T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KRİPTOGRAFİK VE UYGULAMA ÖZELLİKLERİ İYİ OLAN İKİLİ MATRİSLERİN ÜRETİLMESİ İÇİN YENİ BİR ARAMA YÖNTEMİ

GÖKHAN TUNCAY

YÜKSEK LİSANS TEZİ

HESAPLAMALI BİLİMLER ANABİLİM DALI

Tez Danışmanı: Doç. Dr. M. Tolga SAKALLI

EDİRNE-2015

T.Ü. Fen Bilimleri Enstitüsü onayı

Prof. Dr. Mustafa ÖZCAN
Fen Bilimleri Enstitüsü Müdürü

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

Prof. Dr. Metin AYDOĞDU
Anabilim Dalı Başkanı

Bu tez tarafımca okunmuş, kapsamı ve niteliği açısından bir Yüksek Lisans tezi olarak kabul edilmiştir.

Doç. Dr. M. Tolga SAKALLI
Tez Danışmanı

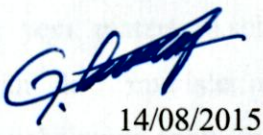
Bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Hesaplamalı Bilimler Anabilim Dalında bir Yüksek Lisans tezi olarak oy birliği ile kabul edilmiştir.

Jüri Üyeleri	İmza
Doç. Dr. M. Tolga SAKALLI	
Yrd. Doç. Dr. Andaç ŞAHİN MESUT	
Yrd. Doç. Dr. Sedat AKLEYLEK	

Tarih: 14/08/2015

T.Ü. FEN BİLİMLERİ ENSTİTÜSÜ
HESAPLAMALI BİLİMLER YÜKSEK LİSANS PROGRAMI
DOĞRULUK BEYANI

İlgili tezin akademik ve etik kurallara uygun olarak yazıldığını ve kullanılan tüm literatür bilgilerinin kaynak gösterilerek ilgili tezde yer aldığını beyan ederim.



14/08/2015
Gökhan TUNCAY

Yüksek Lisans Tezi

Kriptografik ve Uygulama Özellikleri İyi Olan İkili Matrislerin Üretilmesi İçin Yeni Bir Arama Yöntemi

T.Ü. Fen Bilimleri Enstitüsü

Hesaplamalı Bilimler Anabilim Dalı

ÖZET

Bu tezde, kriptografik ve uygulama özellikleri iyi olan ikili matrislerin üretilmesi için yeni bir arama yöntemi önerilmektedir. Buna ek olarak 6×6, 8×8, 12×12, 16×16 ve 32×32 boyutlarındaki maksimum dallanma sayısına sahip ikili matrislere odaklanılmaktadır. Düşük arama karmaşıklığına sahip ve bazı yeni matematiksel fikirlere dayanan bu arama yöntemi, blok şifrelerde kullanılan ikili matrislerin üretilmesine ve kodlama teorisi alanında önemli bir konu olan maksimum uzaklığa sahip ikili [*2n, n*] kodların elde edilmesine dair yeni çözümler getirmektedir.

Çalışma altı bölüme ayrılmıştır. İlk bölümde, kriptografi bilimine kısa bir giriş yapılmıştır. İkinci bölümde, çalışmanın anlaşılabilmesi için gerekli olan matematik alt yapı verilmiştir. Üçüncü bölümde, kriptografik ve uygulama özellikleri iyi olan ikili matrislerin üretilmesi için geliştirilen yeni bir yöntem tanıtılmaktadır. Dördüncü ve beşinci bölüm, sırasıyla 3×3 ve 4×4 boyutlarındaki devirli matris grupları kullanılarak elde edilen ikili matrislerin örneklerle açıklanmasına ayrılmıştır. Altıncı bölümde ise çalışmada elde edilen sonuçlar verilmektedir.

Yıl : 2015

Sayfa Sayısı : 78

Anahtar Kelimeler : Blok şifreler, ikili matrisler, dallanma sayısı, sabit nokta sayısı, yayılım katmanı, genişletilmiş ikili Golay kodlar

Master's Thesis
A New Search Method to Generate Cryptographically Good Binary Matrices with Good Implementation Properties
Trakya University Institute of Natural Sciences
Computational Sciences

ABSTRACT

In this thesis, a new search method to generate cryptographically good binary matrices with good implementation properties is proposed. In addition, the binary matrices with the sizes 6×6, 8×8, 12×12, 16×16 and 32×32 having maximum branch numbers are focused. The search method based on some novel mathematical ideas with low search complexity has significant properties since it gives new solutions to generate binary matrices to be used in block ciphers and generating binary [*2n, n*] codes with maximum distance is an important subject in the field of coding theory.

The study is composed of six sections. In the first section, there is a brief introduction to the science of cryptography. In the second section, the mathematical background needed for the study is given. In the third section, a new method for constructing cryptographically good binary matrices with good implementation properties is presented. The fourth and fifth sections are reserved to exemplifying binary matrices obtained by using 3×3 and 4×4 cyclic matrix groups, respectively. In the sixth section, there is a list of results obtained by the study.

Year : 2015
Number of Pages : 78
Keywords : Block ciphers, binary matrices, branch number, number of fixed points, diffusion layer, extended binary Golay codes

TEŞEKKÜRLER

Tüm akademik yaşamım boyunca bilgisi, tecrübesi ve dostluğuyla bana daima destek olan danışmanım Sayın Doç. Dr. Tolga SAKALLI'ya,

Çalışmaya yaptığı bilimsel katkıları için, Sayın Yrd. Doç Dr. Sedat AKLEYLEK'e,

Deneysel sonuçların elde edilmesi aşamasında sağladığı destek için, Sayın Arş. Gör. Emir ÖZTÜRK'e,

Çalışmamın her aşamasında yardımlarını esirgemeyen bölüm hocalarıma ve arkadaşlarıma,

Bugünlere gelmemi sağlayan ve hep yanımda olan aileme,

Yol arkadaşım Telay'a,

Sonsuz teşekkürler…

İÇİNDEKİLER

ÖZET i
ABSTRACT ii
TEŞEKKÜRLER iii
İÇİNDEKİLER iv
SEMBOLLER ve KISALTMALAR vii
ŞEKİLLER DİZİNİ viii
TABLOLAR DİZİNİ ix
BÖLÜM 1 1
GİRİŞ 1
1.1. Kriptoloji 1
1.2. Kriptoloji Tarihi 3
1.3. Modern Kriptoloji 4
1.4. Blok Şifreler 5
1.5. Blok Şifrelerin Parametreleri 6
1.5.1. Anahtar Uzunluğu 6
1.5.2. S-Kutuları (Substitution-Boxes) 6
1.5.3. Doğrusal Dönüşümler 7
1.5.4. Anahtar Genişletme Rutini 8
1.6. Tezin Gerekçesi ve Önemi 8
BÖLÜM 2 10

MATEMATİK ALTYAPI 10

BÖLÜM 3 19

ÖNERİLEN YÖNTEM 19

3.1. İndirgenemez Polinomlar Yardımıyla Cebirsel Yöntem 19

3.2. Yöntemin Altyapısı 23

3.3. Yöntemin Algoritması 25

BÖLÜM 4 26

3×3 BOYUTUNDA DEVİRLİ MATRİS GRUPLARI 26

4.1. 3×3 Boyutundaki Devirli Matris Grupları ile 6×6 Boyutunda İkili Matrislerin Elde Edilmesi 27

4.2. 3×3 Boyutundaki Devirli Matris Grupları ile 12×12 Boyutunda İkili Matrislerin Elde Edilmesi 34

BÖLÜM 5 39

4×4 BOYUTUNDA DEVİRLİ MATRİS GRUPLARI 39

5.1. Elemanları $\mathbb{F}_{2^4}$'ten Olan 2×2 Boyutundaki Hadamard Matrisler ve 4×4 Boyutundaki Devirli Matris Grupları ile 8×8 Boyutunda İkili Matrislerin Elde Edilmesi 42

5.2. Elemanları $\mathbb{F}_{2^4}$'ten Olan 4×4 Boyutundaki Hadamard Matrisler ve 4×4 Boyutundaki Devirli Matris Grupları ile 16×16 Boyutunda İkili Matrislerin Elde Edilmesi 47

5.3. Elemanları $\mathbb{F}_{2^4}$'ten Olan 4×4 Boyutundaki Dairesel Matrisler ve 4×4 Boyutundaki Devirli Matris Grupları ile 16×16 Boyutunda İkili Matrislerin Elde Edilmesi 50

5.4. Elemanları $\mathbb{F}_{2^4}$'ten Olan 8×8 Boyutundaki Hadamard Matrisler ve 4×4 Boyutundaki Devirli Matris Grupları ile 32×32 Boyutunda İkili Matrislerin Elde Edilmesi 52

BÖLÜM 6 55

SONUÇ ve TARTIŞMA 55

EK – A 58

8×8 BOYUTUNDA İKİLİ MATRİSLER 58

EK – B 64

16×16 BOYUTUNDAKİ İKİLİ MATRİSLER İÇİN DENKLİK SINIFLARI 64

EK – C 70

16×16 BOYUTUNDA İKİLİ MATRİSİN 8 – BİT PLATFORMDA UYGULANMASINA DAİR BİR ÖRNEK 70

KAYNAKLAR 73

ÖZGEÇMİŞ 77

TEZ ÇALIŞMASI SIRASINDA GERÇEKLEŞTİRİLEN BİLİMSEL FAALİYETLER 78

SEMBOLLER ve KISALTMALAR

AES **:** Advanced Encryption Standard

DEA **:** Data Encryption Algorithm

S-Box **:** Yer Değiştirme Kutuları (Substitution Box)

FPN **:** Sabit Nokta Sayısı (Number of Fixed Points)

BN **:** Dallanma Sayısı (Branch Number)

MDBL **:** Maximum Distance Binary Linear

MDS **:** Maximum Distance Separable

SPN **:** Substitution-Permutation Network

XOR **:** Exclusive Or

$\mathbb{F}_2$ **:** Elemanları 0 veya 1 olan cisim

$\mathbb{F}_{2^n}$ **:** Elemanları 0 veya 1 olan *n* elemanlı vektörleri temsil eden cisim

$\{0,1\}^n$ **:** Elemanları 0 veya 1 olan *n*-bit vektör

wt() **:** Hamming Ağırlığı

had() **:** Hadamard Matris

circ() **:** Circulant (Dairesel) Matris

ŞEKİLLER DİZİNİ

Şekil 1.1. Simetrik Şifreleme Sistemleri 4
Şekil 1.2. Asimetrik Şifreleme Sistemleri 5

TABLOLAR DİZİNİ

Tablo 2.1. İkili [*2n, n*] Doğrusal Kodların Maksimum Uzaklıkları 14
Tablo 3.1. İndirgenemez Polinom $x^3 + x + 1$ ile Tanımlı $\mathbb{F}_{2^3}$ cisminin Elemanlarının x Sonlu Cisim Elemanı ile Çarpımı Sonucu Üretilen 3×3 Boyutunda İkili Doğrusal Dönüşümler 21
Tablo 3.2. İndirgenemez Polinom $x^4 + x + 1$ ile Tanımlı $\mathbb{F}_{2^4}$ cisminin Elemanlarının x Sonlu Cisim Elemanı ile Çarpımı Sonucu Üretilen 4×4 Boyutunda İkili Doğrusal Dönüşümler 22
Tablo 4.1. 3×3 Boyutunda Devirli Matris Grupları 26
Tablo 4.2. Grup Elemanlarının İkilik ve Onaltılık Notasyonda Gösterimi 27
Tablo 4.3. 001-011-111 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 28
Tablo 4.4. 001-100-110 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 29
Tablo 4.5. 001-110-011 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 31
Tablo 4.6. 010-101-100 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 32
Tablo 4.7. 010-111-011 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 33
Tablo 4.8. 001-011-111 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 35
Tablo 4.9. 010-111-011 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 37
Tablo 5.1. 4×4 Boyutunda Devirli Matris Grupları 40
Tablo 5.2. Grup Elemanlarının İkilik ve Onaltılık Notasyonda Gösterimi 41
Tablo 5.3. 0100-1001-0110-0011 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 42
Tablo 5.4. 1100-1101-0100-0010 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 45
Tablo 5.5. 0001-0110-0101-1011 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 48
Tablo 5.6. 0001-0011-0110-1101 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu 52
Tablo 6.1. Önerilen Yöntem ile Elde Edilen Deneysel Sonuçlar 55

Tablo 6.2. M_{10} Matrisi ile ARIA'da kullanılan 16×16 İkili Matrislerin Karşılaştırılması 56
Tablo 6.3. M_{12} Matrisi ile Literatürdeki Bazı 32×32 İkili Matrislerin Karşılaştırılması 57
Tablo A.1. 4×4 Boyutundaki Üreteç Matrisler 58
Tablo A.2. 1. Grupta Bulunan Üreteç Matrisler Kullanılarak Elde Edilen Maksimum Dallanma Sayısına Sahip 8×8 Boyutundaki İkili Matrisler 60
Tablo A.3. 2. Grupta Bulunan Üreteç Matrisler Kullanılarak Elde Edilen Maksimum Dallanma Sayısına Sahip 8×8 Boyutundaki İkili Matrisler 60
Tablo A.4. 3. Grupta Bulunan Üreteç Matrisler Kullanılarak Elde Edilen Maksimum Dallanma Sayısına Sahip 8×8 Boyutundaki İkili Matrisler 61
Tablo B.1. Maksimum Dallanma Sayısına Sahip 16×16 Boyutundaki İkili Matrisler İçin Denklik Sınıfları.....66

BÖLÜM 1

GİRİŞ

Bilgi, insanlık için her zaman değerli bir olgu olmuştur. Özellikle yazının keşfedilmesi ile saklanabilir ve iletilebilir hale gelen bilgi, tarih boyunca savaşları kazanmak, gelir elde etmek ve medeniyetlerin gelişimini şekillendirmek için kullanılan bir araç haline gelmiştir. Uygarlıkların ilerleme sürecinde de rekabetin ve çekişmelerin artması, bilginin iletilmesi esnasında gizlenmesinin kaçınılmaz bir gereklilik olduğunu göstermiştir. Bu gereklilik kriptoloji biliminin doğmasına sebep olmuş, bilginin güvenliği ve gizliliğine dair hassasiyetlerin artması da gelişmesine uygun zemini hazırlamıştır.

Bilgisayarların gündelik hayatın bir parçası olmaya başladığı 1970'lerden günümüze kadar uzanan zaman diliminde ise iletişim teknolojilerindeki gelişmelerle birlikte bilginin değeri gitgide artmaktadır. Bu durum da, bilginin saklanması ve iletilmesi sırasında; yetkisiz olarak değiştirilmesine, ifşa edilmesine, izinsiz incelenmesine, kaydedilmesine ve hasar verilmesine karşı sürekli yeni koruma yöntemlerinin geliştirilmesini zorunlu kılmaktadır.

1.1. Kriptoloji

Kriptoloji, Türk Dil Kurumu tarafından, "Gizli yazılar, şifreli belgeler bilimi veya incelenmesi" şeklinde tanımlanmaktadır. Kriptografi ve kriptanaliz adı verilen iki alt bilim dalının birleşmesinden oluşmaktadır.

Kriptografi bilimi, iletişim halinde olan iki veya daha fazla tarafın bilgi alışverişini güvenli olarak yapmasını sağlayan, matematiksel teknik ve uygulamalar

bütünü olarak tanımlanabilir. Bu teknik ve uygulamalar temelde, okunabilir bir metnin istenmeyen kişiler tarafından okunamayacak bir hale dönüştürülmesi sağlar.

Bir kriptografik sistem aşağıdaki bileşenlerden oluşmaktadır [1];

- Alfabetik karakterden oluşan bir açık metin uzayı,
- Şifrelenmiş karakterlerden oluşan bir şifreli metin uzayı,
- Olası şifreleme anahtarları kümesinden oluşan bir şifreleme anahtar uzayı,
- Olası şifre çözme anahtarları kümesinden oluşan bir şifre çözme anahtar uzayı,
- Etkin bir şifreleme algoritması,
- Etkin bir şifre çözme algoritması,

Kriptanaliz ise kriptografik sistemlerin kırılması ile ilgilenen bilim dalıdır. Kriptografik sistemlerin kurduğu mekanizmaları inceler ve çözümünü araştırır. Diğer bir deyişle; şifreli metinlerden çeşitli yöntemler kullanılarak okunabilir metnin veya anahtarın elde edilmesi işlemidir. Kriptografik sistemlerin zayıflıklarını anlamak ve zaaflarını ortaya çıkarmak açısından oldukça önemlidir. Yaygın olarak kullanılan kriptanaliz saldırı modelleri aşağıda belirtilmiştir [2].

- ***Sadece Şifreli metin Saldırısı (Ciphertext-only):*** Sadece şifreli metin saldırısında, saldırgan sadece bazı şifreli metinlere erişime sahiptir. Bu şifreli metinle ilişkili anahtarı ve açık metni elde etmeye çalışır.
- ***Bilinen Açık Metin Saldırısı (Known-Plaintext Attack):*** Bilinen açık metin saldırısında saldırgan, bazı açık metin ve bunların şifreli metin çiftlerinin erişimine sahiptir.
- ***Seçilmiş Açık Metin Saldırısı (Chosen-Plaintext Attack):*** Seçilmiş açık metin saldırısı, bilinen açık metin saldırısına benzerdir. Fakat açık metin ve şifreli metin çiftleri saldırgan tarafından seçilmiştir.
- ***Seçilmiş Şifreli Metin Saldırısı (Chosen-Ciphertext Attack):*** Saldırgan bir şifreli metin dizisi seçebilir ve bunların açık metinlerini oluşturabilir.

