T.C.

TRAKYA ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

MDS YAYILIM MATRİSLERİNDE İZOMORFİZMALAR ÜZERİNE YENİ BİR ÇALIŞMA

KEMAL AKKANAT

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Tez Danışmanı: Doç. Dr. M. TOLGA SAKALLI

EDİRNE-2017

Kemal AKKANAT'ın hazırladığı "MDS Yayılım Matrislerinde İzomorfizmalar Üzerine Yeni Bir Çalışma" başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar Mühendisliği Anabilim Dalında bir Yüksek Lisans tezi olarak kabul edilmiştir.

Jüri Üyeleri — İmza

Doç. Dr. Sedat AKLEYLEK

Yrd. Doç. Dr. Andaç ŞAHİN MESUT

Doç. Dr. M. Tolga SAKALLI

Tez Savunma Tarihi: 18/12/2017

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Doç. Dr. M. Tolga SAKALLI

Tez Danışmanı

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

Prof. Dr. Murat YURTCAN

Fen Bilimleri Enstitüsü Müdürü

T.Ü.FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI YÜKSEK LİSANS PROGRAMI

DOĞRULUK BEYANI

Trakya Üniversitesi Fen Bilimleri Enstitüsü, tez yazım kurallarına uygun olarak hazırladığım bu tez çalışmasında, tüm verilerin bilimsel ve akademik kurallar çerçevesinde elde edildiğini, kullanılan verilerde tahrifat yapılmadığını, tezin akademik ve etik kurallara uygun olarak yazıldığını, kullanılan tüm literatür bilgilerinin bilimsel normlara uygun bir şekilde kaynak gösterilerek ilgili tezde yer aldığını ve bu tezin tamamı ya da herhangi bir bölümünün daha önceden Trakya Üniversitesi ya da farklı bir üniversitede tez çalışması olarak sunulmadığını beyan ederim.

18/12/2017

Kemal AKKANAT



Yüksek Lisans Tezi
MDS Yayılım Matrislerinde İzomorfizmalar Üzerine Yeni Bir Çalışma
T.Ü. Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

ÖZET

Blok şifrelerde ve kriptografik hash (özet) fonksiyonlarında özellikle yayılım katmanı olarak kullanılan $GF(2^m)$'deki MDS matrisler, çok iyi yayılım özellikleri taşırlar. Bu tez, var olan MDS matrislerden yeni MDS matrisler elde edilmesini sağlayan yeni bir metod üzerinedir. Bu tezde, açık bir şekilde aynı ikili genişletilmiş cisimlerdeki MDS matrsilerin otomorfizmaları tanımlanmaktadır. Daha sonra bu fikir genişletilerek, $GF(2^m)$ üzerindeki MDS matrislerle $GF(2^{mt})$ ($t \geq 1$ ve $m > 1$) üzerindeki MDS matrisler arasındaki izomorfizmalar sunulmaktadır. Daha sonra var olan MDS matrislerden yeni MDS matrisler üretilmesinde kullanılan otomorfizmalarla ve izomorfimalarla ilgili farklı fonksiyonların elde edilmesi için yeni bir metod sunulmaktadır. Sunulan metod, yeni MDS matrisler üretmek için girdi olarak MDS matris alır. Bu bakımdan, bu metod diğer MDS matris tasarlama metodlarının etkinliğini onlara yeni MDS matrisler üretme imkanı sağlayarak artırabilir. Yeni üretilen matrisler, var olan matrislerden daha iyi uygulama özelliğine sahip olabilirler. Bununla beraber bu tez, $GF(2^m)$ üzerinde MDS matrisler ile $GF(2^{mt})$ üzerinde MDS matrisler arasındaki ilişkiyi ortaya çıkarmaktadır.

Yıl : 2017
Sayfa Sayısı : 60
Anahtar Kelimeler : Blok şifreler, MDS Matrisler, Dallanma Sayısı, Yayılım Katmanı, İzomorfizma, Otomorfizma

Master's Thesis

A Novel Study on the Isomorphisms of MDS Diffusion Matrices

Trakya University Institute of Natural Sciences

Department of Computer Engineering

ABSTRACT

MDS matrices over $GF(2^m)$, which offer perfect diffusion properties, are especially used as diffusion layers in block ciphers and cryptographic hash functions. This thesis is on a novel method that allows to obtain new MDS (Maximum Distance Separable) matrices from existing ones. In this thesis, the automorphisms of MDS matrices over the same binary extension field are explicitly defined. By extending the same idea, the isomorphisms between MDS matrices over $GF(2^m)$ and MDS matrices over $GF(2^{mt})$ where ($t \geq 1$ and $m > 1$) are presented. Then a novel method is proposed to obtain distinct functions related to these automorphisms and isomorphisms to be used in generating new MDS matrices from the existing ones. The proposed method takes an MDS matrix as input to generate new MDS matrices. In this respect, it can increase the efficiency of other construction methods by allowing them generating new MDS matrices, which may have better implementation properties than the existing ones. Moreover, it presents the relationship between MDS matrices over $GF(2^m)$and MDS matrices over $GF(2^{mt})$.

