A New Matrix Form to Generate All 3×3 Involutory MDS Matrices over F_{2^m}". Inf.Process.Lett. 147: 61-68 (2019)

[46] Sarkar, S., Syed, H. (2017). Analysis of Toeplitz MDS Matrices. In: Pieprzyk, J., Suriadi, S. (eds) Information Security and Privacy. ACISP 2017. Lecture Notes in Computer Science(), vol 10343. Springer, Cham. https://doi.org/10.1007/978-3-319-59870-3_1

[47] K. C. Gupta, S. K. Pandey, I. G. Ray and S. Samanta. Cryptographically significant mds matrices over finite fields: A brief survey and some generalized results. Advances in Mathematics of Communications, 2019, 13(4): 779-843. doi: 10.3934/amc.2019045

[48] Kurt Pehlivanoğlu,M. Maksimum Uzaklıkta Ayrılabilen Matrislerin Elde Edilebilmesi İçin Yeni Bir Matris Formu ve Bir Hafif Sıklet Blok Şifreye Uygulanması, Doktora Tezi, Kocaeli Üniversitesi, Fen Bilimleri Enstitüsü, Edirne, 2018, 519410

[49] Akkanat K., MDS Yayılım Matrislerinde İzomorfizmalar Üzerine Yeni Bir Çalışma, Yüksek Lisans Tezi, Trakya Üniversitesi, Fen Bilimleri Enstitüsü, Edirne, 2017, 495069.

ÖZGEÇMİŞ

Ad-Soyad : Tuğçe TUFANÇLI

ÖĞRENİM DURUMU:

- **Lisans** **:** 2012, Ege Üniversitesi, Fen Fakültesi, Matematik Bölümü
- **Yükseklisans** **:** Devam ediyor, Sakarya Üniversitesi, Matematik, Cebir ve Sayılar Teorisi

MESLEKİ DENEYİM VE ÖDÜLLER:

- 2013 yılından itibaren Milli Eğitim Bakanlığı'nda öğretmen olarak çalışmaya devam etmektedir.