1.2. Kriptoloji Tarihi

Bilinen ilk kriptografik belge MÖ 1900 yıllarında yazıldığı tahmin edilen bir Mısır hiyeroglifidir. İlk askeri amaçlı kullanımın ise Yunanlılar tarafından MÖ 5. yüzyılın başlarında Skytale adını verdikleri bir şifreleme cihazı ile olduğu bilinmektedir. Bu cihaz aynı zamanda bilinen ilk kriptografik cihazdır. Skytale kullanarak bir mesajı şifrelemek için öncelikle uzun bir parşömen ya da papirüs, silindirik bir sopa etrafına sarıldıktan sonra, gizlenecek mesaj uzunlamasına papirüs sarılı sopa üzerine her bir şerit turunda bir harf gelecek şekilde yazılmaktadır. Şerit açılıp kaldırıldıktan sonra anlamsız harflerin oluşturduğu şifreli metin ortaya çıkmaktadır. Şifre çözme işlemi için ise, şifrelemede kullanılan sopa ile aynı çapta ve uzunlukta bir sopaya sahip olmak gerekmektedir. MÖ 60-50 yılları arasında ise Roma imparatoru Julius Ceasar, komutanları ile haberleşmek için, bugün Sezar şifresi olarak bilinen monoalfabetik yer değiştirme şifresini kullanmıştır. Sezar şifresi, düz metinde bulunan her harfin, normal alfabede kendisinden sonra üçüncü olarak gelen harf ile yer değiştirmesi ile oluşturulmuştur. İlerleyen yüzyıllarda buna benzer pek çok monoalfabetik yer değiştirme şifresi kullanılmıştır. Fakat MS 9. yüzyılda keşfedilen Frekans analizi yöntemiyle, Sezar şifresi gibi monoalfabetik yer değiştirme şifrelerinin çok kolayca kırılabileceği anlaşılmıştır. Kriptanalistlerin bu başarısı, kriptografları yeni yöntem arayışlarına yöneltmiştir. 1518 yılında, Johannes Trithemius adında bir Alman, "Polygraphiae" adlı kitabında ilk kez polialfabetik yer değiştirme şifrelerinden bahsetmiştir. 1586'da Blaise de Vigenere, kendi adıyla bilinen Vigenere şifresini tasarlamıştır. Bu şifrede düz metindeki her harf, ayrı bir şifre alfabesiyle şifrelenmektedir. Hangi alfabenin seçileceğine anahtar sözcüğe bakılarak karar verilmiştir. Böylece düz metindeki aynı kelimeler için farklı şifrelenmiş metinler oluşmaktadır. Bu da frekans analizinin tek başına uygulanmasına engel olmaktadır. Uzun yıllar güvenliğini koruyan bu şifre, 1854-1863 yılları arasında İngiliz matematikçi Charles Babbage ve Avusturyalı kriptanalist Friedrich Kasiski tarafından kırılmıştır [3,4].

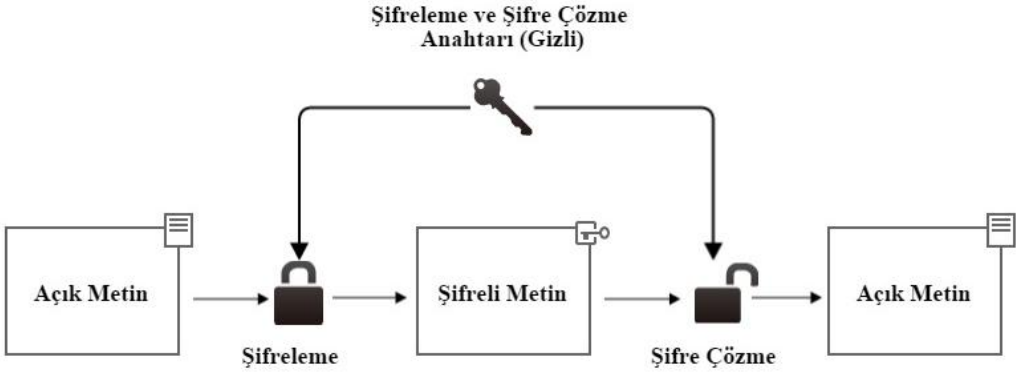
Sanayi devrimine kadar ilkel yöntemlerle oluşturulan şifreleme sistemleri, sanayi devrimi ile birlikte boyut değiştirmiş ve kriptoloji, matematiksel bir bilim dalı olarak

kabul görmeye başlamıştır. 20. yüzyıla gelindiğinde, dünya savaşları kriptolojinin gelişiminde önemli rol oynamıştır. I. Dünya savaşı ve takip eden yıllarda Rusların 56 adet yeni şifre geliştirdiği bilinmektedir. Şifreleme makinelerinin ortaya çıkışı ise 1930'lu yıllarda olmuştur. Almanların geliştirdiği Enigma şifreleme makinesi ile Japonların geliştirdiği Krieg ve Purple Code isimli şifreleme makineleri II. Dünya savaşı sırasında yoğun olarak kullanılmıştır [5].

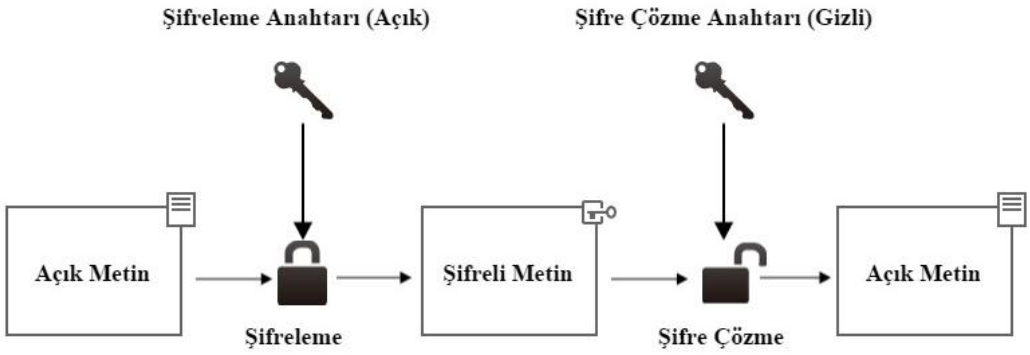
Bilgisayarların keşfi ile birlikte kriptoloji bilimindeki gelişmeler önemli ölçüde ivme kazanmış ve teknolojinin hızı ile doğru orantılı olarak kırılamayacak şifreleme sistemleri oluşturma çabaları devam etmiştir.

1.3. Modern Kriptoloji

Günümüzde, şifreleme algoritmaları simetrik, asimetrik olmak üzere iki kısımda incelenmektedir. Simetrik şifreleme algoritmaları hem şifreleme hem de şifre çözme adımlarında aynı ve gizli olan bir anahtar kullanırken, asimetrik şifreleme algoritmaları şifreleme adımı için açık bir anahtar, şifre çözme adımı için ise gizli bir anahtar kullanırlar. Ayrıca simetrik şifreleme algoritmalarının kendi içinde blok şifreleme ve akan şifreleme olmak üzere iki çeşidi bulunmaktadır. Blok şifreleme algoritmaları, açık veya şifreli metni, belirli uzunluktaki bloklara bölerek şifreleme ve şifre çözme işlemi yaparken, akan şifre algoritmaları her bit veya byte değeri için şifreleme ve şifre çözme işlemleri gerçekleştirirler. Şekil 1.1 ve Şekil 1.2'de sırasıyla simetrik ve asimetrik şifreleme sistemleri görülmektedir.



Şekil 1.1. Simetrik Şifreleme Sistemleri



Şekil 1.2. Asimetrik Şifreleme Sistemleri

1.4. Blok Şifreler

Blok şifreleme algoritmaları, açık metni sabit uzunluğa sahip ve blok olarak adlandırılan bit gruplarına bölerek işleme tabi tutar. Bloklar bir gizli anahtar yardımıyla şifrelenerek şifreli metin elde edilir. Şifre çözme işleminde ise yine aynı anahtar kullanılarak şifreli metinden açık metine ulaşılır. Blok şifreler, karıştırma ve yayılma teknikleri üzerine inşa edilmiştir [6]. Yer değiştirme yapıları (Substitution boxes: S-boxes), blok şifrelerde şifreli metin ve anahtar arasındaki ilişkiyi gizlemeyi, diğer bir deyişle, karıştırmanın gerçekleştirilmesini sağlarken, doğrusal dönüşüm yapıları ise açık metindeki izlerin şifreli metinde sezilmemesi olarak tanımlanabilen yayılmayı sağlar. Karıştırma yer değiştirme işlemleri ile gerçekleştirilirken yayılma ise doğrusal dönüşüm veya dönüşümler ile gerçeklenir. Ayrıca, blok şifre tasarımı için en çok kullanılan iki mimari, Feistel ağları ve SPN olarak da bilinen Yer değiştirme – Permütasyon ağlarıdır [7]. Feistel ağları kullanan blok şifrelere örnek olarak DEA algoritması, SPN ağlarını kullanan blok şifrelere örnek olarak ise AES algoritması verilebilir. Her iki mimaride yer değiştirme ve doğrusal dönüşüm yapılarını kullanmaktadırlar ve birden fazla şifreleme işleminin birleşmesi ile oluşturulurlar. Bu şifreler, aynı şifreleme adımının tekrarlanan uygulamasını içerir ve şifreleme işleminde her bir adımda tekrar eden matematiksel işlemler topluluğu döngüyü meydana getirir. Bir döngü birden fazla şifreleme adımı içerebilir. Örneğin bir döngüde hem S-kutuları gibi yer değiştirme yapıları, hem doğrusal dönüşümler, hem de basit aritmetik işlemler kullanılabilir. Bu yapıların her döngüde kullanılmasından ortaya çıkabilecek olası simetriyi bozmak için ise bir anahtar genişletme rutini yardımıyla, gizli anahtardan elde edilen farklı anahtarlar

bloğa eklenir. Diğer yandan bu mimarilerin arasındaki en temel fark döngü içerisinde bir bloğun işlenmesinde ortaya çıkmaktadır. Örneğin Feistel mimarisinde bir döngüde o anki bloğun yarısı işlenirken, SPN mimarisinde o anki bloğun tümü işlenir.

1.5. Blok Şifrelerin Parametreleri

Anahtar uzunluğu, S-kutuları, doğrusal dönüşümler, anahtar genişletme rutini, blok şifrelerin gücünü belirleyen önemli parametrelerdir.

1.5.1. Anahtar Uzunluğu

Blok şifrelerde anahtar uzunluğunun, şifrenin kaba kuvvet (brute-force) saldırısı olarak bilinen ve tüm olası anahtarları denemeye dayanan saldırı tipine karşı dayanıklılığını arttırmak için dikkatle seçilmesi önemlidir.

Bazı örnek blok şifrelerin anahtar uzunlukları aşağıda verilmektedir.

- DEA: 56-bit [8]
- AES: 128, 192, 256-bit [9]
- Camellia: 128, 192, 256-bit [10]
- ARIA: 128-bit [11]
- Khazad: 128-bit [12]
- Present: 80 veya 128-bit [13]
- Serpent: 128, 192, 256-bit [14]

1.5.2. S-Kutuları (Substitution-Boxes)

Blok şifreleme algoritmalarının diğer bir önemli elemanı, karıştırma işlevini üstlenen S-kutularıdır. Algoritmanın doğrusal olmayan tek elemanıdır. Bu nedenle kriptografik özellikleri iyi bir S-kutusu seçimi, şifrenin dayanıklılığını doğrudan etkilemektedir.

1.5.3. Doğrusal Dönüşümler

Blok şifrelerin önemli bir özelliği olan yayılma işlemini sağlayan yapılar, doğrusal dönüşümlerdir. Doğrusal dönüşümler, sabit uzunluktaki bir giriş bloğunu doğrusal olarak karıştırarak aynı uzunlukta bir çıkış bloğu elde edilmesini mümkün kılar [15]. Bir doğrusal dönüşümün şifre içerisinde kullanılıp kullanılamayacağını belirleyen ölçütler şu şekilde sıralanabilir;

- ***Çığ etkisi (Avalanche effect):*** Giriş bloğundaki bir bitlik değişimin, çıkış bloğunun yarısının değişmesine sebep olmasıdır [16].
- ***Katı çığ etkisi (Strict avalanche effect):*** Tek bir giriş bitinin değiştirilmesi, her çıkış bitinin %50 olasılıkla değişmesiyle sonuçlanacaktır [17].
- ***Bütünlük özelliği (Completeness property):*** Çıkış bitlerinin her birinin, giriş bitlerine bağımlılığını ifade etmektedir [18].
- ***Dallanma sayısı (Branch number):*** İkili doğrusal dönüşümler için, 0 giriş vektörü hariç diğer giriş vektörlerinin her birinin Hamming ağırlığı ile çıkış vektörlerinin her birinin Hamming ağırlığının toplamının minimum değeridir [19].
- ***Sabit nokta sayısı (Number of fixed point):*** Bir giriş bloğu, bu bloğa bir doğrusal dönüşüm uygulandıktan sonra elde edilen çıkış bloğu ile aynı ise o zaman bu giriş bloğuna o doğrusal dönüşümün sabit noktasıdır denilmektedir [15].

Doğrusal dönüşümlerin şifreye yapılan saldırılara karşı şifreyi güçlü kılacak şekilde seçilmeleri önemlidir. Diğer yandan, seçilen doğrusal dönüşümlerin yazılım ve donanıma uygulanmasının etkin ve verimli olması beklenir. Pek çok blok şifre, yayılım katmanı olarak Maximum Distance Separable (MDS) ve Maximum Distance Binary Linear (MDBL) olarak bilinen matrisleri kullanmaktadır. Örneğin, literatürde iyi bilinen şifrelerden olan AES'in doğrusal dönüşüm katmanı, $\mathbb{F}_{2^8}$ üzerinde 4×4 boyutunda MDS matris iken, Khazad şifresinin doğrusal dönüşüm katmanında ise $\mathbb{F}_{2^8}$ üzerinde 8×8 boyutunda involutif MDS matris kullanımı tercih edilmiştir. Camellia ve ARIA

şifrelerinde ise MDBL ikili matrislerin kullanıldığı görülmektedir. Camellia şifresinde, doğrusal dönüşüm katmanı olarak $\mathbb{F}_{2^8}$ üzerinde 8×8 boyutunda MDBL ikili matris, ARIA şifresinde ise $\mathbb{F}_{2^8}$ üzerinde 16×16 boyutunda involutif MDBL ikili matris kullanılmaktadır.

MBDL matrislerin uygulama safhasında sadece XOR işleminden faydalanılması, MDS matrislerin hem XOR hem de tablo okuma ve xtime (sola öteleme ile koşullu XOR'dan oluşan ve sonlu cisim çarpımında kullanılan işlem) işlemlerine gereksinim duyması yanında bir avantaj olarak kabul edilebilir [25]. Diğer yandan, Khazad ve ARIA gibi bazı şifrelerin tasarımlarında involutif (tersi kendisi) özelliğe sahip matrislerin kullanımı söz konusuyken, AES ve Camellia şifrelerinde ise involutif olmayan matrislerin kullanıldığı görülmektedir. İnvolutif yayılım katmanı kullanılması, hem uygulama maliyetlerini düşürmesi hem de şifreleme ve şifre çözme aşamalarının aynı ya da yakın maliyete ve kriptografik güce sahip olması açısından avantaj sağlar.

1.5.4. Anahtar Genişletme Rutini

Bir blok şifreleme algoritmasının her döngüsünde, aynı yapıların ardı ardına kullanılması nedeniyle istenmeyen ilişkilerin oluşması olasıdır. Oluşabilecek bu ilişkilerin bozulması için, her döngüde gizli anahtardan farklı anahtarlar elde edilmesini sağlayan anahtar genişletme rutinleri kullanılmaktadır. Anahtar genişletme rutinleri; şifrenin simetrik yapısının ortadan kaldırılmasının yanı sıra, şifre anahtarının bir kısmının saldırgan tarafından bilindiği saldırılar, şifre anahtarının bilindiği veya seçilebildiği saldırılar ve ilişkili-anahtar saldırılarından da şifrenin korunmasına yardımcı olur [20].

1.6. Tezin Gerekçesi ve Önemi

Blok şifrelerde Bölüm 1.5.3'te bahsedilen doğrusal dönüşümler için en önemli yayılım ölçütlerinden biri dallanma sayısıdır. Dallanma sayısı ölçütü, S-kutuları ile beraber doğrusal dönüşümün, doğrusal ve diferansiyel kriptanalize karşı dayanıklılığının belirlenmesini sağlar. Sabit nokta sayısı ise doğrusal dönüşümünün

kriptografik başarımını belirleyen diğer bir yayılım ölçütüdür. Çoğu zaman, dallanma sayısı yüksek ve sabit nokta sayısı düşük bir yayılım katmanı bulmak önemli bir sorundur. Söz konusu kriptografik özelliklere sahip doğrusal dönüşümler (ikili matris), rastgele arama yapılarak elde edilebilir. Ancak matrisin boyutu arttıkça, arama karmaşıklığı artacağından yüksek boyutlarda (örneğin 16×16 boyutundaki ikili matrisler) bu yöntem pratik olmamaktadır. Bu tez çalışması; yukarıda bahsi geçen soruna odaklanan, arama uzayını küçülten ve MDBL (maksimum dallanma sayısı özelliklerine sahip ikili matrisler) matrislerin geliştirilmesi üzerinedir. Tez çalışmasında düşük sabit nokta sayısına (fixed points) sahip ikili matrislerin üretilmesi de göz önüne alınacak diğer bir kriptografik kriterdir.

Bu noktadan yola çıkarak, 6×6, 8×8, 12×12, 16×16 ve 32×32 boyutlarında maksimum dallanma sayısına (söz konusu boyutlarda, doğrusal ve diferansiyel kriptanaliz saldırılarında şifrenin güvenliğini arttıracak) ve minimum sabit nokta sayısına sahip ikili matrislerin üretilmesi için bir arama yönteminin geliştirilmesi amaçlanmaktadır. Bu yöntem, farklı boyutlarda (Örn: 10×10, 20×20, 24×24) benzer kriptografik özelliklere sahip ikili matrislerin geliştirilmesi için de kullanılabilmektedir.

Literatürde MDBL matrislerin, bir blok şifre tasarımında kullanılabilecek şekilde geliştirilmesi üzerine fazla çalışmanın olmaması ve tez konusunun kodlama teorisinde önemli bir çalışma konusu olması tezin önemini ortaya koymaktadır.

BÖLÜM 2

MATEMATİK ALTYAPI

Bu bölümde, tez çalışması esnasında yararlanılan matematiksel ifadelerin anlaşılabilmesi adına temel bir altyapı verilecektir. Verilen tanım, teorem ve önermelerin ispatlarına [21, 22, 23, 24, 25]'den ulaşılabilir.

Tanım 2.1. "■" sembolü ile gösterilen ve $a■b$ şeklinde ifade edilen herhangi bir ikili işlem için A kümesi, aşağıdaki 4 aksiyomu sağlıyorsa grup olarak adlandırılır.

i. Kapalılık Özelliği: $a, b \in A$ ise $a■b \in A$'dır.
ii. Birleşme Özelliği: Her $a, b, c \in A$ için $(a■b)■c = a■(b■c)$
iii. Etkisiz (birim) Eleman: Her $a \in A$ için $a■e = e■a = a$ olacak şekilde bir $e \in A$ vardır.
iv. Ters Eleman: Her $a \in A$ için öyle bir $a' \in A$ vardır ki $a■a' = a'■a = e$ olur.

Tanım 2.2. Tanım 2.1'de verilen 4 özelliğe ek olarak A kümesi, her $a, b \in A$ için $a■b = b■a$ ifadesini, diğer bir deyişle; değişme özelliğini sağlıyorsa, değişmeli veya abelyan (abelian) grup olarak isimlendirilir.