Year : 2017

Number of Pages : 60

Keywords : Block Ciphers, MDS Matrices, Branch Number, Diffusion Layer, Isomorphism, Automorphism

TEŞEKKÜR

Bu çalışmanın hazırlanması sürecinde her türlü konuda bana yardımcı olan ve yol gösteren değerli hocam Doç. Dr. M. Tolga SAKALLI ’ya çok teşekkür ederim.

İÇİNDEKİLER

ÖZET iv
ABSTRACT v
TEŞEKKÜR vi
İÇİNDEKİLER vii
ÇİZELGELER DİZİNİ ix
ŞEKİLLER DİZİNİ x
BÖLÜM 1 1
GİRİŞ 1
1.1. Kriptografi 2
1.1.1. Akan Şifreler 4
1.1.2. Blok Şifreler 6
1.1.2.1. S-Kutuları (Substitution-Boxes, Yer Değiştirme Kutuları) 9
1.1.2.2. Doğrusal Dönüşümler 9
1.1.2.2.1. AES Blok Şifreleme Algoritmasında Doğrusal Dönüşüm 10
1.1.2.2.2. ARIA Blok Şifreleme Algoritmasında Doğrusal Dönüşüm 12
1.2. Kriptanaliz 13
1.2.1. Diferansiyel Kriptanaliz 14
1.2.2. Doğrusal Kriptanaliz 15
1.3. MDS (Maximum Distance Separable-Maksimum Uzaklıkta Ayrılabilen) Matrisler 15
1.4. Tez Konusu ve Önemi 16
BÖLÜM 2 18
2. MATEMATİK ALTYAPI 18

2.1. Sonlu Cisimler 18
2.1.1. Genişletilmiş Sonlu Cisimlerde Toplama, Çarpma İşlemleri 21
2.1.1.1. Genişletilmiş Sonlu Cisimlerde Toplama İşlemi 21
2.1.1.2. Genişletilmiş Sonlu Cisimlerde Çarpma İşlemi 22
2.2 MDS Matrisler ile İlgili Altyapı 25
2.3. İzomorfizma 30
2.4. Otomorfizma 32
BÖLÜM 3 33
3. $GF(2^m)$'DE TANIMLI MDS MATRİSLERDEN $GF(2^{mt})$'DE TANIMLI MATRİSLER ÜRETME 33
3.1. MDS Matris Otomorfizmaları 33
3.2. MDS Matris İzomorfizmaları 38
3.3. MDS Matris İzomorfizmalarının Genelleştirilmesi için Yöntem 43
BÖLÜM 4 53
4. GELİŞTİRİLEN YÖNTEMİN BAZI ÖNEMLİ ÖZELLİKLERİ ve UYGULAMA AVANTAJLARI 53
4.1. Geliştirilen Yöntemin Önemli Özellikleri 53
4.2. MDS Matris Üretmek için Geliştirilen Yöntemin Uygulama Özellikleri 54
BÖLÜM 5 60
5. SONUÇ 60
KAYNAKLAR 61
ÖZGEÇMİŞ 64

ÇİZELGELER DİZİNİ

Çizelge 1.1 Şifreleme Algoritmaları ve Hash (Özet) Fonksiyonları.....3

Çizelge 1.2 Vigenère Tablosu.....6

Çizelge 3.1 $GF(2^4)/(x^4+x+1)$ Cisminde Otomorfik Fonksiyon $f_{2,1}: \alpha \to \alpha^4$ 37

Çizelge 4.1 $GF(2^8)$'de, 4×4 MDS Matrislerin Karşılaştırılması 56

ŞEKİLLER DİZİNİ

Şekil 1.1 Basit Bir SPN (Substitution Permutation Networks) Yapısı 8
Şekil 1.2 Feistel Yapısı 9
Şekil 1.3 AES Döngü Fonksiyonu 11
Şekil 2.1 Z_5 te Toplama ve Çarpım İşlemleri 20

BÖLÜM 1

GİRİŞ

Kriptoloji bilgilerin güvenliğinin sağlanması, şifreli bilgilerin çözülmesi, sayısal verinin güvenli bir şekilde iletilmesinde kullanılan şifreleme algoritmalarının tasarlanması, kullanıma hazır hale getirilmesi ve optimize edilmesini kapsayan kriptografi ile şifreleme algoritmalarını kırmaya yönelik saldırıları inceleyen kriptanalizin birleşmesiyle ortaya çıkan bir bilim dalıdır (Sakallı, 2006).

Kriptografi, Yunancadan alınan "kryptos" gizli ve saklı anlamıyla "graf" ise yazı anlamıyla birleşerek bilgileri, mesajları istenilen kişi haricindeki kişilerin okuyamayacağı forma dönüştürme veya gizli yazı oluşturmadır. Günümüz kriptografisi bünyesinde matematik, bilgisayar bilimleri ve elektronik mühendisliğini de barındırarak çok disiplinli bir bilim haline gelmiştir.

Kriptanaliz köken olarak Yunanca kryptos (gizli) ve analýein (çözmek) kelimelerinin birleşmesiyle oluşmuş, şifreli metinlerin çözümünü araştıran bir bilim dalıdır.

Şifrelemenin ilk örneklerinden biri Milattan önce Julius Caesar (MÖ:100-44) zamanında kullanılan Sezar şifresidir. Basit olarak alfabedeki her harfi üç sıra kaydırarak değiştirmiş böylece sadece üçlü kaydırma yöntemini bilen kişilerin şifreli metinleri çözebilmesini sağlamıştır. Modern örnek olarak da II. Dünya savaşında Almanların askeri sırlarını gizlemek amacıyla geliştirdikleri "Enigma makinesi" akla gelebilir. Bu sistem ilk olarak 1932 yılında Polonyalı matematikçiler Marian Rejewski, Jerzy Rozycki ve Henryk Zygalski tarafından, ele geçirilen şifreli metin ve ajanların sağladığı 3 ay süreyle kullanılmış anahtarların olduğu liste sayesinde kırılmıştır (Kozaczuk, 2004).

Tarihte kriptanalizden ilk olarak, 9. yy da matematikçi Ebu Yusuf Yakup'un "A Manuscript on Deciphering Cryptographic Messages" adlı eserinde frekans analizi olarak bahsedilmiştir. Bu yöntem ile şifreli metindeki harflerin tekrar etme sayısı veya harf gruplarının tekrar etme sayısı göz önüne alınarak yapılan klasik şifreli metinleri kırma amaçlıdır.

Bölüm 1.1 ve 1.2'de sırasıyla kriptografi ve kriptanaliz hakkında bilgi verilmektedir.

1.1. Kriptografi

Günümüz bilgi çağında teknolojinin gelişmesi ile kriptografik konular hayatımıza daha çok girmeye başlamıştır. Hatta kriptografinin casusluk amacıyla kullanılabilmesinden dolayı birçok yönetim kriptografiyi bir silah olarak değerlendirmektedir. Diğer taraftan yine aynı nedenden dolayı kriptografi çeşitli limit ve yasaklamalarla karşı karşıya kalmaktadır (Britannica, 2017). Kriptografi ile gizli bilgiler, ilgili olmayan kişilerin bilgilere erişimi engellenerek güvenli bir iletişim amaçlanmaktadır.

Güvenliğin sağlanması için gerekli üç güvenlik hedefi sırasıyla gizlilik, bütünlük ve kullanılabilirliktir. Gizlilik, bilgilere sadece ilgili kişilerce ulaşılmasını ve bu bilgilerin diğer kişilerden korunmasını ifade eder. Bütünlük, bilgilerin eksiksiz, tutarlı ve tam olmasını ifade eder. Kullanılabilirlik, bilgilere gereksinim duyulduğu anda ulaşılabilmesini ifade eder. Gizlilik hedefi şifreleme algoritmalarının kullanımı ile gerçekleştirilir. Şifreleme algoritmaları sırasıyla simetrik ve asimetrik şifreler olarak ikiye ayrılır. Simetrik şifreleme algoritmaları şifreleme ve şifre çözme aşamalarında aynı anahtarı kullanır. Asimetrik şifreleme algoritmaları ise şifreleme işleminde halka açık bir anahtar (public) kullanırken şifre çözme aşamasında gizli (private) bir anahtar (dolayısıyla iki farklı anahtar) kullanır. Bütünlük hedefi için temel olarak hash (özet) fonksiyonları kullanılır. Hash fonksiyonları kullanmaktaki amaç bütün veriler için birbirine kesinlikle benzemeyecek, sabit uzunlukta mesaj özetlerinin elde edilmesini sağlamaktır. Hash fonksiyonlarının çalışma prensibi, simetrik ve asimetrik şifrelemeden farklı olarak tek yönlüdür. Bu nedenle, hash fonksiyonlarında simetrik veya asimetrik şifrelemede olduğu gibi mesaj özetinden açık metne ulaşılamaz ve bu özelliklerinden

dolayı veri tabanındaki verilerin güvenliğinin ve özellikle web sitelerinde şifre denetiminin sağlanmasında tercih edilirler.

Çizelge 1.1'de şifreleme algoritmalarına ve hash fonksiyonlarına örnekler verilmektedir.