Tanım 2.3. B, A grubunun bir alt kümesi olmak üzere, A grubu üzerinde tanımlı **"■"** işlemine göre bir grup oluşturuyorsa A'nın alt grubu olarak adlandırılır. Tanım gereği;

i. a ve b her iki grubun elemanı ise $c = a■b$'de her iki grubun elemanıdır.
ii. Aynı birim elemana sahiptirler.
iii. a her iki grubun elemanı ise a'nın tersi de her iki grubun elemanıdır.
iv. A kümesinin birim elemanından elde edilen grup, A grubunun bir alt grubudur.

v. Her grup, kendisinin alt grubudur.

Tanım 2.4. Bir grubun alt grubu, bu grubun bir elemanının üsleri alınarak, diğer bir deyişle; grup işlemi bu elemana devamlı uygulanarak elde edilebiliyorsa bu gruba devirli (cyclic) alt grup adı verilir.

Tanım 2.5. Bir grubun tüm elemanları, grubun bir elemanı kullanılarak (elemanın üsleri alınarak) elde edilebiliyorsa bu gruba devirli grup, bu elemana ise üreteç (generator) eleman denilmektedir. Bir devirli grubun, birden fazla üreteç elemanı bulunabilmektedir.

Tanım 2.6. Bir doğrusal dönüşümün elemanları $A: (\{0,1\}^m)^n \rightarrow (\{0,1\}^m)^n$ olmak üzere (2.1) ifadesindeki gibi tanımlanabilir.

$$A(x) = A.x^T = \begin{bmatrix} a_{11} & a_{12} & . & . & . & a_{1n} \\ a_{21} & a_{22} & . & . & . & a_{2n} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ a_{n1} & a_{n2} & . & . & . & a_{nn} \end{bmatrix} . \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_n \end{bmatrix} \tag{2.1}$$

Doğrusal dönüşüm elemanları (a_{ij}) $\mathbb{F}_2$ üzerinden seçilirse ($m = 1$ alınırsa) bu doğrusal dönüşüme ikili doğrusal dönüşüm denilmektedir.

Tanım 2.7. C kod kelimesinin Hamming ağırlığı $wt(C)$ olarak ifade edilebilir ve kod kelimesinin 0 olmayan elemanlarının sayısı veya kod kelimesindeki 1'lerin sayısı olarak tanımlanır. Ayrıca, $(\mathbb{F}_{2^m})^n$ vektör uzayından n boyutlu iki vektör arasındaki Hamming uzaklığı da vektörlerin farklılaştığı pozisyon sayısı olarak tanımlanır.

Tanım 2.8. $n \times n$ boyutunda bir A matrisinin diferansiyel dallanma sayısı (branch number) ifade (2.2)'deki gibi tanımlanabilir.

$$\beta_d(A) = \min\{wt(x) + wt(A.x^T) | \, x \in (\{0,1\}^m)^n, x \neq 0\} \tag{2.2}$$

Tanım 2.9. $n \times n$ boyutunda bir A matrisinin doğrusal dallanma sayısı ifade (2.3)'deki gibi tanımlanabilir.

$$\beta_l(A) = \min\{wt(x) + wt(A^T.x^T) | \, x \in (\{0,1\}^m)^n, x \neq 0\} \tag{2.3}$$

(2.2) ve (2.3)'deki ifadelere göre ikili bir doğrusal dönüşüm matrisinin dallanma sayısı, 0 giriş vektörü hariç diğer giriş vektörlerinin her birinin Hamming ağırlığı ile çıkış vektörlerinin her birinin Hamming ağırlığının toplamının minimum değeridir [26].

Teorem 2.1. Eğer $G_{n\times 2n} = [I_{n\times n}, A_{n\times n}]$, $[2n, n, d]$ ikili doğrusal kodu üreten matrisin indirgenmiş basamak matrisi (echelon form) ise A^T'nin dallanma sayısı d'dir [28].

Açıklama 2.1. Bir doğrusal dönüşümün dallanma sayısı, birbirini takip eden iki döngüde bulunan aktif S-kutularının en düşük sınırıdır.

Tanım 2.10. U ve V $2^{n-1} \times 2^{n-1}$ sonlu cisim Hadamard matrisleri olmak üzere bir $2^n \times 2^n$ sonlu cisim Hadamard matrisi ifade (2.4)'de görüldüğü gibi tanımlanabilir [27].

$$had(U,V) = \begin{bmatrix} U & V \\ V & U \end{bmatrix} \tag{2.4}$$

Tanım 2.11. Dairesel (circulant) formdaki matrisler, dairesel olarak matrisin her satırının 1 pozisyon sağa ötelenmesi ile elde edilmektedirler. Dairesel formdaki bir A matrisi (2.5) ifadesinde verilmektedir.

$$A = circ(a_1, a_2, \ldots, a_n) = \begin{bmatrix} a_1 & a_2 & \ldots & a_n \\ a_n & a_1 & \ldots & a_{n-1} \\ . & . & \ldots & . \\ a_2 & a_3 & \ldots & a_1 \end{bmatrix} \tag{2.5}$$

Tanım 2.12. Eğer bir A matrisinin tersi kendisine eşit ise $(A = A^{-1})$, bu A matrisine involutif matris adı verilmektedir.

Tanım 2.13. Bir $\mathbb{F}_{2^m}$ üzerine bir $[n, k, d]$ kod, vektör uzayı $(\mathbb{F}_{2^m})^n$'in k boyutlu bir alt uzayıdır ve n elemanlı iki vektör arasındaki Hamming uzaklığı minimum d'dir. Bu özellik ile d en büyük değerdir. Doğrusal bir $[n, k, d]$ kod C için bir G üreteç matris, satırları C için bir taban oluşturan $k \times n$ boyutunda bir matristir. Doğrusal $[n, k, d]$ kodlar Singleton sınırı olan $d \leq n - k + 1$ eşitsizliğini sağlamaktadırlar.

Tanım 2.14. Doğrusal bir $[n, k, d]$ kod C, $d = n - k + 1$ eşitliğini sağlıyor ise, Maximum Distance Separable (MDS) kod olarak adlandırılır.

Teorem 2.2. Üreteç matris $G = [I|A]$ ile doğrusal bir $[n, k, d]$ kod C, A matrisinin tüm alt matrisleri nonsingular ise, MDS matris olarak adlandırılır.

MDS matrislerin temel özellikleri aşağıda verilmektedir.

i. Bir $m \times m$ kare matrisi A'nın tüm kare alt matrisleri nonsingular (determinantı 0'dan farklı) ise A bir MDS matristir.
ii. $m \times m$ boyutundaki bir MDS matrisin tüm girişleri 0'dan farklıdır.
iii. Eğer $m \times m$ boyutundaki bir A matrisi MDS ise A matrisinin dallanma sayısı $m + 1$'dir.

Tanım 2.15. $n \times n$ ikili matrislerin maksimum dallanma sayısı, ikili $[2n, n]$ doğrusal kodların maksimum uzaklığına eşittir [28].

Tanım 2.15'e ek olarak, ikili bir doğrusal dönüşümün maksimum dallanma sayısına sahip olabilmesi için bu kodların maksimum uzaklığının alt ve üst sınırlarının birbirine eşit olması gerekir. Bu tür kodlara maksimum uzaklığa sahip ikili doğrusal kodlar (Maximum Distance Binary Linear Codes – MDBL) adı verilmektedir. İkili [$2n$, n] doğrusal kodlarda $n > 18$ maksimum uzaklığın alt ve üst sınırları bazı n değerleri için eşit değildir. Dolayısıyla bu tür kodlarda maksimum uzaklığın erişilebilir değeri ve teorik sınırlarından bahsetmek daha uygun olur. Örneğin [64, 32] doğrusal kodların (n = 32) maksimum uzaklığının erişilebilir değeri 12 iken teorik sınırı 16'dır. Diğer bir

deyişle 32×32 bir ikili matrisin erişilebilir dallanma sayısı 12'dir. Tablo 2.1, ikili [*2n, n*] doğrusal kodlardaki maksimum uzaklığın alt ve üst sınırlarını göstermektedir.

Tablo 2.1. İkili [*2n, n*] Doğrusal Kodların Maksimum Uzaklıkları

n	***Alt Sınır***	***Üst Sınır***	***n***	***Alt Sınır***	***Üst Sınır***
1	2	2	**17**	8	8
2	2	2	**18**	8	8
3	3	3	**19**	8	9
4	4	4	**20**	9	10
5	4	4	**21**	10	10
6	4	4	**22**	10	10
7	4	4	**23**	11	11
8	5	5	**24**	12	12
9	6	6	**25**	10	12
10	6	6	**26**	10	12
11	7	7	**27**	11	13
12	8	8	**28**	12	14
13	7	7	**29**	12	14
14	8	8	**30**	12	14
15	8	8	**31**	12	15
16	8	8	**32**	12	16

Tanım 2.16. *A* bir doğrusal dönüşüm ve x bu doğrusal dönüşüme giriş bloğu olmak üzere, $A \cdot x = x$ ise, x bu doğrusal dönüşümdeki sabit noktadır denilmektedir. Diğer bir deyişle; *A* doğrusal dönüşümü giriş vektörünü aynı çıkış vektörüne haritalıyorsa bu giriş vektörüne sabit nokta adı verilir (İfade (2.6) ve (2.7)).

$$A \cdot x = x \tag{2.6}$$

$$\begin{bmatrix} a_{11} & a_{12} & . & . & . & a_{1n} \\ a_{21} & a_{22} & . & . & . & a_{2n} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ a_{n1} & a_{n2} & . & . & . & a_{nn} \end{bmatrix} . \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_n \end{bmatrix} = \begin{bmatrix} x_1 \\ x_2 \\ . \\ . \\ . \\ x_n \end{bmatrix} \tag{2.7}$$

Bir doğrusal dönüşümde giriş bitlerinin m-bit değerlerden oluştuğunu düşünelim. Ayrıca, doğrusal dönüşüm matrisinin $n \times n$ boyutunda ve *I* birim matrisinin

yine $n \times n$ boyutunda olduğunu varsayalım. Bu halde doğrusal dönüşüm matrisi A için tüm sabit noktaların sayısı (2.8)'deki ifadenin çözülmesi ile elde edilebilir.

$$(A + I)x^T = 0 \tag{2.8}$$

(2.8) ifadesinden A doğrusal dönüşümündeki sabit noktaların sayısı, (2.9) ifadesindeki gibi elde edilebilir.

$$F_A = 2^{m(rank(A)-rank(A+I))} = 2^{m(n-rank(A+I))} \tag{2.9}$$

Tanım 2.17. I, 12×12 boyutunda birim matris ve A, 12×12 boyutunda bir ikili matris olmak üzere $G = [I_{12}|A]$ şeklinde yazıldığında ve Önerme 2.1'de verilen özellikleri sağladığında G genişletilmiş ikili Golay kod (Extended Binary Golay Code) olarak adlandırılır ve G_{24} notasyonu ile gösterilir [29].

Önerme 2.1. Tanım 2.17'de verilen G_{24} genişletilmiş ikili Golay kodun özellikleri aşağıda görüldüğü gibi sıralanabilir.

i. Kodun uzunluğu 24, boyutu ise 12'dir.
ii. G_{24}'ün eşlik denetimi matrisi 12×24 boyutunda bir matris olup $H = [A|I_{12}]$ şeklinde gösterilir.
iii. G_{24} kodu kendinin dualidir. Diğer bir deyişle; $G_{24}^{\perp} = G_{24}$'tür.
iv. G_{24}'ün bir diğer eşlik denetimi matrisi yine 12×24 boyutunda bir matris olup $H' = [I_{12}|A] = G$ olarak gösterilebilir.
v. G_{24} için bir diğer 12×24 boyutundaki üreteç matris, $G' = [A|I_{12}] = H$'tır.
vi. G_{24}'ün her bir kodsözünün Hamming ağırlığı 4'ün katlarıdır.
vii. G_{24} kodunun minimum uzaklığı $d = 8$'dir.
viii. G_{24} kodu üç biti hatayı düzeltebilmektedir.

MAGMA Hesaplamalı Cebir Sistemi

MAGMA hesaplamalı cebir sistemi; sayılar teorisi ve cebirsel hesaplamalar için tasarlanmış bir yazılım paketidir. Avustralya Sydney Üniversitesi bünyesinde geliştirilmiştir. Ticari bir yazılım olmakla birlikte, ücretsiz fakat kısıtlanmış bir sürümüne http://magma.maths.usyd.edu.au/calc/ adresinden ulaşılabilmektedir. Seminer çalışması esnasında geliştirilen yapılar, MAGMA yazılımı yardımı ile test edilmiştir [30].

C programlama dilinin sözdizimine benzer bir yapıya sahip olan MAGMA yazılımında gerçekleştirilen bazı işlemlere ait örnek kodlar aşağıda verilmiştir.

Örnek 2.1. 8×8 boyutundaki bir M ikili matrisi, MAGMA ile aşağıdaki şekilde kodlanabilmektedir.

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

```
n:=8;
M:=Matrix(GF(2),n,n,[
1,0,0,0,1,1,1,0,
0,1,0,0,1,0,1,1,
0,0,1,0,0,1,1,1,
0,0,0,1,1,1,1,1,
1,1,1,0,1,0,0,0,
1,0,1,1,0,1,0,0,
0,1,1,1,0,0,1,0,
1,1,1,1,0,0,0,1]);
```

M ikili matrisinin determinantını bulmak için aşağıdaki kod kullanılabilmektedir.

```
Determinant(M);
```

M ikili matrisinin ve transpozunun (M^T) dallanma sayısını bulmak için aşağıdaki kod kullanılabilmektedir.

```
B:=HorizontalJoin(IdentityMatrix(GF(2),8),M);
C:=LinearCode(B);
printf("Bn: ");
MinimumWeight(C);
B:=HorizontalJoin(IdentityMatrix(GF(2),8),Transpose(M));
C:=LinearCode(B);
printf("T Bn: ");
MinimumWeight(C);
```

M ikili matrisinin sabit nokta sayısını bulmak için aşağıdaki kod kullanılabilmektedir.

```
I:=IdentityMatrix(GF(2),n);
printf("FPn: ");
2^(n-Rank(M+I));
```

M ikili matrisinin genişletilmiş ikili Golay kod olup olmadığı ise aşağıda görülen kod yardımıyla anlaşılabilmektedir.

```
n:=12;
M:=Matrix(GF(2),n,n,[
1,0,0,0,1,0,1,1,1,1,0,1,
0,1,0,1,1,1,1,1,0,0,0,1,
0,0,1,0,1,1,1,0,0,1,1,1,
0,1,0,1,0,0,1,0,1,1,1,1,
1,1,1,0,1,0,0,0,1,1,1,0,
0,1,1,0,0,1,1,1,1,1,0,0,
1,1,1,1,0,1,1,0,0,0,1,0,
1,1,0,0,0,1,0,1,0,1,1,1,
1,0,0,1,1,1,0,0,1,0,1,1,
1,0,1,1,1,1,0,1,0,1,0,0,
0,0,1,1,1,0,1,1,1,0,1,0,
1,1,1,1,0,0,0,1,1,0,0,1
]);
B:=HorizontalJoin(IdentityMatrix(GF(2),n),M);
C:=LinearCode(B);
IsEquivalent(C, GolayCode(GF(2), true));
```

BÖLÜM 3

ÖNERİLEN YÖNTEM

Tezin bu bölümünde, $k \in \{3,4\}$ ve $t \in \{1,2\}$ olmak üzere $n = k.2^t$ için, $k \times k$ boyutunda devirli matris grupları ve $2^t \times 2^t$ Hadamard matrisler kullanılarak maksimum dallanma sayısı ve minimum sabit nokta sayısına sahip $n \times n$ boyutundaki ikili matrislerin üretilmesi için yeni bir yöntem önerilmektedir. Bu önerilen yöntem, daha büyük k ve t değerleri için de uygulanabilmektedir. Özellikle büyük k değerleri için oluşabilecek hesaplama ile ilgili zorluklar nedeniyle tez çalışmasında $k \in \{3,4\}$ durumlarına odaklanılmıştır.

Bölüm 3.1, bir diğer çalışmada [31] gerçekleştirilen ve bu tezde yapılan çalışmaya temel oluşturan yöntemin özetlenmesine ayrılmıştır. Bölüm 3.2'de, bu tez çalışmasında önerilen yöntemin altyapısı ile ilgili bilgiler verilmekte, Bölüm 3.3'te ise yöntemin algoritması açıklanmaktadır.

3.1. İndirgenemez Polinomlar Yardımıyla Cebirsel Yöntem

$\mathbb{F}_{2^3}$ cisminin tanımlanması amacıyla kullanılabilecek 2 indirgenemez polinom $x^3 + x + 1$ ve $x^3 + x^2 + 1$ şeklindedir.

$x^3 + x + 1$ ile tanımlanan $\mathbb{F}_{2^3}$ cisminin üreteç elemanı α olarak alındığında, oluşan cismin tüm elemanları ile bu elemanların ikili ve onaltılık (hexadecimal) gösterimleri aşağıda görüldüğü şekildedir.

$\alpha^1 = \alpha$	010	2_H
$\alpha^2 = \alpha^2$	100	4_H
$\alpha^3 = \alpha + 1$	011	3_H
$\alpha^4 = \alpha^2 + \alpha$	110	6_H
$\alpha^5 = \alpha^2 + \alpha + 1$	111	7_H
$\alpha^6 = \alpha^2 + 1$	101	5_H
$\alpha^7 = 1$	001	1_H

Diğer taraftan, $\mathbb{F}_{2^3}$ cismi $x^3 + x + 1$ polinomu ile tanımlandığında ve bu polinomu bir kökü α olarak alındığında herhangi bir $x \in \mathbb{F}_{2^3}$ için;

$$x = \alpha^2 x_2 + \alpha x_1 + x_0$$

olarak yazılabilir. Burada, $(x_2, x_1, x_0) \in \mathbb{F}_2$'dir ve $(\alpha_2, \alpha_1, \alpha_0) = (\alpha^2, \alpha^1, 1)\mathbb{F}_2$ üzerine $\mathbb{F}_{2^3}$'ün bir polinom tabanıdır. Sonlu cisim $\mathbb{F}_{2^3}$'ün bir elemanı olan α'nın x ile çarpımı;

$$\begin{aligned} \alpha(\alpha^2 x_2 + \alpha x_1 + x_0) &= \alpha^3 x_2 + \alpha^2 x_1 + \alpha x_0 \\ &= \alpha^2 x_1 + \alpha x_2 + x_2 + \alpha x_0 \\ &= \alpha^2 x_1 + \alpha(x_2 + x_0) + x_2 \end{aligned}$$

olarak elde edilebilir ve bu da aşağıda görüldüğü gibi 3×3 boyutunda bir ikili matris şeklinde yazılabilir.

$$\begin{bmatrix} x_0' \\ x_1' \\ x_2' \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} . \begin{bmatrix} x_0 \\ x_1 \\ x_2 \end{bmatrix}$$

Bu işlemler $\mathbb{F}_{2^3}$ cisminin diğer elemanlarına uygulandığında her elemanın 3×3 boyutunda ikili matris karşılıkları oluşturulabilir. Tablo 3.1, söz konusu ikili doğrusal dönüşümleri göstermektedir.