Çizelge 1.1 Şifreleme Algoritmaları ve Hash (Özet) Fonksiyonları

ŞİFRELEME ALGORTİMALARI ve HASH FONKSİYONLARINA ÖRNEKLER	**SİMETRİK ŞİFRELEME**	BLOK ŞİFRELER	DES Square Camellia Khazad IDEA AES ARIA
		AKAN ŞİFRELER	RC4 Trivium HC-256
	ASİMETRİK ŞİFRELEME	RSA	
		Rabin	
		ElGamal	
	HASH (ÖZET) FONKSİYONLARI	MD2	
		MD5	
		SHA-512	
		HAVAL	

Çizelge 1.1'de örnek verilen şifreleme ve Hash (Özet) fonksiyonlarına ait kaynaklar aşağıda verilmektedir.

DES (NIST, 1999).

Square (Daemen, Knudsen & Rijmen, 1997).

Camellia (Aoki vd., 2000, s. 39-56).

Khazad (Barreto & Rijmen, 2000c).

IDEA (Schneier, 1996).

AES (Daemen & Rijmen, 2002).

ARIA (Chee vd., 2004, s. 432-445).

RC4 (Schneier, 1996).

Trivium (Cannière & Preneel, 2005).

HC-256 (Wu, 2005).

RSA (Forouzan, 2008).

Rabin (Forouzan, 2008).

ELGamal (Forouzan, 2008).

MD2 (Schneier, 1996).

MD5 (Schneier, 1996).

SHA-512 (Schneier, 1996).

HAVAL (Schneier, 1996).

1.1.1. Akan Şifreler

Akan şifreleme algoritmaları, simetrik şifreleme algoritmalarının bir alt grubudur ve bir kerede açık metnin sadece bir karakterini (birimini), zamana göre değişen bir algoritmayla şifrelerler. Akan şifreleme algoritmalarında, açık metnin her bir hanesine karşılık şifrelemede kullanılan anahtarın tek bir hanesi kullanılarak şifreleme gerçekleştirilir. Akan şifrelerde, açık metindeki her bir karakter anahtar dizisindeki karşılık gelen karakterle bir kez işleme tabi tutulur. Akan şifreler genellikle blok şifrelere göre daha hızlı şifreleme algoritmalarıdır.

Kral IX. Charles için çalışan diplomat Frenchman Blaise de Vigenère'in keşfettiği algoritma akan şifrelere benzer özellikler taşıdığı için akan şifre olarak

düşünülebilir. Bu algoritmaya göre açık metin arasında boşluk olmayacak şekilde yazılır ve belirlenen anahtara göre Vigenère tablosuyla işleme alınır. Bulunan sonuç o harf için şifreli hali olmuş olur. Vigenère tablosunu ise alfabedeki her harfe 0'dan başlayan sayılar vererek (A=0 B=1… Z=25) yatay ve düşey oluşturmuştur. Bir açık metin şifrelenecekken metindeki bir haneye karşılık gelen harfin sayısal değeri ile anahtarın karşılık gelen sayısal değeri toplanarak bulunan sonuç şifrelenmiş halidir. Eğer toplam sayısı 26'dan büyük çıkarsa (mod26) uygulanıp sonuç yazılır.

Güncel akan şifre algoritmalarında ise genel olarak haneler bit olarak isimlendirilir ve anahtar dizisiyle olan işlem ise XOR işlemidir. Her bir hane ikili sisteme göre rakamlar içerir. Sözde (pseudorandom) anahtar dizileri, rastgele çekirdek değerlerden oluşturulur. Asıl değerler aynı zamanda şifreli metnin çözülmesinde de kullanılır. Akan şifre algoritmasında şifrenin kolay çözülmemesi için aynı asıl değerler iki kez kullanılmaz. Akan şifreler temelde ikiye ayrılarak incelenir. Bunlardan eş zamanlı akan şifrelerde anahtar dizileri, asıl metin ve şifreli metinden bağımsız olarak üretilir. Eş zamansız akan şifrelerde ise anahtar dizisi bir önceki şifreli metnin veya anahtarın bir fonksiyonu ile elde edilir. Kısa olan anahtar dizisinin genişletilmesi oluşturulan şifrenin çözülmesini zorlaştırmaktadır. Literatürde en bilindik akan şifreleme algoritması RC4 son yıllarda yerini Chacha (Aumasson, Fischer, Khazaei, Meier & Rechberger, 2007) ve Salsa20 (Aumasson, Fischer, Khazaei, Meier & Rechberger, 2007) gibi akan şifreleme algoritmalarına bırakmıştır.

Çizelge 1.2 Vigenère Tablosu

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Açık metin: TRAKYAUNIVERSITY

Anahtar: BESTBESTBESTBEST

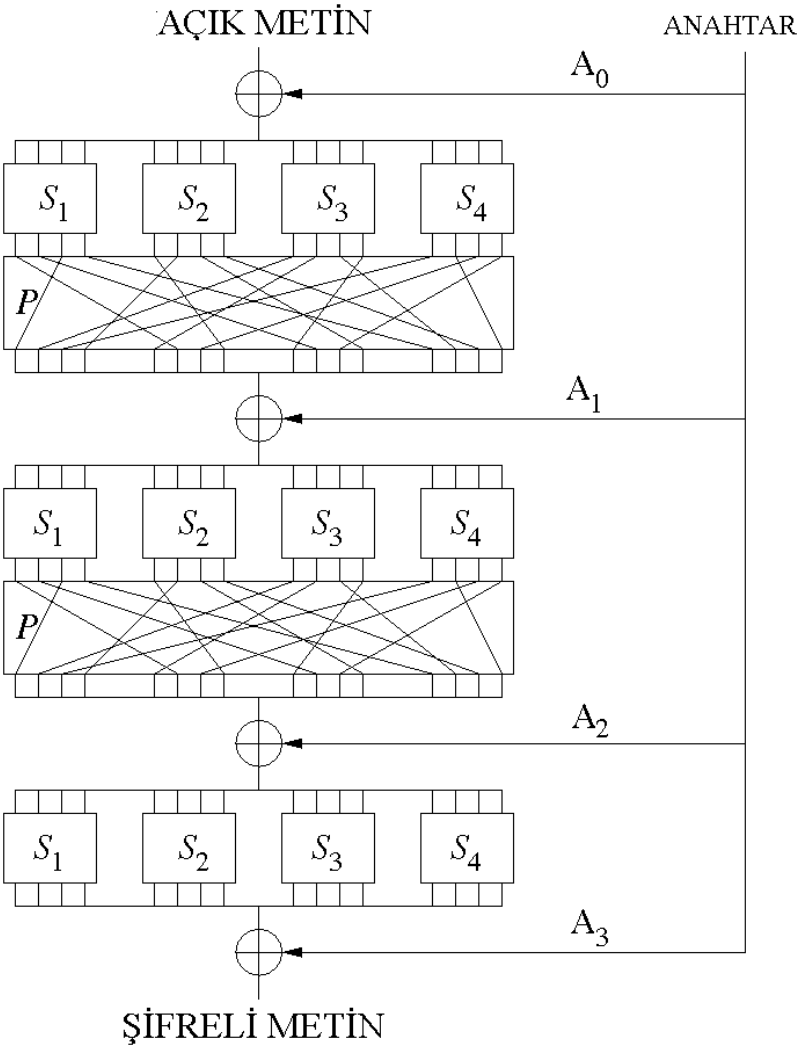
Şifreli Metin: UVSDZEMGJZWKTMLR

1.1.2. Blok Şifreler

Bugün kullanımda olan blok şifreler, yinelenen ürün şifreleme kavramına dayanmaktadır. Ürün şifreleme, 1949 yılında Claude Shannon'un Communication Theory of Secrecy Systems makalesinde analiz edilmiştir. Yinelenen ürün şifreleme kavramı, şifreleme sürecinin birden fazla döngü sonucunda oluşmasını belirtir. Her döngüde kullanılan alt anahtar birbirinden farklıdır ve ilk oluşturulan orijinal anahtardan türetilir. Blok şifre tasarımında kullanılan en geniş uygulama alanına sahip yapılar Feistel yapısı ve SPN (Yer değiştirme-Permütasyon) yapısıdır. SPN yapısı ile çalışan şifreleme algoritmalarına örnek olarak AES (Advanced Encryption Standard) verilebilir. Feistel yapısı Horst Feistel tarafından bulunmuş ve DES şifrelerin tasarımında da kullanılan bir yapıdır. NIST (The Unites States National Institute of Standards in Technology (o zamanki adıyla NBS (National Bureau of Standards))) 1977'de DES şifreleme algoritmasını ortaya çıkarmıştır. Bu şifreleme algoritması, insanların modern