Tablo 3.1. İndirgenemez Polinom $x^3 + x + 1$ ile Tanımlı $\mathbb{F}_{2^3}$ cisminin Elemanlarının x Sonlu Cisim Elemanı ile Çarpımı Sonucu Üretilen 3×3 Boyutunda İkili Doğrusal Dönüşümler

Onaltılık Değer	***3×3 Boyutunda İkili Doğrusal Dönüşümü***	***Onaltılık Değer***	***3×3 Boyutunda İkili Doğrusal Dönüşümü***
1	$\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$	5	$\begin{bmatrix}1 & 1 & 0\\0 & 0 & 1\\1 & 0 & 0\end{bmatrix}$
2	$\begin{bmatrix}0 & 0 & 1\\1 & 0 & 1\\0 & 1 & 0\end{bmatrix}$	6	$\begin{bmatrix}0 & 1 & 1\\1 & 1 & 0\\1 & 1 & 1\end{bmatrix}$
3	$\begin{bmatrix}1 & 0 & 1\\1 & 1 & 1\\0 & 1 & 1\end{bmatrix}$	7	$\begin{bmatrix}1 & 1 & 1\\1 & 0 & 0\\1 & 1 & 0\end{bmatrix}$
4	$\begin{bmatrix}0 & 1 & 0\\0 & 1 & 1\\1 & 0 & 1\end{bmatrix}$		

Benzer şekilde, $\mathbb{F}_{2^4}$ cismi $x^4 + x + 1$ polinomu ile tanımlandığında ve bu polinomu bir kökü α olarak alındığında herhangi bir $x \in \mathbb{F}_{2^4}$ için;

$$x = \alpha^3 x_3 + \alpha^2 x_2 + \alpha x_1 + x_0$$

olarak yazılabilir. Burada, $(x_3, x_2, x_1, x_0) \in \mathbb{F}_2$'dir. Buna ek olarak $(\alpha_3 \alpha_2, \alpha_1, \alpha_0) = (\alpha^3, \alpha^2, \alpha^1, 1)$ $\mathbb{F}_2$ üzerine $\mathbb{F}_{2^4}$'ün bir polinom tabanıdır. Sonlu cisim $\mathbb{F}_{2^4}$'ün bir elemanı olan α'nın x ile çarpımı;

$$\begin{aligned}\alpha(\alpha^3 x_3 + \alpha^2 x_2 + \alpha x_1 + x_0) &= \alpha^3 x_2 + \alpha^2 x_1 + \alpha x_0\\ &= \alpha^4 x_3 + \alpha^3 x_2 + \alpha x_1 + \alpha x_0\\ &= \alpha^3 x_2 + \alpha^2 x_1 + \alpha(x_3 + x_0) + x_3\end{aligned}$$

olarak elde edilebilir ve bu da aşağıda görüldüğü gibi 4×4 boyutunda bir ikili matris şeklinde yazılabilir.

$$\begin{bmatrix} x_0' \\ x_1' \\ x_2' \\ x_3' \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix}$$

Bu işlemler $\mathbb{F}_{2^4}$ cisminin diğer elemanlarına uygulandığında her elemanın 4×4 boyutunda ikili matris karşılıkları oluşturulabilir. Tablo 3.2, söz konusu ikili doğrusal dönüşümleri göstermektedir [31, 37].

Tablo 3.2. İndirgenemez Polinom $x^4 + x + 1$ ile Tanımlı $\mathbb{F}_{2^4}$ cisminin Elemanlarının x Sonlu Cisim Elemanı ile Çarpımı Sonucu Üretilen 4×4 Boyutunda İkili Doğrusal Dönüşümler

Onaltılık Değer	***4×4 Boyutunda İkili Doğrusal Dönüşümü***	***Onaltılık Değer***	***4×4 Boyutunda İkili Doğrusal Dönüşümü***	***Onaltılık Değer***	***4×4 Boyutunda İkili Doğrusal Dönüşümü***
1	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	2	$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	3	$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$
4	$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$	5	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$	6	$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$
7	$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$	8	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$	9	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$
A	$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$	B	$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$	C	$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$
D	$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	E	$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	F	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \end{bmatrix}$

3.2. Yöntemin Altyapısı

Bu tez çalışmasında önerilen yöntem, yukarıda indirgenemez polinomlar yardımıyla oluşturulan cebirsel yöntemin genelleştirilmiş hali olarak düşünülebilmekte ve aşağıda görülen iki temel aşamadan oluşmaktadır.

- Mertebesi $2^k - 1$ olan tüm $k \times k$ boyutundaki ikili matrislerin hesaplanması,
- Hadamard formda yayılım katmanının oluşturulması.

İlk aşama olan ön hesaplama aşamasında, $k \in \{3,4\}$ olmak üzere mertebesi $2^k - 1$ olan tüm $k \times k$ boyutundaki ikili matrisler taranmış ve yine $k \in \{3,4\}$ olacak şekilde k derecesine sahip indirgenemez polinomun bir köküne karşılık gelen matrisler gruplanmıştır. Bu işlemlerle $\mathbb{F}_{2^k}$ sonlu cisminin matrislerle temsil edilebilmesi sağlanmıştır.

Tanım 3.1. Matris çarpımı altında $k \times k$ boyutundaki tersi alınabilir matrislerinin kümesi, genel lineer grup $(GL(k, \mathbb{F}_q))$ olarak adlandırılır ve eğer $k \times k$ boyutundaki bir A matrisi $A \in GL(k, \mathbb{F}_q)$ ise $\det(A) \neq 0$'dır.

Yukarıda bahsi geçen ön hesaplama aşaması sonucunda elde edilen gruplar ise Tanım 3.1'de verilen $GL(k, \mathbb{F}_q)$ grubunun bir alt kümesi olup özel lineer grup olarak adlandırılır ve $(SL(k, \mathbb{F}_q))$ şeklinde gösterilir. Ek olarak; $k \times k$ boyutundaki bir A matrisi için, $A \in SL(k, \mathbb{F}_q)$ ise $\det(A) = 1$'dir.

Önerme 3.1. $\mathbb{F}_2$ sonlu cismindeki $k \times k$ boyutunda tersi alınabilir matris sayısı, $GL(k, \mathbb{F}_2)$ genel lineer grubunun eleman sayısına eşittir ve bu eleman sayısı $\prod_{i=0}^{k-1}(2^k - 2^i)$ eşitliği ile hesaplanabilir [32].

Açıklama 3.1. Önerme 3.1 gereği 3×3 boyutunda 168, 4×4 boyutunda ise 20,160 tersi alınabilir ikili matris bulunmaktadır.

$2^t \times 2^t$ boyutunda Hadamard matrisler kullanılarak, $n \times n$ boyutunda iyi kriptografik özelliklere sahip yayılım katmanları elde edilirken daha verimli çalışabilmek adına Açıklama 3.1'de bahsedilen $k \times k$ boyutundaki tersi alınabilir matrislerin sayısının azaltılması önemlidir. Bunu gerçekleştirebilmek için ise aşağıdaki yol izlenmiştir.

- $\mathbb{F}_2$ sonlu cismi üzerinde, $k \in \{3,4\}$ olacak şekilde üretilmiş tüm $k \times k$ boyutundaki matrislerin mertebesi hesaplanır.
- $\mathbb{F}_2$ sonlu cismi üzerinde, derecesi k olan indirgenemez polinomun kökü ve mertebesi $2^k - 1$ olan matrisler tespit edilir. Belirtilmelidir ki, $k \in \{3,4\}$ olmak üzere $k \times k$ boyutundaki ikili matrisler için, $x^3 + x + 1$ ve $x^4 + x + 1$ indirgenemez polinomları kullanılmaktadır.
- $k \times k$ boyutundaki birbirinden farklı tüm devirli matris grupları elde edilir.

Yukarıda sözü edilen strateji takip edilerek 3×3 boyutunda, $x^3 + x + 1$ polinomunun bir kökü ve mertebesi 7 olan, 8 adet devirli matris grubu ve 4×4 boyutunda ise $x^4 + x + 1$ polinomunun bir kökü ve mertebesi 15 olan, 336 adet devirli matris grubu elde edilmiştir. Diğer bir ifadeyle; $k \in \{3,4\}$ olmak üzere $\mathbb{F}_2$ sonlu cismi üzerindeki üreteç matrisler, bir ön hesaplama yapılarak elde edilmiştir. Dolayısıyla, Önerme 3.2 ve Önerme 3.3'de de özetlendiği gibi arama uzayı önemli ölçüde azaltılmıştır.

Önerme 3.2. g bir üreteç matrisi, I ise birim matrisi temsil etmek üzere, $\mathbb{F}_2$ sonlu cismi üzerinde derecesi 3 olan $f(g) = g^3 + g + 1$ ve $f(g) = g^3 + g^2 + 1$ indirgenemez polinomlarının bir kökü ve mertebesi 7'ye eşit 3×3 boyutundaki ikili matrislerin sayısı $6.8 = 48$'dir.

Önerme 3.3. g bir üreteç matrisi, I ise birim matrisi temsil etmek üzere, $\mathbb{F}_2$ sonlu cismi üzerinde derecesi 4 olan $f(g) = g^4 + g + 1$ ve $f(g) = g^4 + g^3 + 1$ indirgenemez polinomlarının bir kökü ve mertebesi 15'e eşit 4×4 boyutundaki ikili matrislerin sayısı $8.336 = 2688$'dir.

Buna ek olarak; elde edilen matrisler $SL(k, \mathbb{F}_q)$ grubunun bir üyesi olduklarından, determinantları 1'e eşittir.

Yöntemin ikinci aşamasında ise yukarıda elde edilen 3×3 ve 4×4 boyutundaki matris gruplarının elemanları, izomorfik olduğu $2^t \times 2^t$ boyutunda Hadamard matrisin $\mathbb{F}_{2^3}$ ve $\mathbb{F}_{2^4}$ elemanları ile sırasıyla yer değiştirilir. Sonuçta maksimum dallanma sayısı ve minimum sabit nokta sayısına sahip 6×6, 8×8, 12×12, 16×16 ve 32×32 boyutlarındaki ikili matrisler MAGMA yazılımı kullanılarak elde edilmektedir.

3.3. Yöntemin Algoritması

$k \in \{3,4\}$ ve $t \in \{1,2\}$ olmak üzere $n = k.2^t$ olarak düşünüldüğünde yöntemin algoritması aşağıdaki adımlar ile tanımlanabilmektedir.

Adım 1. Mertebesi $2^k - 1$ olan $k \times k$ boyutunda devirli matris grupları oluşturulur. Bu işlem, rastgele seçilen bir nonsingular $k \times k$ boyutundaki matrisin $2^k - 1$'e kadar kuvvetinin alınması ile gerçekleştirilebilir. Bu şekilde 3×3 boyutunda 8, 4×4 boyutunda ise 336 adet devirli matris grubu elde edilmiştir.

Adım 2. Birinci adımda elde edilen $k \times k$ boyutundaki devirli matris grupları, Hadamard formda $2^t \times 2^t$ bloklar halinde dizilerek $n \times n$ boyutunda ikili matrisler elde edilir.

Adım 3. Tüm $n \times n$ boyutundaki ikili matrisler elde edilene kadar tüm $k \times k$ boyutundaki devirli matris grupları için işlem tekrarlanır.

Adım 4. Nonsingular olan $n \times n$ boyutundaki ikili matrislerden maksimum dallanma sayısı ve minimum sabit nokta sayısına sahip olanlar elde edilir.

Açıklama 3.2. Elde edilen ikili matrislerden kriptografik özellikleri iyi olanlar MAGMA yazılımı yardımı ile tespit edilmiştir.

BÖLÜM 4

3×3 BOYUTUNDA DEVİRLİ MATRİS GRUPLARI

Tezin bu bölümü, 3×3 boyutundaki devirli matris grupları kullanılarak 6×6 ve 12×12 boyutunda, maksimum dallanma sayısı ile minimum sabit nokta sayısına sahip matrislerin elde edilmesiyle ilgili örnek ve açıklamaları içermektedir.

Üçüncü bölümde de bahsedildiği gibi 3×3 ikili matris uzayında tüm 3×3 ikili matrisler taranarak 8 adet devirli matris grubu (g, 3×3 boyutunda ikili bir matris, $g^3 = g + I$ olmak üzere ve $g^7 = I$ olacak şekilde) elde edilmiştir. Bu gruplar bir Tablo 4.1'de verilmektedir. Verilen tabloda örneğin 001-011-111, 3×3 boyutunda grubun $\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ şeklinde ikili bir üreteç matrisini temsil etmektedir.

Tablo 4.1. 3×3 Boyutunda Devirli Matris Grupları

001-011-111
001-100-110
001-110-011
010-011-101
010-101-100
010-111-011
011-001-100
011-100-010

g, $f(x) = x^3 + x + 1$ indirgenemez polinomunun bir kökü ve $g^7 = I$ olmak üzere 3×3 boyutunda bir ikili matris olarak düşünüldüğünde üretilecek devirli grup $\mathbb{F}_{2^3}^*$

(0 elemanı hariç diğer elemanların olduğu $\mathbb{F}_{2^3}$ cismi) cismi ile izomorf olduğundan grubun elemanları onaltılık (hexadecimal) notasyonda aşağıda görüldüğü şekilde yazılabilmektedir.

Tablo 4.2. Grup Elemanlarının İkilik ve Onaltılık Notasyonda Gösterimi

$g^1 = g$	010	2_H
$g^2 = g^2$	100	4_H
$g^3 = g + I$	011	3_H
$g^4 = g^2 + g$	110	6_H
$g^5 = g^3 + g^2 = g^2 + g + I$	111	7_H
$g^6 = g^3 + g^2 + g = g^2 + I$	101	5_H
$g^7 = g^3 + g = I$	001	1_H

6×6 boyutundaki ikili matrisler, 3×3 boyutundaki devirli matris grup elemanlarının 2×2 Hadamard matris elemanları ile yer değiştirilmesiyle, 12×12 boyutundaki ikili matrisler ise yine 3×3 boyutundaki devirli matris grup elemanlarının 4×4 Hadamard matris elemanları ile yer değiştirilmesiyle üretilebilmektedirler. Üretilen bu matrislerden iyi kriptografik özelliklere sahip olanlar MAGMA yazılımı yardımıyla elde edilmektedir.

4.1. 3×3 Boyutundaki Devirli Matris Grupları ile 6×6 Boyutunda İkili Matrislerin Elde Edilmesi

6×6 boyutundaki ikili matrisler, Tablo 4.1'de gösterilmiş olan 3×3 boyutundaki devirli matris gruplarının elemanları kullanılarak elde edilebilmektedir. Bu bölümde 2×2 boyutunda Hadamard matrisler ve 3×3 boyutunda devirli matris grup elemanları kullanılarak elde edilen 6×6 boyutunda kriptografik özellikleri iyi ikili matrislerin örneklerle gösterimi yapılmaktadır. Not edilmelidir ki; çalışma esnasında 6×6 boyutunda kriptografik özellikleri iyi ikili matrisler elde edilirken tüm 2×2 boyutundaki matrisler ile 3×3 boyutundaki devirli grup elemanları kullanılarak 6×6 boyutunda matrislere dönüştürülmüş ve deneysel sonuçlar elde edilmiştir.

Örnek 4.1. 3×3 boyutundaki $g = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ üreteç bir ikili matris ve I 3×3 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 4.3'te verildiği gibi elde edilebilir.

Tablo 4.3. 001-011-111 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$	4_H
$g^3 = g + I$	$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$	3_H
$g^4 = g^2 + g$	$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$	6_H
$g^5 = g^3 + g^2 = g^2 + g + I$	$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$	7_H
$g^6 = g^3 + g^2 + g = g^2 + I$	$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	5_H
$g^7 = g^3 + g = I$	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	1_H

a ve b bu grubun herhangi bir elemanını ve dolayısıyla 3×3 boyutunda ikili matrisleri temsil etmek üzere, 2×2 boyutunda $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ Hadamard matrisinde bu elemanların yerine konmasıyla 6×6 boyutunda ikili matrisler elde edilebilmektedir.

Tablo 4.3'te verilen grup elemanları kullanılarak; $\begin{bmatrix} g & g^3 \\ g^3 & g \end{bmatrix}$ veya elemanları $\mathbb{F}_{2^3}$'ten olan (onaltılık gösterimle) 2×2 boyutunda $\begin{bmatrix} 2_H & 3_H \\ 3_H & 2_H \end{bmatrix}$ matrisi, 6×6 boyutundaki ikili matris (M_1) haline getirilebilir.

$$M_1 = \begin{bmatrix} 2_H & 3_H \\ 3_H & 2_H \end{bmatrix} = \begin{bmatrix} g & g^3 \\ g^3 & g \end{bmatrix} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}$$

Elde edilen 6×6 boyutundaki ikili matris (M_1) involutif olup; dallanma sayısı 4, sabit nokta sayısı ise 2^3'tür. Elemanları $\mathbb{F}_{2^3}$'ten tüm 2×2 boyutundaki matrisler ve Tablo 4.3'te verilen devirli matris grubunun tüm elemanları dikkate alındığında ise, dallanma sayısı 4 olan, 114 adet 6×6 boyutunda ikili matris elde edilebildiği görülmüştür.

Örnek 4.2. 3×3 boyutundaki $g = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$ üreteç bir ikili matris ve I 3×3 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 4.4'te verildiği gibi elde edilebilir.

Tablo 4.4. 001-100-110 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix} 1 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 1 \end{bmatrix}$	4_H
$g^3 = g + I$	$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$	3_H
$g^4 = g^2 + g$	$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$	6_H
$g^5 = g^3 + g^2 = g^2 + g + I$	$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$	7_H
$g^6 = g^3 + g^2 + g = g^2 + I$	$\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \end{bmatrix}$	5_H
$g^7 = g^3 + g = I$	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	1_H

Tablo 4.4'te verilen grup elemanları kullanılarak; $\begin{bmatrix} g^2 & g^6 \\ g^6 & g^2 \end{bmatrix}$ veya elemanları $\mathbb{F}_{2^3}$'ten olan (onaltılık gösterimle) 2×2 boyutunda $\begin{bmatrix} 4_H & 5_H \\ 5_H & 4_H \end{bmatrix}$ matrisi, 6×6 boyutundaki ikili matris (M_2) haline getirilebilir.

$$M_2 = \begin{bmatrix} 4_H & 5_H \\ 5_H & 4_H \end{bmatrix} = \begin{bmatrix} g^2 & g^6 \\ g^6 & g^2 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Elde edilen 6×6 boyutundaki ikili matris (M_2) involutif olup; dallanma sayısı 4, sabit nokta sayısı ise 2^3'tür. Elemanları $\mathbb{F}_{2^3}$'ten tüm 2×2 boyutundaki matrisler ve Tablo 4.4'te verilen devirli matris grubunun tüm elemanları dikkate alındığında ise, dallanma sayısı 4 olan, 186 adet 6×6 boyutunda ikili matris elde edilebildiği görülmüştür.