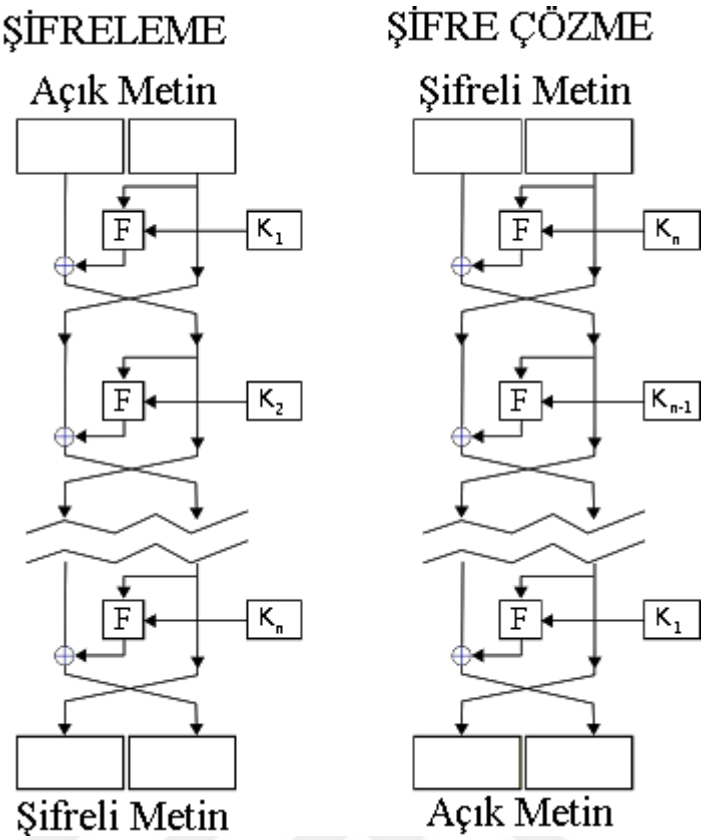
şifrelemenin nasıl çalıştığını anlamasına yardımcı olmuştur. Bununla beraber kriptanalizin gelişmesine etki etmiş, kriptanalizin akademik ve serbest alanda yer bulmasına neden olmuştur. Yeni blok şifre tasarlanması ve bu şifrelerin yeni üretilen çok çeşitli saldırılara karşı denenmesinin temeli bu algoritmaya dayanır. Blok şifreler aynı zamanda daha karmaşık kriptografik protokollerin (pseudorandom number generators ve yaygın hash (özet) fonksiyonları gibi) temel altyapısını oluşturur.

Blok şifre algoritmaları açık metni sabit uzunluklu n-bit'ten oluşan bir blok haline çevirir. Genellikle kullanılan blok uzunlukları 64 bit, 128 bit, 256 bit'tir. Şifreleme işleminde n-bit uzunluğunda bir açık metin bloğu ve en azından n-bit uzunluğunda bir anahtar kullanılarak n-bit uzunluğunda bir şifreli metin elde edilmiş olur. Örneğin 64 bit uzunluktaki bir açık metin bloğu şifrelendiğinde 64 bit uzunluğunda bir şifreli metin elde edilmiş olur. Şifre çözme işlemi de şifreleme işleminin ters fonksiyonudur. Buradaki birbirine dönüşümü sağlayan esas parça anahtardır. Blok şifreler döngü adı verilen aynı işlem adımlarının tekrarlanarak uygulamasını içerir. Örneğin SPN yapısında ilk döngü sonucu üretilen şifreli metin ve yine ilk döngüdeki orijinal anahtardan türetilen anahtar bir sonraki döngüde girdi olarak kullanılır ve o döngüye ait yer değiştirme ve permütasyon işlemleri kullanılarak bir sonraki döngü için şifreli metin çıktısı oluşturulur. S-kutuları her döngüde karıştırma görevini görür. Karıştırma görevi sayesinde bir sonraki döngünün girdisi (bir önceki döngünün şifreli metni) ile orijinal anahtardan üretilen alt anahtar arasındaki ilişkiyi gizler. Güvenli bir blok şifre için güvenilir bir S-kutusu seçilmelidir. Aynı işlem adımlarının tekrarlanarak uygulanması sonucu oluşabilecek simetrinin engellenmesi için her döngüde kullanılmak üzere orijinal anahtardan alt anahtarlar elde edilir. Bu alt anahtarların elde edilmesi işlemi anahtar planlama rutini ile gerçekleştirilir.



Şekil 1.1 Basit Bir SPN (Substitution Permutation Networks) Yapısı

Feistel yapısında ise SPN yapısından farklı olarak açık metin bloğu iki eşit parçaya ayrılır. Her döngüde alt anahtarlarla beraber diğer işlemler bu parçalardan birine uygulandıktan sonra diğer parçayla XOR işlemine tabi tutulur. Daha sonra bu iki parça yer değiştirir.



Şekil 1.2 Feistel Yapısı

Tüm bu yapılar ve algoritmalarla kriptografik yapıların kriptanalitik saldırılara karşı direnç göstermesi amaçlanmaktadır.

1.1.2.1. S-Kutuları (Substitution-Boxes, Yer Değiştirme Kutuları)

Blok şifrelerin oluşturulmasında S-kutuları kullanılır. S-kutuları vektörel boole fonksiyonları ile ifade edilebilirler. Bu fonksiyonlar $GF(2^m)$'den $GF(2)$'ye tanımlanır. S-kutuları verilerin karıştırılmasını sağlayarak, güvenli bir şifreleme algoritmasının temel taşlarından birini oluşturmaktadır. Veriler S-kutusundaki dönüşüm fonksiyonlarına göre başka verilerle değişmekte böylelikle doğrusal olmayan bir dönüşüm sağlanmaktadır.

1.1.2.2. Doğrusal Dönüşümler

Claude Shannon prensipleri doğrultusunda, bir şifreleme algoritmasının kuvvetli olması karıştırma ve yayılım işlemlerine bağlıdır. Yayılımın amacı açık metinle şifreli metin arasındaki ilişkiyi mümkün olduğunca bulunması zor hale getirmektir. Karıştırma

ise şifre anahtarı ile şifreli metin arasındaki ilişkiyi gizler. Şifreleme algoritmalarında yayılım işlemi doğrusal dönüşümlerle sağlanır. Doğrusal dönüşüm belli bir uzunluktaki girdi değerlerinin, çeşitli işlemlere tabi tutularak yeni çıktı değerlerinin elde edilmesidir. Bu işlemler, matris şeklinde ifade edilen girdi değerlerinin, sonlu cisimlerdeki işlem kurallarıyla uygun boyutlarda bir matris ile çarpılması suretiyle yeni değerlere dönüştürülmesi şeklinde veya matrislerle ifade edilen girdi değerleri üzerine çeşitli şekillerde döndürme işlemleri uygulanması şeklinde olabilir. Şifreleme algoritmalarının doğrusal veya diferansiyel kriptanaliz gibi saldırılarına karşı daha dirençli olabilmesi için doğrusal dönüşümü gerçekleştiren yayılım katmanlarında genellikle farklı boyutlarda MDS (Maximum Distance Separable) veya MDBL (Maximum Distance Binary Linear) (Akleylek, Sakallı, Öztürk, Mesut & Tuncay, 2016, s. 3558-3569., Akleylek, Rijmen, Sakallı & Öztürk, 2017, s. 177-187) matrisler kullanılır. Bölüm 1.1.2.2.1 ve 1.1.2.2.2'de sırasıyla AES ve ARIA şifreleme algoritmalarında kullanılan doğrusal dönüşümler hakkında bilgi verilmektedir.

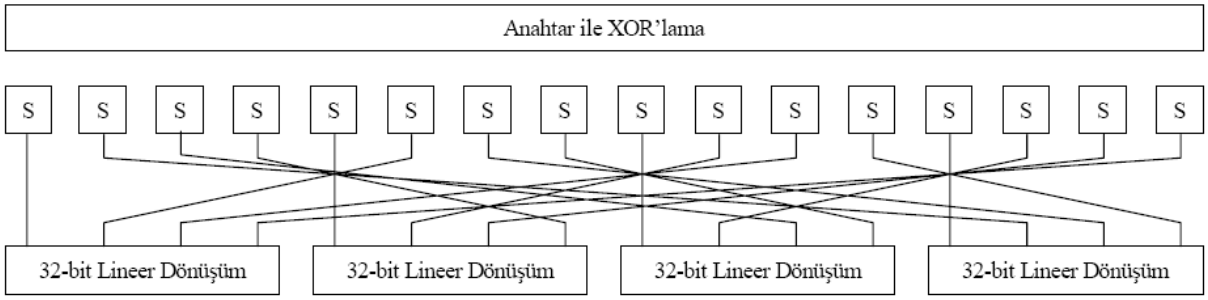
1.1.2.2.1. AES Blok Şifreleme Algoritmasında Doğrusal Dönüşüm

AES şifreleme algoritması verileri 128 bitlik bloklar şeklinde işleyen bir algoritmadır (Forouzan, 2008). Kullandığı anahtar uzunluğu 128, 196 ve 256 bit olarak değişebilir. AES şifreleme algoritmasının doğrusal dönüşüm işlemleri için Satırları Döndürme (ShiftRows) ve Sütunları Karıştırma (MixColumns) işlemleri uygulanır. Satırları Döndürme işlemlerinde, 4×4 byte dizisi şeklinde olan veri her bir satırın sola döndürülmesi şeklinde kaydırma işlemine tabi tutulur. 4×4 byte dizisi şeklinde alınan verinin ilk satıra hiçbir işlem yapılmaz, ikinci satır bir sola döndürme işlemine, üçüncü satır iki sola döndürme işlemine, dördüncü satır üç sola döndürme işlemine tabi tutularak yeni 4×4 byte dizisi şeklindeki veri elde edilmiş olur. Satırları döndürme işlemi için bir uygulama Örnek 1.1'de verilmiştir.