Örnek 4.3. 3×3 boyutundaki $g = \begin{bmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{bmatrix}$ üreteç bir ikili matris ve I 3×3 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 4.5'te verildiği gibi elde edilebilir.

Tablo 4.5. 001-110-011 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix}0 & 0 & 1\\1 & 1 & 0\\0 & 1 & 1\end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix}0 & 1 & 1\\1 & 1 & 1\\1 & 0 & 1\end{bmatrix}$	4_H
$g^3 = g + I$	$\begin{bmatrix}1 & 0 & 1\\1 & 0 & 0\\0 & 1 & 0\end{bmatrix}$	3_H
$g^4 = g^2 + g$	$\begin{bmatrix}0 & 1 & 0\\0 & 0 & 1\\1 & 1 & 0\end{bmatrix}$	6_H
$g^5 = g^3 + g^2 = g^2 + g + I$	$\begin{bmatrix}1 & 1 & 0\\0 & 1 & 1\\1 & 1 & 1\end{bmatrix}$	7_H
$g^6 = g^3 + g^2 + g = g^2 + I$	$\begin{bmatrix}1 & 1 & 1\\1 & 0 & 1\\1 & 0 & 0\end{bmatrix}$	5_H
$g^7 = g^3 + g = I$	$\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$	1_H

Tablo 4.5'te verilen grup elemanları kullanılarak; $\begin{bmatrix}g & g^3\\g^3 & g\end{bmatrix}$ veya elemanları $\mathbb{F}_{2^3}$'ten olan (onaltılık gösterimle) 2×2 boyutunda $\begin{bmatrix}2_H & 3_H\\2_H & 2_H\end{bmatrix}$ matrisi, 6×6 boyutundaki ikili matris (M_3) haline getirilebilir.

$$M_3 = \begin{bmatrix}2_H & 3_H\\2_H & 2_H\end{bmatrix} = \begin{bmatrix}g & g^3\\g^3 & g\end{bmatrix} = \begin{bmatrix}0 & 0 & 1 & 1 & 0 & 1\\1 & 1 & 0 & 1 & 0 & 0\\0 & 1 & 1 & 0 & 1 & 0\\1 & 0 & 1 & 0 & 0 & 1\\1 & 0 & 0 & 1 & 1 & 0\\0 & 1 & 0 & 0 & 1 & 1\end{bmatrix}$$

Elde edilen 6×6 boyutundaki ikili matris (M_3) involutif olup; dallanma sayısı 4, sabit nokta sayısı ise 2^3'tür. Elemanları $\mathbb{F}_{2^3}$'ten tüm 2×2 boyutundaki matrisler ve Tablo 4.5'te verilen devirli matris grubunun tüm elemanları dikkate alındığında ise, dallanma sayısı 4 olan, 186 adet 6×6 boyutunda ikili matris elde edilebildiği görülmüştür.

Örnek 4.4. 3×3 boyutundaki $g = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$ üreteç bir ikili matris ve I 3×3 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 4.6'da verildiği gibi elde edilebilir.

Tablo 4.6. 010-101-100 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$	4_H
$g^3 = g + I$	$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$	3_H
$g^4 = g^2 + g$	$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$	6_H
$g^5 = g^3 + g^2 = g^2 + g + I$	$\begin{bmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$	7_H
$g^6 = g^3 + g^2 + g = g^2 + I$	$\begin{bmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{bmatrix}$	5_H
$g^7 = g^3 + g = I$	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	1_H

Tablo 4.6'da verilen grup elemanları kullanılarak; $\begin{bmatrix} g^2 & g^6 \\ g^6 & g^2 \end{bmatrix}$ veya elemanları $\mathbb{F}_{2^3}$'ten olan (onaltılık gösterimle) 2×2 boyutunda $\begin{bmatrix} 4_H & 5_H \\ 5_H & 4_H \end{bmatrix}$ matrisi, 6×6 boyutundaki ikili matris (M_4) haline getirilebilir.

$$M_4 = \begin{bmatrix} 4_H & 5_H \\ 5_H & 4_H \end{bmatrix} = \begin{bmatrix} g^2 & g^6 \\ g^6 & g^2 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

Elde edilen 6×6 boyutundaki ikili matris (M_4) involutif olup; dallanma sayısı 4, sabit nokta sayısı ise 2^3'tür. Elemanları $\mathbb{F}_{2^3}$'ten tüm 2×2 boyutundaki matrisler ve Tablo 4.6'da verilen devirli matris grubunun tüm elemanları dikkate alındığında ise, dallanma sayısı 4 olan, 186 adet 6×6 boyutunda ikili matris elde edilebildiği görülmüştür.

Örnek 4.5. 3×3 boyutundaki $g = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ üreteç bir ikili matris ve I 3×3 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 4.7'de verildiği gibi elde edilebilir.

Tablo 4.7. 010-111-011 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	4_H
$g^3 = g + I$	$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$	3_H
$g^4 = g^2 + g$	$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$	6_H
$g^5 = g^3 + g^2 = g^2 + g + I$	$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$	7_H
$g^6 = g^3 + g^2 + g = g^2 + I$	$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$	5_H
$g^7 = g^3 + g = I$	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	1_H

Tablo 4.7'de verilen grup elemanları kullanılarak; $\begin{bmatrix} g & g^6 \\ g^6 & g \end{bmatrix}$ veya elemanları $\mathbb{F}_{2^3}$'ten olan (onaltılık gösterimle) 2×2 boyutunda $\begin{bmatrix} 2_H & 5_H \\ 5_H & 2_H \end{bmatrix}$ matrisi, 6×6 boyutundaki ikili matris (M_5) haline getirilebilir.

$$M_5 = \begin{bmatrix} 2_H & 5_H \\ 5_H & 2_H \end{bmatrix} = \begin{bmatrix} g & g^6 \\ g^6 & g \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

Elde edilen 6×6 boyutundaki ikili matris (M_5) involutif değildir; dallanma sayısı 4, sabit nokta sayısı ise 1'dir. Elemanları $\mathbb{F}_{2^3}$'ten tüm 2×2 boyutundaki matrisler ve Tablo 4.7'de verilen devirli matris grubunun tüm elemanları dikkate alındığında ise, dallanma sayısı 4 olan, 114 adet 6×6 boyutunda ikili matris elde edilebildiği görülmüştür.

4.2. 3×3 Boyutundaki Devirli Matris Grupları ile 12×12 Boyutunda İkili Matrislerin Elde Edilmesi

Bu bölümde 4×4 boyutunda Hadamard matrisler ve 3×3 boyutunda devirli matris grup elemanları kullanılarak elde edilen 12×12 boyutunda kriptografik özellikleri iyi ikili matrislerin örneklerle gösterimi yapılmaktadır. 12×12 boyutundaki ikili matrisler, Tablo 4.1'de gösterilmiş olan 3×3 boyutundaki grubun, 001-011-111 ve 010-111-011 üreteç elemanları kullanılarak üretilen devirli matris grupları ile elde edilmektedirler. Not edilmelidir ki; çalışma esnasında 12×12 boyutunda kriptografik özellikleri iyi ikili matrisler elde edilirken tüm 4×4 boyutundaki matrisler ile 3×3 boyutundaki devirli grup elemanları kullanılarak 12×12 boyutunda matrislere dönüştürülmüş ve deneysel sonuçlar elde edilmiştir.

Örnek 4.6. 3×3 boyutundaki $g = \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ üreteç bir ikili matris ve I 3×3 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 4.8'de verildiği gibi elde edilebilir.

Tablo 4.8. 001-011-111 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \end{bmatrix}$	4_H
$g^3 = g + I$	$\begin{bmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{bmatrix}$	3_H
$g^4 = g^2 + g$	$\begin{bmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 0 \end{bmatrix}$	6_H
$g^5 = g^3 + g^2 = g^2 + g + I$	$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$	7_H
$g^6 = g^3 + g^2 + g = g^2 + I$	$\begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}$	5_H
$g^7 = g^3 + g = I$	$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$	1_H

$a, b, c\ ve\ d$ grubun herhangi bir elemanını ve dolayısıyla 3×3 boyutunda ikili matrisleri temsil etmek üzere, 4×4 boyutunda $\begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}$ Hadamard matrisinde bu elemanların yerine konmasıyla 12×12 boyutunda ikili matrisler elde edilebilmektedir.

Örnek olarak; 4×4 boyutunda $had(1_H, 2_H, 4_H, 6_H) = had(I, g, g^2, g^4)$ matrisi Tablo 4.8'de verilen grup elemanları kullanılarak 12×12 boyutunda ikili matris (M_6) haline getirilebilir.

$$M_6 = had(1_H, 2_H, 4_H, 6_H) = \begin{bmatrix} 1_H & 2_H & 4_H & 6_H \\ 2_H & 1_H & 6_H & 4_H \\ 4_H & 6_H & 1_H & 2_H \\ 6_H & 4_H & 2_H & 1_H \end{bmatrix} = \begin{bmatrix} I & g & g^2 & g^4 \\ g & I & g^4 & g^2 \\ g^2 & g^4 & I & g \\ g^4 & g^2 & g & I \end{bmatrix}$$

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

Elde edilen 12×12 boyutundaki ikili matris (M_6) involutif olup, dallanma sayısı 8, sabit nokta sayısı ise 2^6'dır. Ayrıca, $G_{12\times 24} = [I|M_6]$ I, 12×12 boyutunda birim matris ve M_6, 12×12 boyutunda yukarıda verilen ikili matris olmak üzere $[24, 12, 8]$ kodu oluşturur ve bu kod genişletilmiş ikili Golay kod özelliklerini sağlamaktadır.

Örnek 4.7. 3×3 boyutundaki $g = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ üreteç bir ikili matris ve I, 3×3 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 4.9'da verildiği gibi elde edilebilir.

Tablo 4.9. 010-111-011 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix}0 & 1 & 0\\1 & 1 & 1\\0 & 1 & 1\end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix}1 & 1 & 1\\1 & 1 & 0\\1 & 0 & 0\end{bmatrix}$	4_H
$g^3 = g + I$	$\begin{bmatrix}1 & 1 & 0\\1 & 0 & 1\\0 & 1 & 0\end{bmatrix}$	3_H
$g^4 = g^2 + g$	$\begin{bmatrix}1 & 0 & 1\\0 & 0 & 1\\1 & 1 & 1\end{bmatrix}$	6_H
$g^5 = g^3 + g^2 = g^2 + g + I$	$\begin{bmatrix}0 & 0 & 1\\0 & 1 & 1\\1 & 1 & 0\end{bmatrix}$	7_H
$g^6 = g^3 + g^2 + g = g^2 + I$	$\begin{bmatrix}0 & 1 & 1\\1 & 0 & 0\\1 & 0 & 1\end{bmatrix}$	5_H
$g^7 = g^3 + g = I$	$\begin{bmatrix}1 & 0 & 0\\0 & 1 & 0\\0 & 0 & 1\end{bmatrix}$	1_H

Örnek olarak; 4×4 boyutunda $had(1_H, 2_H, 4_H, 6_H) = had(I, g, g^2, g^4)$ matrisi Tablo 4.9'da verilen grup elemanları kullanılarak 12×12 boyutunda ikili matris (M_7) haline getirilebilir.

$$M_7 = had(1_H, 2_H, 4_H, 6_H) = \begin{bmatrix}1_H & 2_H & 4_H & 6_H\\2_H & 1_H & 6_H & 4_H\\4_H & 6_H & 1_H & 2_H\\6_H & 4_H & 2_H & 1_H\end{bmatrix} = \begin{bmatrix}I & g & g^2 & g^4\\g & I & g^4 & g^2\\g^2 & g^4 & I & g\\g^4 & g^2 & g & I\end{bmatrix}$$

$$M_7 = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

Elde edilen 12×12 boyutundaki ikili matris (M_7) involutif olup, dallanma sayısı 8, sabit nokta sayısı ise 2^6'dır. Ayrıca bu ikili matriste, Örnek 4.6'da verilen M_6 ikili matrisi ile benzer şekilde $G_{12\times 24} = [I|M_7]$ I, 12×12 boyutunda birim matris ve M_7, 12×12 boyutunda yukarıda verilen ikili matris olmak üzere $[24, 12, 8]$ kodu oluşturur ve bu kod genişletilmiş ikili Golay kod özelliklerini sağlamaktadır. Önerilen yöntem ile bahsi geçen Golay kod özeliklerini sağlayan, 48 adet 12×12 boyutunda ikili matris elde edilmiştir.

BÖLÜM 5

4×4 BOYUTUNDA DEVİRLİ MATRİS GRUPLARI

Tezin bu bölümü, 4×4 boyutundaki devirli matris grupları kullanılarak 8×8, 16×16 ve 32×32 boyutlarında, maksimum dallanma sayısı ile minimum sabit nokta sayısına sahip ikili matrislerin elde edilmesiyle ilgili örnek ve açıklamaları içermektedir.

Tezin üçüncü bölümünde de bahsedildiği gibi 4×4 ikili matris uzayında tüm 4×4 ikili matrisler taranarak 336 adet devirli (cyclic) matris grubu (g, 4×4 boyutunda ikili bir matris ve $g^4 = g + I$ olmak üzere $g^{15} = I$ olacak şekilde) elde edilmiştir. Bu elde edilen gruplardan, iyi kriptografik özelliklere sahip 8×8 boyutunda ikili matrisler üretilmesini sağlayan, 72 grubun 36 tanesi, Tablo 5.1'de verilmektedir. Diğer 36 grup, Tablo 5.1'de verilen grupların transpozları olup aynı sonuçları ürettiklerinden tabloya dahil edilmemiştir. Verilen tabloda örneğin 0100-1001-0110-0011, 4×4 boyutunda grubun $\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ şeklinde ikili bir üreteç matrisini temsil etmektedir. 16×16 boyutunda ise 336 devirli matris grubunun 216 tanesinin, iyi kriptografik özelliklere sahip matrislerin elde edilmesinde başarılı olduğu gözlenmiştir.

Tablo 5.1. 4×4 Boyutunda Devirli Matris Grupları

0100-1001-0110-0011	0100-0001-1100-0010	0001-0011-1111-0111
0001-0101-0110-1010	0001-0010-1000-0110	0110-1111-1110-0010
1001-0001-1010-0110	0001-0010-1001-0100	1111-1010-1110-0010
1001-0010-1100-0011	0010-1000-0001-1100	1111-1110-1100-0100
1001-1100-0001-0110	0001-1000-0100-0110	0001-1111-0101-0111
0010-0110-1001-0101	0001-1000-1100-0010	0101-1111-0001-1101
1001-1010-0100-0101	0001-1001-0100-0010	1111-1001-0001-1101
1010-1100-0101-0010	0100-0001-1000-1010	1111-1101-0100-1100
1010-1001-0110-0100	0001-1010-1000-0100	0010-1111-0111-0110
0101-1000-1010-0011	0010-1000-0101-0100	0011-0001-1111-1011
0011-1100-0110-1000	0010-1001-0100-1000	1011-1000-1001-1111
0011-1100-1000-0101	0100-0010-1001-1000	1011-1000-1111-1010

g, $f(x) = x^4 + x + 1$ indirgenemez polinomunun bir kökü ve $g^{15} = I$ olmak üzere 4×4 boyutunda üreteç bir ikili matris olarak düşünüldüğünde, üretilecek devirli grup $\mathbb{F}_{2^4}^*$ cismi ile izomorf olduğundan, grubun elemanları onaltılık gösterimle Tablo 5.2'de verildiği gibi yazılabilmektedir.

Tablo 5.2. Grup Elemanlarının İkilik ve Onaltılık Notasyonda Gösterimi

$g^1 = g$	0010	2_H
$g^2 = g^2$	0100	4_H
$g^3 = g^3$	1000	8_H
$g^4 = g + I$	0011	3_H
$g^5 = g^2 + g$	0110	6_H
$g^6 = g^3 + g^2$	1100	C_H
$g^7 = g^3 + g + I$	1011	B_H
$g^8 = g^2 + I$	0101	5_H
$g^9 = g^3 + g$	1010	A_H
$g^{10} = g^4 + g^2 = g^2 + g + I$	0111	7_H
$g^{11} = g^3 + g^2 + g$	1110	E_H
$g^{12} = g^4 + g^3 + g^2 = g^3 + g^2 + g + I$	1111	F_H
$g^{13} = g^4 + g^3 + g^2 + g = g^3 + g^2 + I$	1101	D_H
$g^{14} = g^4 + g^3 + g = g^3 + I$	1001	9_H
$g^{15} = g^4 + g = I$	0001	1_H

8×8 boyutundaki ikili matrisler, 4×4 boyutundaki devirli matris grup elemanlarının 2×2 Hadamard matris elemanları ($\mathbb{F}_{2^4}$'ten elemanlar) ile yer değiştirilmesiyle, 16×16 boyutundaki ikili matrisler 4×4 boyutundaki devirli matris grup elemanlarının 4×4 Hadamard matris elemanları ($\mathbb{F}_{2^4}$'ten elemanlar) ile yer değiştirilmesiyle üretilebilmektedirler. 32×32 boyutundaki ikili matrisler ise 4×4 boyutundaki devirli matris grup elemanlarının 8×8 Hadamard matris elemanları ($\mathbb{F}_{2^4}$'ten elemanlar) ile yer değiştirilmesiyle üretilebilmektedir. Üretilen bu matrislerden iyi kriptografik özelliklere sahip olanlar, MAGMA yazılımı yardımıyla elde edilmektedir.

5.1. Elemanları $\mathbb{F}_{2^4}$'ten Olan 2×2 Boyutundaki Hadamard Matrisler ve 4×4 Boyutundaki Devirli Matris Grupları ile 8×8 Boyutunda İkili Matrislerin Elde Edilmesi

8×8 boyutundaki ikili matrisler, Tablo 5.1'de gösterilmiş olan 4×4 boyutundaki devirli matris gruplarının elemanları kullanılarak elde edilebilmektedir. Bu bölümde 2×2 boyutunda Hadamard matrisler ve 4×4 boyutunda devirli matris grup elemanları kullanılarak elde edilen 8×8 boyutunda kriptografik özellikleri iyi ikili matrislerin örneklerle gösterimi yapılmaktadır. Not edilmelidir ki; çalışma esnasında 8×8 boyutunda kriptografik özellikleri iyi ikili matrisler elde edilirken tüm 2×2 boyutundaki matrisler ile 4×4 boyutundaki devirli grup elemanları kullanılarak 8×8 boyutunda matrislere dönüştürülmüş ve deneysel sonuçlar elde edilmiştir.

Örnek 5.1. 4×4 boyutundaki $g = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ üreteç bir ikili matris ve I, 4×4 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 5.3'de verildiği gibi elde edilebilir.

Tablo 5.3. 0100-1001-0110-0011 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{bmatrix}$	4_H
$g^3 = g^3$	$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$	8_H
$g^4 = g + I$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	3_H

$g^5 = g^2 + g$	$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$	6_H
$g^6 = g^3 + g^2$	$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	C_H
$g^7 = g^3 + g + I$	$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$	B_H
$g^8 = g^2 + I$	$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \end{bmatrix}$	5_H
$g^9 = g^3 + g$	$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$	A_H
$g^{10} = g^4 + g^2 = g^2 + g + I$	$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$	7_H
$g^{11} = g^3 + g^2 + g$	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	E_H
$g^{12} = g^4 + g^3 + g^2 = g^3 + g^2 + g + I$	$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \end{bmatrix}$	F_H
$g^{13} = g^4 + g^3 + g^2 + g = g^3 + g^2 + I$	$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$	D_H
$g^{14} = g^4 + g^3 + g = g^3 + I$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$	9_H
$g^{15} = g^4 + g = I$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1_H

$a\ ve\ b$, bu grubun elemanlarını ve dolayısıyla 4×4 boyutunda ikili matrisleri temsil etmek üzere, 2×2 boyutunda $\begin{bmatrix} a & b \\ b & a \end{bmatrix}$ Hadamard matrisinde bu elemanların yerine konmasıyla 8×8 boyutunda ikili matrisler elde edilebilmektedir.

Tablo 5.3'de verilen grup elemanları kullanılarak; $\begin{bmatrix} I & g^6 \\ g^6 & I \end{bmatrix}$ veya elemanları $\mathbb{F}_{2^4}$'ten olan (onaltılık gösterimle) 2×2 boyutunda $\begin{bmatrix} 1_H & C_H \\ C_H & 1_H \end{bmatrix}$ matrisi, 8×8 boyutundaki ikili matris (M_8) haline getirilebilir.

$$M_8 = \begin{bmatrix} 1_H & C_H \\ C_H & 1_H \end{bmatrix} = \begin{bmatrix} I & g^6 \\ g^6 & I \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Elde edilen 8×8 boyutundaki ikili matris M_8'in dallanma sayısı 5, sabit nokta sayısı ise 1 olup; ikili matris involutif değildir ($M_8 \neq M_8^{-1}$).

Örnek 5.2. 4×4 boyutundaki $g = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}$ üreteç bir ikili matris ve I, 4×4 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 5.4'te verildiği gibi elde edilebilir.

Tablo 5.4. 1100-1101-0100-0010 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix}1 & 1 & 0 & 0\\ 1 & 1 & 0 & 1\\ 0 & 1 & 0 & 0\\ 0 & 0 & 1 & 0\end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix}0 & 0 & 0 & 1\\ 0 & 0 & 1 & 1\\ 1 & 1 & 0 & 1\\ 0 & 1 & 0 & 0\end{bmatrix}$	4_H
$g^3 = g^3$	$\begin{bmatrix}0 & 0 & 1 & 0\\ 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 1\\ 1 & 1 & 0 & 1\end{bmatrix}$	8_H
$g^4 = g + I$	$\begin{bmatrix}0 & 1 & 0 & 0\\ 1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 1\end{bmatrix}$	3_H
$g^5 = g^2 + g$	$\begin{bmatrix}1 & 1 & 0 & 1\\ 1 & 1 & 1 & 0\\ 1 & 0 & 0 & 1\\ 0 & 1 & 1 & 0\end{bmatrix}$	6_H
$g^6 = g^3 + g^2$	$\begin{bmatrix}0 & 0 & 1 & 1\\ 0 & 1 & 0 & 1\\ 1 & 1 & 1 & 0\\ 1 & 0 & 0 & 1\end{bmatrix}$	C_H
$g^7 = g^3 + g + I$	$\begin{bmatrix}0 & 1 & 1 & 0\\ 1 & 1 & 1 & 1\\ 0 & 1 & 0 & 1\\ 1 & 1 & 1 & 0\end{bmatrix}$	B_H
$g^8 = g^2 + I$	$\begin{bmatrix}1 & 0 & 0 & 1\\ 0 & 1 & 1 & 1\\ 1 & 1 & 1 & 1\\ 0 & 1 & 0 & 1\end{bmatrix}$	5_H
$g^9 = g^3 + g$	$\begin{bmatrix}1 & 1 & 1 & 0\\ 1 & 0 & 1 & 1\\ 0 & 1 & 1 & 1\\ 1 & 1 & 1 & 1\end{bmatrix}$	A_H
$g^{10} = g^4 + g^2 = g^2 + g + I$	$\begin{bmatrix}0 & 1 & 0 & 1\\ 1 & 0 & 1 & 0\\ 1 & 0 & 1 & 1\\ 0 & 1 & 1 & 1\end{bmatrix}$	7_H

$g^{11} = g^3 + g^2 + g$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{bmatrix}$	E_H
$g^{12} = g^4 + g^3 + g^2 = g^3 + g^2 + g + I$	$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$	F_H
$g^{13} = g^4 + g^3 + g^2 + g = g^3 + g^2 + I$	$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$	D_H
$g^{14} = g^4 + g^3 + g = g^3 + I$	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	9_H
$g^{15} = g^4 + g = I$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1_H

Tablo 5.4'te verilen grup elemanları kullanılarak; $\begin{bmatrix} I & g^9 \\ g^9 & I \end{bmatrix}$ veya elemanları $\mathbb{F}_{2^4}$'ten olan (onaltılık gösterimle) 2×2 boyutunda $\begin{bmatrix} 1_H & A_H \\ A_H & 1_H \end{bmatrix}$ matrisi, 8×8 boyutundaki ikili matris (M_9) haline getirilebilir.

$$M_9 = \begin{bmatrix} 1_H & A_H \\ A_H & 1_H \end{bmatrix} = \begin{bmatrix} I & g^9 \\ g^9 & I \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Elde edilen 8×8 boyutundaki ikili matris M_9'un dallanma sayısı 5, sabit nokta sayısı ise 1 olup; ikili matris involutif değildir ($M_9 \neq M_9^{-1}$).

Bu bölümde iki örneği verilen 8×8 boyutundaki ikili matrislerle ilgili tüm deneysel sonuçlar ve ilave bilgiler tezin EK – A bölümünde verilmiştir.

5.2. Elemanları $\mathbb{F}_{2^4}$'ten Olan 4×4 Boyutundaki Hadamard Matrisler ve 4×4 Boyutundaki Devirli Matris Grupları ile 16×16 Boyutunda İkili Matrislerin Elde Edilmesi

16×16 boyutundaki ikili matrisler, tezin EK – B bölümünde detaylı bilgileri verilmiş olan, 4×4 boyutundaki 216 adet devirli matris grubunun elemanları kullanılarak elde edilebilmektedir.

Bu bölümde 4×4 boyutunda Hadamard matrisler ve 4×4 boyutunda devirli matris grup elemanları kullanılarak elde edilen 16×16 boyutunda kriptografik özellikleri iyi ikili matrislerin örneklerle gösterimi yapılmaktadır. Not edilmelidir ki; çalışma esnasında 16×16 boyutunda kriptografik özellikleri iyi ikili matrisler elde edilirken tüm 4×4 boyutundaki matrisler ile 4×4 boyutundaki devirli grup elemanları kullanılarak 16×16 boyutunda matrislere dönüştürülmüş ve deneysel sonuçlar elde edilmiştir.

Örnek 5.3. 4×4 boyutundaki $g = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$ üreteç bir ikili matris ve I, 4×4 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 5.5'te verildiği gibi elde edilebilir.

Tablo 5.5. 0001-0110-0101-1011 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	4_H
$g^3 = g^3$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$	8_H
$g^4 = g + I$	$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$	3_H
$g^5 = g^2 + g$	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$	6_H
$g^6 = g^3 + g^2$	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$	C_H
$g^7 = g^3 + g + I$	$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$	B_H
$g^8 = g^2 + I$	$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$	5_H
$g^9 = g^3 + g$	$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	A_H
$g^{10} = g^4 + g^2 = g^2 + g + I$	$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$	7_H

$g^{11} = g^3 + g^2 + g$	$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$	E_H
$g^{12} = g^4 + g^3 + g^2 = g^3 + g^2 + g + I$	$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	F_H
$g^{13} = g^4 + g^3 + g^2 + g = g^3 + g^2 + I$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$	D_H
$g^{14} = g^4 + g^3 + g = g^3 + I$	$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$	9_H
$g^{15} = g^4 + g = I$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1_H

$a, b, c\ ve\ d$ bu grubun herhangi bir elemanını ve dolayısıyla 4×4 boyutunda ikili matrisleri temsil etmek üzere, 4×4 boyutunda $\begin{bmatrix} a & b & c & d \\ b & a & d & c \\ c & d & a & b \\ d & c & b & a \end{bmatrix}$ Hadamard matrisinde bu elemanların yerine konmasıyla 16×16 boyutunda ikili matrisler elde edilebilmektedir.

Tablo 5.5'te verilen grup elemanları kullanılarak; 4×4 boyutunda $had(1_H, 6_H, B_H, D_H) = had(I, g^5, g^7, g^{13})$ matrisi 16×16 boyutunda ikili matris (M_{10}) haline getirilebilir.

$$had(1_H, 6_H, B_H, D_H) = \begin{bmatrix} 1_H & 6_H & B_H & D_H \\ 6_H & 1_H & D_H & B_H \\ B_H & D_H & 1_H & 6_H \\ D_H & B_H & 6_H & 1_H \end{bmatrix} = \begin{bmatrix} I & g^5 & g^7 & g^{13} \\ g^5 & I & g^{13} & g^7 \\ g^7 & g^{13} & I & g^5 \\ g^{13} & g^7 & g^5 & I \end{bmatrix}$$

$$M_{10} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

Elde edilen 16×16 boyutundaki ikili matris (M_{10}) involutif olup, dallanma sayısı 8, sabit nokta sayısı ise 2^8'dir.

Açıklama 5.1. Yukarıdaki örnekte verilen 16×16 boyutundaki M_{10} ikili matrisi, ARIA [11] blok şifresinde difüzyon katmanı olarak kullanılan ve 2^9 adet sabit nokta içeren 16×16 boyutundaki involutif ikili matristen daha iyi uygulama özelliğine (52 XOR) sahiptir ve 2^8 adet sabit nokta içermektedir. Uygulama detayları tezin EK – C bölümünde verilmiştir.

5.3. Elemanları $\mathbb{F}_{2^4}$'ten Olan 4×4 Boyutundaki Dairesel Matrisler ve 4×4 Boyutundaki Devirli Matris Grupları ile 16×16 Boyutunda İkili Matrislerin Elde Edilmesi

Bu tez çalışmasında her ne kadar Hadamard matrislere yoğunlaşılmış olsa da $n = m.k$ olmak üzere, $m \times m$ boyutunda Dairesel (Circulant) matrisler ve $k \times k$ boyutunda devirli matris grupları kullanılarak da $n \times n$ boyutunda, kriptografik özellikleri iyi ikili matrislerin elde edilmesi mümkündür.

Örnek 5.4. 4×4 boyutundaki $g = \begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$ üreteç bir ikili matris ve I, 4×4 boyutunda birim matris olmak üzere elde edilen gruptan faydalanılarak, AES [19] blok şifresinde de yayılım katmanı olarak kullanılan ve $\mathbb{F}_{2^4}[x]/(x^4 + x^3 + 1)$ üzerinde tanımlı $circ(2_H, 3_H, 1_H, 1_H) = circ(g, g^{12}, I, I)$ matrisi, 16×16 boyutunda ikili matris (M_{11}) haline getirilebilir.

$$circ(2_H, 3_H, 1_H, 1_H) = \begin{bmatrix} 2_H & 3_H & 1_H & 1_H \\ 1_H & 2_H & 3_H & 1_H \\ 1_H & 1_H & 2_H & 3_H \\ 3_H & 1_H & 1_H & 2_H \end{bmatrix} = \begin{bmatrix} g & g^{12} & I & I \\ I & g & g^{12} & I \\ I & I & g & g^{12} \\ g^{12} & I & I & g \end{bmatrix}$$

$$M_{11} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \end{bmatrix}$$

Elde edilen 16×16 boyutundaki ikili matris (M_{11}) involutif değildir ($M_{11} \neq M_{11}^{-1}$) ve dallanma sayısı 8'dir.

5.4. Elemanları $\mathbb{F}_{2^4}$'ten Olan 8×8 Boyutundaki Hadamard Matrisler ve 4×4 Boyutundaki Devirli Matris Grupları ile 32×32 Boyutunda İkili Matrislerin Elde Edilmesi

Önerilen yöntem $n > 16$ olduğu durumlarda da $n \times n$ boyutunda ikili matrislerin üretilmesi için kullanılabilmektedir. Örneğin; 32×32 boyutunda ikili matrisler, 4×4 boyutunda devirli matris grupları ve $\mathbb{F}_{2^4}[x]/(x^4 + x + 1)$ üzerinde tanımlı 8×8 boyutunda Hadamard matrisler kullanılarak elde edilebilmektedir.

Örnek 5.5. 4×4 boyutundaki $g = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$ üreteç bir ikili matris ve I, 4×4 boyutunda birim matris olmak üzere, devirli matris grubunun diğer elemanları Tablo 5.6'da verildiği gibi elde edilebilir.

Tablo 5.6. 0001-0011-0110-1101 Üreteç Elemanı ile Elde Edilen Devirli Matris Grubu

$g^1 = g$	$\begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$	2_H
$g^2 = g^2$	$\begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{bmatrix}$	4_H
$g^3 = g^3$	$\begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{bmatrix}$	8_H
$g^4 = g + I$	$\begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \end{bmatrix}$	3_H
$g^5 = g^2 + g$	$\begin{bmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$	6_H

$g^6 = g^3 + g^2$	$\begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix}$	C_H
$g^7 = g^3 + g + I$	$\begin{bmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{bmatrix}$	B_H
$g^8 = g^2 + I$	$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \end{bmatrix}$	5_H
$g^9 = g^3 + g$	$\begin{bmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$	A_H
$g^{10} = g^4 + g^2 = g^2 + g + I$	$\begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$	7_H
$g^{11} = g^3 + g^2 + g$	$\begin{bmatrix} 0 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$	E_H
$g^{12} = g^4 + g^3 + g^2 = g^3 + g^2 + g + I$	$\begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$	F_H
$g^{13} = g^4 + g^3 + g^2 + g = g^3 + g^2 + I$	$\begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$	D_H
$g^{14} = g^4 + g^3 + g = g^3 + I$	$\begin{bmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$	9_H
$g^{15} = g^4 + g = I$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}$	1_H

$a, b, c, d, e, f, g\ ve\ h$ bu grubun herhangi bir elemanını ve dolayısıyla 4×4 boyutunda ikili matrisleri temsil etmek üzere, 8×8 boyutunda

$$\begin{bmatrix} a & b & c & d & e & f & g & h \\ b & a & d & c & f & e & h & g \\ c & d & a & b & g & h & e & f \\ d & c & b & a & h & g & f & e \\ e & f & g & h & a & b & c & d \\ f & e & g & h & b & a & d & c \\ g & h & e & f & c & d & a & b \\ h & g & f & e & d & c & b & a \end{bmatrix}$$

bir Hadamard matrisinde bu elemanların yerine konmasıyla 32×32 boyutunda ikili matrisler elde edilebilmektedir.

Tablo 5.6'da verilen grup elemanları kullanılarak; 8×8 boyutunda $had(2_H, F_H, C_H, 5_H, A_H, 4_H, 8_H, 3_H) = had(g, g^{12}, g^6, g^8, g^9, g^2, g^3, g^4)$ matrisi [36], 32×32 boyutunda ikili matris (M_{12}) haline getirilebilir.

$$M_{12} = \begin{bmatrix} 2_H & F_H & C_H & 5_H & A_H & 4_H & 8_H & 3_H \\ F_H & 2_H & 5_H & C_H & 4_H & A_H & 3_H & 8_H \\ C_H & 5_H & 2_H & F_H & 8_H & 3_H & A_H & 4_H \\ 5_H & C_H & F_H & 2_H & 3_H & 8_H & 4_H & A_H \\ A_H & 4_H & 8_H & 3_H & 2_H & F_H & C_H & 5_H \\ 4_H & A_H & 3_H & 8_H & F_H & 2_H & 5_H & C_H \\ 8_H & 3_H & A_H & 4_H & C_H & 5_H & 2_H & F_H \\ 3_H & 8_H & 4_H & A_H & 5_H & C_H & F_H & 2_H \end{bmatrix}$$

$$= \begin{bmatrix} g & g^{12} & g^6 & g^8 & g^9 & g^2 & g^3 & g^4 \\ g^{12} & g & g^8 & g^6 & g^2 & g^9 & g^4 & g^3 \\ g^6 & g^8 & g & g^{12} & g^3 & g^4 & g^9 & g^2 \\ g^8 & g^6 & g^{12} & g & g^4 & g^3 & g^2 & g^9 \\ g^9 & g^2 & g^3 & g^4 & g & g^{12} & g^6 & g^8 \\ g^2 & g^9 & g^4 & g^3 & g^{12} & g & g^8 & g^6 \\ g^3 & g^4 & g^9 & g^2 & g^6 & g^8 & g & g^{12} \\ g^4 & g^3 & g^2 & g^9 & g^8 & g^6 & g^{12} & g \end{bmatrix}$$

Elde edilen 32×32 boyutundaki ikili matris (M_{12}) involutif olup, dallanma sayısı 12, sabit nokta sayısı ise 2^{16}'dır.

BÖLÜM 6

SONUÇ ve TARTIŞMA

Bu tez çalışmasında; 6×6, 8×8, 12×12, 16×16 ve 32×32 boyutlarında kriptografik ve uygulama özellikleri iyi olan ikili matrislerin üretilmesi için bir yöntem önerilmiştir.

3×3 ve 4×4 ikili matris uzayının tümü taranarak 3×3 boyutunda 8 adet, 4×4 boyutunda ise 336 adet devirli (cyclic) matris grubu elde edilmiştir. Önerilen yöntem ile elde edilen deneysel sonuçlar Tablo 6.1'de sunulmaktadır. Verilen tabloda *n* matris boyutunu, *k* kullanılan devirli matris grubunun boyutunu, *d* ise söz konusu boyutta elde edilen matrislerin maksimum dallanma sayısını göstermektedir. Ayrıca *s* maksimum dallanma sayısına (*d)* sahip *n*×*n* boyutunda matris sayısını, *i* maksimum dallanma sayısına sahip *n*×*n* boyutunda involutif matris sayısını, *l* ve *h* ise sırasıyla ikili matrislerin en düşük ve en yüksek Hamming ağırlığını temsil etmektedir. Matris sütunu istenilen özellikleri sahip birer örnek içermekte iken, XOR sütunu örneği verilen ikili matrisin uygulaması için gerekli olan en düşük XOR sayısına karşılık gelmektedir. Başarım sütunu ise maksimum dallanma sayısına sahip ikili matrislerin üretilebildiği devirli matris gruplarının sayısını vermektedir.

Tablo 6.1. Önerilen Yöntem ile Elde Edilen Deneysel Sonuçlar

n	***k***	***max(d)***	***d***	***s***	***i***	***l***	***h***	***XOR***	***Matris***	***Başarım***
6	3	4	4	1344	144	18	27	12	had(A^2,A^6)	8/8
8	4	5	5	2304	384	34	44	26	had(A^4, A^{10})	72/336
12	3	8	8	48	48	84	84	56	had(I,A,A^2,A^4)	2/8
16	4	8	8	67104	67104	112	176	52	had(I,A^5,A^7,A^{13})	216/336

Deneysel sonuçlardan da görülebileceği gibi 3×3 boyutundaki 8 devirli matris grubunun tamamı ile 6×6 boyutunda maksimum dallanma sayısı 4 olan ikili matrisler elde edilebilmekte iken, 8 devirli matris grubunun 2'si, 12×12 boyutunda maksimum dallanma sayısı 8 olan ikili matrislerin elde edilmesinde başarılıdır. 4×4 boyutundaki 336 devirli matris grubunun 72 tanesi, 8×8 boyutunda maksimum dallanma sayısı 5 olan ikili matrislerin elde edilmesini sağlarken, 336 devirli matris grubunun 216 tanesi ile 16×16 boyutunda maksimum dallanma sayısı 8 olan ikili matrisler elde edilebilmektedir. Elde edilen maksimum dallanma sayısına sahip 16×16 boyutundaki ikili matrislere ait detaylar ve bunlara karşılık gelen MDS yapıları ile ilgili bilgiler EK-B'de verilmektedir.

Açıklama 6.1. 12×12 boyutunda elde edilen ve maksimum dallanma sayısı 8 olan ikili matrisler, 12×12 boyutunda ikili birim matris ile birlikte genişletilmiş ikili Golay kodları (Extended Binary Golay Code) oluşturmaktadırlar.

Açıklama 6.2. Deneysel sonuçlar ayrıca, 4×4 boyutundaki 336 devirli matris grubunun 264 tanesinin, $\mathbb{F}_{2^4}$ cismi üzerinde tanımlı $x^4 + x + 1$ indirgenemez polinomu ve Bölüm 5 Örnek 5.5'de verilen 8×8 boyutunda involutif bir MDS matrisi kullanılarak, 32×32 boyutundaki dallanma sayısı 12 olan ikili matrislerin elde edilmesinde de başarılı olduğunu göstermektedir.

Tablo 6.2, ARIA blok şifresinde kullanılan 16×16 boyutundaki involutif ikili matris ile Bölüm 5 Örnek 5.3'de verilen aynı boyut ve dallanma sayısına sahip involutif ikili matrisin uygulama özeliklerinin karşılaştırılmasını içermektedir.

Tablo 6.2. M_{10} Matrisi ile ARIA'da kullanılan 16×16 İkili Matrislerin Karşılaştırılması

				Uygulama Maliyeti	
	Dallanma Sayısı	***M + I Rankı***	***İnvolutif***	***8-bit İşlemcilerde***	***32-bit İşlemcilerde***
M_{ARIA} [11]	8	7	Evet	60 XOR	19 XOR
M_{10} Matrisi (Bölüm 5-Örnek 5.3)	8	8	Evet	52 XOR	18 XOR

Tablo 6.3, literatürde bulunan 32×32 boyutundaki bazı matrislerin, Bölüm 5 Örnek 5.5'de verilen matrisle çeşitli kriptografik özellikleri açısından karşılaştırılmasını içermektedir.

Tablo 6.3. M_{12} Matrisi ile Literatürdeki Bazı 32×32 İkili Matrislerin Karşılaştırılması

	Dallanma Sayısı	***M + I Rankı***	***Involutif***
[33]	10	26	Hayır
[34]	12	16	Evet
M_{12} Matrisi (Bölüm 5-Örnek 5.5)	12	16	Evet

Sonuçlardan anlaşılabileceği gibi bu tez çalışmasında önerilen yöntemin; 6×6, 8×8, 12×12, 16×16 ve 32×32 boyutlarında kriptografik ve uygulama özellikleri iyi olan ikili matrislerin üretilmesi için başarılı olduğu görülmektedir.

Önerilen yöntem ile tasarlanan doğrusal dönüşümler; daha iyi yazılım uygulama özelliklerine sahip olmakla birlikte, maksimum dallanma sayısı özelliği sayesinde doğrusal ve diferansiyel kriptanaliz saldırılarına karşı dayanıklı blok şifrelerin tasarımında kullanılabilirler. Bunlara ek olarak, tasarlanan doğrusal dönüşümler minimum sabit nokta sayısı ve involutif olma gibi kriptografik açıdan beklenen özelliklere sahiptirler.

Yöntemin diğer bir avantajı; 10×10, 20×20, 24×24 ve $n \leq 32$ gibi farklı boyutlardaki matrisler için de uygulanabilir olmasıdır. Diğer yandan; bu tezde Hadamard formdaki matrisler üzerine yoğunlaşılmış olup, Hankel ve dairesel matrisler kullanılarak yöntem kolaylıkla genişletilebilir.

EK – A

8×8 BOYUTUNDA İKİLİ MATRİSLER

Bu bölüm; 4×4 boyutundaki devirli matris grupları kullanılarak elde edilen tüm 8×8 boyutundaki ikili matrislerin tablosunu içermektedir.

g üreteç matrisi, $f(x) = x^4 + x + 1$ indirgenemez polinomunun bir kökü ve 4×4 boyutunda bir ikili matris olarak düşünüldüğünde, $g^{15} = I$ olmak üzere üretilen devirli grubun elemanları onaltılık (hexadecimal) notasyonda elde edilmektedir. g üreteç matrisleri, 3 grup halinde Tablo A.1'de verilmektedir.

Tablo A.1. 4×4 Boyutundaki Üreteç Matrisler

1. Grup	***2. Grup***	***3. Grup***
1100-1101-0100-0010	0100-0001-1100-0010	0001-0011-1111-0111
1001-0001-0100-1011	0001-0010-1000-0110	0110-1111-1110-0010
0001-0101-1000-0111	0001-0010-1001-0100	1111-1010-1110-0010
0001-0110-1110-0010	0010-1000-0001-1100	1111-1110-1100-0100
0001-1000-0011-0111	0001-1000-0100-0110	0001-1111-0101-0111
1010-0010-1011-0100	0001-1000-1100-0010	0101-1111-0001-1101
0001-1110-0110-0100	0001-1001-0100-0010	1111-1001-0001-1101
0010-1000-0111-0011	0100-0001-1000-1010	1111-1101-0100-1100
0010-1101-0100-0101	0001-1010-1000-0100	0010-1111-0111-0110
1101-1100-1000-0010	0010-1000-0101-0100	0011-0001-1111-1011
1011-1000-0100-1001	0010-1001-0100-1000	1011-1000-1001-1111
1011-1000-1010-0100	0100-0010-1001-1000	1011-1000-1111-1010

Tablo A.1'de verilen üreteç matrisler kullanılarak 8×8 boyutundaki ikili matrisler elde edilmektedir. 1. Grup üreteç elemanları ile elde edilen 8×8 boyutundaki ikili matrisler Tablo A.2'de, 2. Grup üreteç elemanları ile elde edilen 8×8 boyutundaki ikili matrisler Tablo A.3'de, 3. Grup üreteç elemanları ile elde edilen 8×8 boyutundaki ikili matrisler ise Tablo A.4'de verilmektedir.

Tablo A.2, A.3 ve A.4'ün matris sütunları, 4×4 boyutundaki üreteç matrislerden elde edilen 8×8 boyutundaki ikili matrislerin onaltılık (hexadecimal) gösterimini içermektedir. Örneğin; Tablo A.2'deki (1-A-A-1) gösterimi, Tablo A.1'in 1. Grubunda bulunan 4×4 boyutundaki üreteç matrislerden elde edilen elemanların, $\begin{bmatrix} 1 & A \\ A & 1 \end{bmatrix} = \begin{bmatrix} 1 & g^9 \\ g^9 & 1 \end{bmatrix}$ şeklinde dizilmesiyle oluşturulan 8×8 boyutundaki ikili matrisi göstermektedir.

Tablo A.2, A.3 ve A.4'ün *w* ile ifade edilen Hamming ağırlığı sütunları, aynı satırda bulunan matrisin Hamming ağırlığını göstermekte, involutif sütunları ise o satırda bulunan matrisin, involutif olup olmadığını belirtmektedir. Ayrıca; tablolarda verilen tüm matrislerin hem diferansiyel hem de doğrusal dallanma sayıları 5 olup, söz konusu boyuttaki maksimum dallanma sayısına sahiptirler.

Tablo A.2. 1. Grupta Bulunan Üreteç Matrisler Kullanılarak Elde Edilen Maksimum Dallanma Sayısına Sahip 8×8 Boyutundaki İkili Matrisler

Matris	***Hamming Ağırlığı (w)***	***İnvolutif***
1-A-A-1	34	-
1-A-A-9	36	-
2-7-7-2	34	-
6-C-C-C	37	-
7-2-2-7	34	-
9-A-A-1	36	-
A-1-1-A	34	-
A-1-9-A	36	+
A-9-1-A	36	+
C-6-C-C	37	+
C-C-6-C	37	+
C-C-C-6	37	-

Tablo A.3. 2. Grupta Bulunan Üreteç Matrisler Kullanılarak Elde Edilen Maksimum Dallanma Sayısına Sahip 8×8 Boyutundaki İkili Matrisler

Matris	***Hamming Ağırlığı (w)***	***İnvolutif***
2-E-E-5	39	-
3-5-A-3	40	+
3-6-F-3	37	+
3-A-5-3	40	+
3-E-E-6	42	-
3-F-6-3	37	+
5-3-3-A	40	-
5-E-E-2	39	-
6-3-3-F	37	-
6-E-E-3	42	-
7-9-9-7	36	-
7-C-C-7	44	-

Matris	*Hamming Ağırlığı (w)*	*İnvolutif*
8-B-B-8	34	-
9-7-7-9	36	-
A-3-3-5	40	-
B-8-8-B	34	-
B-E-E-B	44	-
C-7-7-C	44	-
E-2-5-E	39	+
E-3-6-E	42	+
E-5-2-E	39	+
E-6-3-E	42	+
E-B-B-E	44	-
F-3-3-6	37	-

Tablo A.4. 3. Grupta Bulunan Üreteç Matrisler Kullanılarak Elde Edilen Maksimum Dallanma Sayısına Sahip 8×8 Boyutundaki İkili Matrisler

Matris	*Hamming Ağırlığı (w)*	*İnvolutif*
1-7-7-9	37	-
1-7-7-F	38	-
2-E-E-D	38	-
3-4-4-F	36	-
3-4-6-6	37	-
3-4-A-3	36	-
3-6-4-6	37	-
3-A-4-3	36	-
4-3-3-A	36	-
4-3-6-6	37	-
4-3-F-4	36	+
4-6-3-6	37	-
4-6-D-4	35	-
4-D-6-4	35	-

Matris	*Hamming Ağırlığı (w)*	*İnvolutif*
4-D-D-7	38	-
4-D-D-8	34	-
4-F-3-4	36	+
4-F-F-7	38	-
6-3-6-4	37	-
6-4-4-D	35	-
6-4-6-3	37	-
6-6-3-4	37	-
6-6-4-3	37	-
6-8-8-6	36	-
6-8-E-D	36	-
6-E-8-D	36	-
7-1-9-7	37	-
7-1-F-7	38	-
7-9-1-7	37	-
7-C-D-7	40	-
7-D-C-7	40	-
7-D-D-4	38	-
7-F-1-7	38	-
7-F-F-4	38	-
8-6-6-8	36	-
8-6-D-E	36	-
8-D-6-E	36	-
8-D-D-4	34	-
9-7-7-1	37	-
A-3-3-4	36	-
C-7-7-D	40	-
D-4-4-6	35	-
D-4-7-D	38	+
D-4-8-D	34	-

Matris	*Hamming Ağırlığı (w)*	*İnvolutif*
D-7-4-D	38	+
D-7-7-C	40	-
D-8-4-D	34	-
D-8-E-6	36	-
D-E-8-6	36	-
D-E-E-2	38	-
D-E-E-D	36	-
E-2-D-E	38	-
E-6-D-8	36	-
E-D-2-E	38	-
E-D-6-8	36	-
E-D-D-E	36	-
F-4-4-3	36	-
F-4-7-F	38	-
F-7-4-F	38	-
F-7-7-1	38	-

EK – B

16×16 BOYUTUNDAKİ İKİLİ MATRİSLER İÇİN DENKLİK SINIFLARI

Bu bölüm; tezde bahsi geçen önerilen yöntem ile üretilen ve dallanma sayısı 8 olan tüm 16×16 boyutundaki ikili matrislerin üreteç matrisleri ile birlikte sınıflandırılmasını içermektedir. Aynı sınıfta bulunan matrisler, yine aynı denklik sınıfının üyesi olan devirli matris grupları ile üretilmektedirler. Tablo B.1'de tanımlanan her sınıf için, üreteç matrisler ile Hadamard matrisleri (satır ve sütun permütasyonlarıyla oluşturulabilecek olası 24 (4!) çeşidi de dahil olmak üzere) kullanarak maksimum dallanma sayısına sahip tüm 16×16 boyutundaki ikili matrisler elde edilebilmektedir. Ayrıca, mevcut üreteç matrislerin transpozları ile Hadamard matrisler ve bu Hadamard matrislerin permütasyonları da, maksimum dallanma sayısına sahip 16×16 boyutundaki ikili matrislerin üretilmesi için kullanılabilmektedir.

Tablo B.1'in matris sütunu; her denklik sınıfı için, bu sınıfın üyeleri olan Hadamard matrisleri göstermektedir. Yıldız (*) ile işaretli olanlar, bu matrisin bir involutif MDS matris olduğunu belirtmektedir. Diğer taraftan; bu MDS matrislerden, satır ve sütun permütasyonları ile türetilen diğer tüm matrisler de MDS matris özelliği taşımaktadır. Üreteç matris sütunu; maksimum dallanma sayısına sahip 16×16 boyutundaki ikili matrislerin üretilmesinde başarılı olan, tüm 4×4 boyutundaki devirli matris gruplarını içermektedir. Ayrıca bu sütundaki (x, y, z, t) gösterimi, her sınıf için ilgili üreteç matrisin onaltılık notasyondaki satır değerlerini temsil etmektedir. Örneğin; (1, 3, 6, D) üreteç matrisinin, 4×4 boyutunda bir ikili matris olarak gösterimi, aşağıda görüldüğü gibi olmaktadır.

$$g = \begin{bmatrix} 1_H \\ 3_H \\ 6_H \\ D_H \end{bmatrix} = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$$

w sütunu; aynı satırdaki 4×4 boyutunda bir Hadamard matris ve bu Hadamard matris ile aynı sınıfta bulunan herhangi bir üreteç matris kullanılarak elde edilen ikili matrisin sıfır olmayan elemanlarının sayısını, diğer bir deyişle; Hamming ağırlığını temsil etmektedir. *XOR* sütunu; $\mathbb{F}_{2^4}$ cismi üzerinde tanımlı $f(x) = x^4 + x + 1$ indirgenemez polinomu kullanılarak elde edilen 4×4 boyutundaki matrislerin yazılıma uygulaması için gerekli olan XOR sayısını göstermektedir. Önerilen yöntem ile en düşük uygulama maliyetine sahip *had*(1, 4, 9, D) MDS matrisi de elde edilebilmektedir [35].

Sınıf numaraların altında gösterilen ikili matrislerin sayısı, maksimum dallanma sayısı ölçütünü sağlayan Hadamard matrislerin sayısı, bu Hadamard matrislerin permütasyonların (4!) sayısı ve üreteç matrislerin sayısından oluşmaktadır. Ayrıca 1 numaralı sınıftaki üreteç elemanlardan üretilen tüm üyeler transpozları ile aynı olma özelliğini ($M^T = M$) göstermektedirler.

Tablo B.1. Maksimum Dallanma Sayısına Sahip 16×16 Boyutundaki İkili Matrisler İçin Denklik Sınıfları

	Matris	***Üreteç Matrisler***	***w***	***XOR***
Sınıf 1 (864)	had(1, 6, B, D)	(1-3-6-D), (1-6-5-B), (2-3-E-5), (2-5-B-6), (3-1-A-D), (3-2-E-9), (4-D-3-6), (4-E-5-3), (5-C-1-B), (5-E-4-9), (6-C-B-2), (6-D-A-4)	112	112
	had(1, 7, 9, E)		112	120
	had(8, A, C, F)		144	128
Sınıf 2 (8064)	had(1, 2, 9, B)*	(1-6-D-F), (1-B-6-F), (2-5-F-E), (2-B-F-5), (7-1-A-F), (7-2-F-9)	128	88
	had(1, 2, C, E)*		120	104
	had(1, 3, 9, A)*		120	96
	had(1, 3, D, E)*		128	112
	had(1, 4, 9, D)*		128	72
	had(1, 4, B, F)*		120	112
	had(1, 5, 8, D)*		120	96
	had(1, 5, B, E)*		128	136
	had(2, 4, 8, F)*		136	96
	had(2, 4, 9, E)*		152	96
	had(2, 5, A, C)*		136	120
	had(2, 5, B, D)*		152	120
	had(2, 6, 8, D)*		144	96
	had(2, 7, 8, C)*		136	120
	had(3, 4, A, C)*		136	120
	had(3, 4, B, D)*		152	120
	had(3, 5, 8, F)*		136	128
	had(3, 5, 9, E)*		152	128
	had(3, 6, B, F)*		144	144
	had(3, 7, A, F)*		136	152
	had(4, 6, C, F)*		136	120
	had(4, 7, C, E)*		144	144
	had(5, 6, 8, A)*		136	128
	had(5, 7, 9, A)*		144	136
	had(8, A, D, E)*		128	128
	had(8, B, C, E)*		128	144
	had(9, A, D, F)*		128	112
	had(9, B, C, F)*		128	128

	Matris	***Üreteç Matrisler***	***w***	***XOR***
Sınıf 3 (13824)	had(1, 2, C, E)*	(4-1-C-2), (1-2-8-6), (1-2-9-4), (2-8-1-C), (1-8-4-6), (1-8-C-2), (1-9-4-2), (4-1-8-A), (1-A-8-4), (2-8-5-4), (2-9-4-8), (4-2-9-8)	120	104
	had(1, 3, 5, 6)*		128	112
	had(1, 3, C, F)*		128	112
	had(1, 3, D, E)*		128	112
	had(1, 5, 8, D)*		112	96
	had(1, 5, 9, C)		112	96
	had(1, 5, B, E)*		144	136
	had(1, 7, B, C)*		144	136
	had(2, 4, 8, F)*		112	96
	had(2, 4, A, D)*		120	96
	had(2, 6, 8, D)*		112	96
	had(3, 4, A, C)*		144	120
	had(3, 4, B, D)*		128	120
	had(3, 5, 9, E)*		144	128
	had(3, 5, A, D)		152	128
	had(3, 7, 8, D)*		144	128
	had(3, 7, A, F)*		176	152
	had(3, 7, B, E)*		176	168
	had(4, 6, C, F)*		136	120
	had(4, 7, C, E)*		160	144
	had(4, 7, D, F)*		144	128
	had(5, 7, C, F)		168	152
	had(9, A, D, F)*		136	112
	had(9, B, C, F)*		136	128
Sınıf 4 (4032)	had(1, 6, A, C)*	(2-6-1-F), (1-5-F-2), (1-8-A-F), (4-1-6-F), (1-C-8-F), (1-F-3-4), (2-8-F-9), (4-2-F-5), (2-C-F-8), (2-F-4-3), (4-F-8-9), (4-F-A-8)	136	112
	had(1, 7, 8, F)*		120	120
	had(2, 7, A, E)*		136	144
	had(3, 7, 9, C)*		136	128
	had(4, 6, 8, B)*		144	120
	had(5, 6, D, F)*		144	128
	had(9, B, D, E)*		128	128

	Matris	***Üreteç Matrisler***	***w***	***XOR***
Sınıf 5 (8064)	had(1, 3, 5, 6)*	(7-3-8-A), (3-B-5-4), (7-8-5-C), (1-9-C-E), (6-3-1-E), (1-A-9-E), (6-1-5-E), (5-3-D-2), (3-B-4-6), (7-3-9-8), (7-8-C-6), (2-9-D-A), (2-A-D-C), (5-2-D-6), (4-B-9-C), (4-B-C-A), (3-9-D-2), (3-A-1-E), (5-1-C-E), (6-2-D-C), (7-9-5-8), (7-A-8-6), (6-B-4-A), (5-B-9-4)	136	112
	had(1, 3, C, F)*		128	112
	had(1, 7, B, C)*		136	136
	had(2, 4, A, D)*		136	96
	had(3, 7, 8, D)*		136	128
	had(3, 7, B, E)*		168	168
	had(4, 7, D, F)*		128	128
Sınıf 6 (8064)	had(1, 2, C, E)*	(F-C-8-A), (9-1-5-F), (1-5-9-F), (1-9-3-F), (F-8-A-C), (A-2-F-6), (2-6-F-A), (2-A-F-3), (F-8-C-9), (C-F-4-6), (5-F-6-4), (6-F-4-5)	120	104
	had(1, 3, D, E)*		112	112
	had(1, 5, 8, D)*		112	96
	had(1, 5, B, E)*		128	136
	had(2, 4, 8, F)*		128	96
	had(2, 6, 8, D)*		144	96
	had(3, 4, A, C)*		144	120
	had(3, 4, B, D)*		144	120
	had(3, 5, 9, E)*		144	128
	had(3, 7, A, F)*		128	152
	had(4, 6, C, F)*		152	120
	had(4, 7, C, E)*		144	144
	had(9, A, D, F)*		120	112
	had(9, B, C, F)*		136	128

	Matris	***Üreteç Matrisler***	***w***	***XOR***
Sınıf 7 (8064)	had(1, 2, 4, 6)*	(4-9-6-3), (1-5-6-A), (9-1-A-6), (9-2-C-3), (9-C-1-6), (2-6-9-5), (9-A-4-5), (A-C-5-2), (A-9-6-4), (5-8-A-3), (3-C-6-8), (3-C-8-5)	128	80
	had(1, 2, 8, A)*		112	88
	had(1, 3, 9, A)*		120	96
	had(1, 4, 9, D)*		144	72
	had(1, 7, A, D)*		136	120
	had(2, 4, 9, E)*		136	96
	had(2, 5, A, C)*		144	120
	had(2, 7, 8, C)*		152	120
	had(2, 7, 9, D)*		152	104
	had(2, 7, B, F)*		128	144
	had(3, 5, B, C)*		136	144
	had(5, 7, 8, B)*		128	152
	had(5, 7, 9, A)*		144	136
	had(8, B, C, E)*		136	144
Sınıf 8 (16128)	had(1, 3, 4, 7)*	(1-3-8-E), (3-1-4-E) ,(7-9-8-2), (6-B-1-4), (5-B-4-2), (1-8-5-E), (5-2-1-E), (3-2-D-4), (1-A-D-2), (1-B-C-4), (7-8-9-4), (2-9-1-E), (4-1-9-E), (6-1-D-2), (2-3-D-8), (7-A-1-8), (2-8-D-6), (2-B-4-C), (7-8-4-A), (4-2-D-A), (7-2-8-C), (7-1-C-8), (4-B-5-8), (4-B-8-6)	128	112
	had(1, 4, 8, C)*		128	88
	had(1, 6, 8, E)*		136	112
	had(1, 6, A, C)*		128	112
	had(1, 7, 8, F)*		128	120
	had(2, 5, 9, F)*		128	104
	had(2, 6, 9, C)*		136	96
	had(2, 7, A, E)*		144	144
	had(3, 7, 9, C)*		152	128
	had(4, 6, 8, B)*		136	120
	had(4, 6, 9, A)*		136	104
	had(4, 6, D, E)*		144	120
	had(5, 6, D, F)*		136	128
	had(9, B, D, E)*		136	128

EK – C

16×16 BOYUTUNDA İKİLİ MATRİSİN 8 – BİT PLATFORMDA UYGULANMASINA DAİR BİR ÖRNEK

Bu bölümde, ARIA blok şifresinde kullanılan doğrusal dönüşüm ile aynı boyuta ve dallanma sayısına sahip M_{10} matrisinin, (Bölüm 5, Örnek 5.3) 8-bit işlemciler (52 XOR sayısı) üzerindeki uygulama maliyet hesabı verilmektedir.

16×16 boyutunda, dallanma sayısı 8 olan M_{10} matrisi aşağıda görülmektedir.

$$M_{10} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

M_{10} matrisi 8 – bit işlemciler üzerine uygulandığında, ikili vektörlerin bayt XOR'ları cinsinden, ifade C.1'de görüldüğü şekilde temsil edilebilir.

$$y = M_{10}.x \tag{C.1}$$

İfade C.1'de; $x_i, y_i \in \mathbb{F}_{2^8}$ ve $i = 0,1,\dots,15$ olmak üzere, $x = (x_0, x_1, \dots, x_{15})^T, y = (y_0, y_1, \dots, y_{15})^T$'dir. Ayrıca $T_0, T_1, \dots, T_{11}$, XOR sayısını 52'ye düşürmek için kullanılan geçici değişkenlerdir.

Geçici *T* değişkenleri aşağıdaki gibi tanımlanır:

$$T_0 = x_0 \oplus x_4 \oplus x_9 \oplus x_{13}$$
$$T_1 = x_1 \oplus x_5 \oplus x_8 \oplus x_{12}$$
$$T_2 = x_2 \oplus x_3 \oplus x_6 \oplus x_7$$
$$T_3 = x_{10} \oplus x_{11} \oplus x_{14} \oplus x_{15}$$
$$T_4 = x_6 \oplus x_{10}$$
$$T_5 = x_7 \oplus x_9$$
$$T_6 = x_2 \oplus x_4$$
$$T_7 = x_3 \oplus x_5$$
$$T_8 = x_8 \oplus x_{14}$$
$$T_9 = x_{11} \oplus x_{13}$$
$$T_{10} = x_0 \oplus x_{12}$$
$$T_{11} = x_1 \oplus x_{15}$$

Son olarak, geçici *T* değişkenlerinin yardımıyla *y* değişkenleri tanımlanır:

$$y_0 = T_0 \oplus T_4 \oplus x_{12}$$
$$y_1 = T_1 \oplus T_5 \oplus x_{15}$$
$$y_2 = T_3 \oplus T_6 \oplus x_8$$
$$y_3 = T_3 \oplus T_7 \oplus x_{12}$$
$$y_4 = T_0 \oplus T_8 \oplus x_2$$
$$y_5 = T_1 \oplus T_9 \oplus x_3$$
$$y_6 = T_3 \oplus T_{10} \oplus x_6$$
$$y_7 = T_3 \oplus T_5 \oplus x_1$$
$$y_8 = T_1 \oplus T_6 \oplus x_{14}$$
$$y_9 = T_0 \oplus T_{11} \oplus x_7$$
$$y_{10} = T_2 \oplus T_{10} \oplus x_{10}$$

$$y_{11} = T_2 \oplus T_9 \oplus x_5$$
$$y_{12} = T_1 \oplus T_4 \oplus x_0$$
$$y_{13} = T_0 \oplus T_7 \oplus x_{11}$$
$$y_{14} = T_2 \oplus T_8 \oplus x_4$$
$$y_{15} = T_2 \oplus T_{11} \oplus x_9$$

Geçici T değişkenlerinin tanımlanması için gereken XOR sayısı 20, y değişkenlerinin tanımlanması için gereken XOR sayısı ise 32'dir. Böylelikle M_{10} matrisinin 8 – bit işlemcilere uygulanmasının toplam maliyeti 20 + 32 = 52 XOR olarak elde edilir.

KAYNAKLAR

[1] M. Wenbo, ***Modern Cryptography: Theory and Practice***, Prentice Hall, (2004).

[2] M. T. Sakallı, ***Modern Şifreleme Yöntemlerinin Gücünün İncelenmesi***, Doktora Tezi, (2006).

[3] D. Khan, ***The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet***, (Scribner, 1996).

[4] C. Çimen, S. Akleylek, E. Akyıldız, ***Şifrelerin Matematiği: Kriptografi***, (Odtü Yayıncılık, 2014).

[5] S. Singh, ***The Code Book: The Science of Secrecy from Ancient Egypt to Quantum Cryptography***, (Anchor, 2000).

[6] C. E. Shannon, ***Communication Theory of Secrecy Systems***, Bell System Technical Journal, No. 30, pp. 50-64, (1949).

[7] L. Keliher, ***Linear Cryptanalysis of Substitution-Permutation Networks***, Doktora Tezi, (2003).

[8] FIPS 46-3, ***Data Encryption Standard, Federal Information Processing Standard (FIPS)***, Publication 46-3, National Bureau of Standards, U.S. Deparment of Commerce, Washington D.C., (1999).

[9] FIPS 197, ***Advanced Encryption Standard, Federal Information Processing Standard (FIPS)***, Publication 197, National Bureau of Standards, U.S. Deparment of Commerce, Washington D.C., (2001).

[10] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita, ***Camellia: A 128-bit block cipher suitable for multiple platforms-design and analysis,*** SAC 2000. Lecture Notes in Computer Science, Vol. 2012, pp. 39–56. Springer, Heidelberg, (2000).

[11] D. Kwon, J. Kim, S. Park, S.H. Sung, Y. Sohn, J.H. Song, Y. Yeom, E-J. Yoon, S, Lee, J. Lee, S. Chee, D. Han, and J. Hong, ***New block cipher: ARIA***, Proceedings of International Conference on Information Security and Cryptology, Lecture Notes in Computer Science, Vol. 2971, 432-445, Springer-Verlag, (2004).

[12] P. S. L. M. Barreto and V. Rijmen, ***The Khazad legacy-level block cipher***, First open NESSIE Workshop, Leuven, (2000).

[13] A. Bogdanov, L.R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin, C. Vikkelsoe. ***PRESENT: An ultra-lightweight block cipher***. In Cryptographic Hardware and Embedded Systems-CHES, 450-466, Springer Berlin Heidelberg, (2007).

[14] A. Ross, E. Biham, and L. Knudsen. ***Serpent: A proposal for the advanced encryption Standard***, NIST AES Proposal, (1998).

[15] M. R. Z'aba, ***Analysis of linear relationships in block ciphers***, Doktora Tezi, (2010).

[16] H. Feistel, ***Cryptography and computer privacy***, Scientific American, 228(5), 15–23, (1973).

[17] A. F. Webster, S. E. Tavares, ***On the design of S-boxes***, In Proceedings of CRYPTO'85 Lecture Notes in Computer Science, Vol. 218, 523–534, (1986).

[18] J. B. Kam, G. I. Davida, ***Structured design of substitutionpermutation encryption Networks***, IEEE Transactions on Computers, 28(10), 747–753, (1979).

[19] J. Daemen, V. Rijmen, ***The Design of Rijndael: AES (The Advanced Encryption Standard)***, Springer-Verlag, (2002).

[20] N. Ajlouni, A. El-Sheikh, A. Rashed, ***A New Approach in Key Generation and Expansion in Rijndael Algorithm***, The International Arab Journal of Information Technology, Vol.3, No.1, (2006).

[21] A. Forouzan, ***Cryptography and Network Security***, (International Edition, 2008).

[22] R. Lidl, H. Niederreiter, ***Introduction to finite fields and their applications***, (Cambridge University Press, 1994).

[23] D. R.Stinson, ***Cryptography, Theory and Practice***, (Chapman & Hall/CRC Press, 2002).

[24] S.Ling, C. Xing, ***Coding Theory: A First Course***, (Cambridge University Press, 2004).

[25] Jr J. Nakahara, E. Abrahão, ***A new Involutory MDS Matrix for the AES***, International Journal of Network Security, Vol. 9, n. 2, 109-116, (2009).

[26] J. Daemen, V. Rijmen, ***The Design of Rijndael: AES (The Advanced Encryption Standard)***, Springer-Verlag, (2002).

[27] P. S. L. M. Barreto, V. Rijmen, ***The ANUBIS legacy-level block cipher***, Proceedings of First Open NESSIE Workshop, Leuven, (2000).

[28] D. Kwon, S.H. Sung, J.H. Song, S. Park, ***Design of block ciphers and coding theory***, Trends in Mathematics 8(1), 13-20, (2005).

[29] S. Ling, C. Xing., ***Coding Theory: A First Course***, (Cambridge University Press, 2004).

[30] W. Bosma, J. Cannon, C. Playoust, ***The Magma Algebra System I: The User Language***, Journal Symbolic Computation, 24 (3-4), 235-265, (1997).

[31] B. Aslan, ***Blok Şifreler İçin Cebirsel İkili Doğrusal Dönüşüm Tasarımı ve Modern Bir Blok Şifreye Uygulanması***, Doktora Tezi, (2013).

[32] K. E. Morrison, ***Integer sequences and matrices over finite fields***, Journal of Integer Sequences, 9, Article 06.2.1, (2006).

[33] B.W. Koo, H.S. Jang, J.H. Song, ***On constructing of a 32×32 binary matrix as a diffusion layer for a 256-bit block cipher***, Proceedings of International Conference on Information Security and Cryptology, LNCS 4296, pp. 51-64, Springer, (2006).

[34] M.T. Sakallı, B. Aslan, ***On the algebraic construction of cryptographically good 32×32 binary linear transformations***, Journal of Computational and Applied Mathematics, 259 (Part B), 485-494, (2014).

[35] K. Khoo, T. Peyrin, A. Poschmann, H. Yap, ***FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison***, Proceedings of Cryptographic Hardware and Embedded Systems (CHES), LNCS 8731, pp. 433-450, Springer, (2014).

[36] S.M. Kim, K. Khoo, F. Oggier, T. Peyrin, ***Lightweight MDS Involution Matrices***, Fast Software Encryption: 22nd International Workshop (FSE), LNCS 9054, pp. 471-493, Springer, (2015).

[37] M. T. Sakallı, S. Akleylek, B. Aslan, E. Buluş, F. B. Sakallı, ***On the Construction of 20x20 and 24x24 Binary Matrices with Good Implementation Properties for Lightweight Block Ciphers and Hash Functions***, Mathematical Problems in Engineering, doi: 10.1155/2014/540253, (2014).

ÖZGEÇMİŞ

1979 yılında İstanbul'da doğdum. İlk, orta ve lise öğretimini İstanbul'da tamamladıktan sonra, 1997 yılında Trakya Üniversitesi Fen – Edebiyat Fakültesi Kimya bölümünü kazandım. 2002 yılında mezun olduktan sonra İstanbul'da özel bir ilaç firmasında çalıştım. 2003 yılında Trakya Üniversitesi Fen Bilimleri Enstitüsü Kimya Öğretmenliği bölümünde tezsiz yüksek lisansa ve eş zamanlı olarak özel bir dershanede kimya öğretmenliğine başladım. 2007 yılında Sakarya Üniversitesi Adapazarı Meslek Yüksekokulu Bilgisayar Programcılığı bölümünü kazandım. 2009'da mezun olduktan sonra dershaneden ayrılarak Trakya Üniversitesi Teknik Bilimler Meslek Yüksekokulu'nda serbest öğretim elemanı olarak ders vermeye başladım. 2010'da dikey geçiş sınavına girerek Trakya Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünü kazandım. 2013 yılında söz konusu bölümden mezun olduktan sonra, 2014 yılında başladığım Trakya Üniversitesi Fen Bilimleri Enstitüsü Hesaplamalı Bilimler Anabilim Dalı Yüksek Lisans programında halen öğrenimime devam etmekteyim.

TEZ ÇALIŞMASI SIRASINDA GERÇEKLEŞTİRİLEN BİLİMSEL FAALİYETLER

1. G. Tuncay, E. Öztürk, S. Akleylek, M. T. Sakallı, A. Ş. Mesut, ***Kriptografik Özellikleri İyi Olan İkili Matrislerin Geliştirilmesi İçin Yeni Bir Yöntem***, TÜBİTAK II. Ulusal Kripto Günleri Çalıştayı, Kocaeli, (2015).

2. S. Akleylek, M. T. Sakallı, A. Ş. Mesut, E. Öztürk, G. Tuncay, ***Generating Binary Diffusion Layers with Maximum Branch Number and Low Search Complexity***, Submitted, (2015).