Örnek 1.1

$$\begin{bmatrix} 87 & F2 & E5 & 98 \\ A1 & B2 & C3 & D2 \\ 24 & 58 & 15 & C2 \\ D1 & 36 & AA & B8 \end{bmatrix} \begin{matrix} \rightarrow Döndürülmez \\ \rightarrow Bir\ sola\ döndürülür \\ \rightarrow İki\ sola\ döndürülür \\ \rightarrow Üç\ sola\ döndürülür \end{matrix} \rightarrow \begin{bmatrix} 87 & F2 & E5 & 98 \\ B2 & C3 & D2 & A1 \\ 15 & C2 & 24 & 58 \\ B8 & D1 & 36 & AA \end{bmatrix}$$

Sütunları Karıştırma (MixColumns) işlemleri 4 byte'lık dizilere bölünmüş verilerin, 4×4 byte dizisi şeklinde aşağıda verilen MDS matrisle (T) sonlu cisimde aritmetik çarpma işlemine tabi tutulmasıyla sağlanır. AES'de aritmetik işlemler, $GF(2^8)/x^8+x^4+x^3+x+1$ sonlu cisminde yapılır bundan dolayı da işlemler sırasında gerekli olan indirgeme işlemleri $x^8+x^4+x^3+x+1$ polinomuna göre yapılır. Bu çarpım işlemleriyle 4 byte şeklinde veriler doğrusal dönüşüme tabi tutularak yeni 4 byte'lık veriler elde edilmiş olur. AES şifreleme doğrusal dönüşümde kullanılan MDS matris involutif olmadığı için şifre çözme işlemi sırasında bu matrisin aynısı kullanılamaz, tersi kullanılır.



Şekil 1.3 AES Döngü Fonksiyonu (Daemen & Rijmen, 2002)

AES şifrelemede kullanılan dönüşüm matrisi T ve şifre çözmede kullanılan T^{-1} matrisleri aşağıda gösterilmektedir.

$$T = \begin{bmatrix} 02_h & 03_h & 01_h & 01_h \\ 01_h & 02_h & 03_h & 01_h \\ 01_h & 01_h & 02_h & 03_h \\ 03_h & 01_h & 01_h & 02_h \end{bmatrix}$$

$$T^{-1} = \begin{bmatrix} 0E_h & 0B_h & 0D_h & 09_h \\ 09_h & 0E_h & 0B_h & 0D_h \\ 0D_h & 09_h & 0E_h & 0B_h \\ 0B_h & 0D_h & 09_h & 0E_h \end{bmatrix}$$

AES'teki Sütunları Karıştırma işlemi için bir uygulama Örnek 1.2'de verilmektedir.

Örnek 1.2

1325BA45DE15A7B84453F153FCDA252A şeklindeki 128 bitlik veri Sütunları Karıştırma (MixColumns) işlemine tabi tutulsun.

Veri 4 byte şeklinde dört parçaya ayrılır. Bu parçalar dikey vektör şekline getirilerek AES doğrusal dönüşüm matrisiyle çarpım işlemine tabi tutulur ve veri doğrusal dönüşümünün bir adımı gerçekleştirilmiş olur.

$$\begin{bmatrix} 02_h & 03_h & 01_h & 01_h \\ 01_h & 02_h & 03_h & 01_h \\ 01_h & 01_h & 02_h & 03_h \\ 03_h & 01_h & 01_h & 02_h \end{bmatrix} \bullet \begin{bmatrix} 13_h \\ 25_h \\ BA_h \\ 45_h \end{bmatrix} = \begin{bmatrix} B6_h \\ C9_h \\ 96_h \\ 20_h \end{bmatrix}$$

$$\begin{bmatrix} 02_h & 03_h & 01_h & 01_h \\ 01_h & 02_h & 03_h & 01_h \\ 01_h & 01_h & 02_h & 03_h \\ 03_h & 01_h & 01_h & 02_h \end{bmatrix} \bullet \begin{bmatrix} DE_h \\ 15_h \\ A7_h \\ B8_h \end{bmatrix} = \begin{bmatrix} 87_h \\ BE_h \\ 4D_h \\ A0_h \end{bmatrix}$$

$$\begin{bmatrix} 02_h & 03_h & 01_h & 01_h \\ 01_h & 02_h & 03_h & 01_h \\ 01_h & 01_h & 02_h & 03_h \\ 03_h & 01_h & 01_h & 02_h \end{bmatrix} \bullet \begin{bmatrix} 44_h \\ 53_h \\ F1_h \\ 12_h \end{bmatrix} = \begin{bmatrix} 9E_h \\ F8_h \\ D8_h \\ 4A_h \end{bmatrix}$$

$$\begin{bmatrix} 02_h & 03_h & 01_h & 01_h \\ 01_h & 02_h & 03_h & 01_h \\ 01_h & 01_h & 02_h & 03_h \\ 03_h & 01_h & 01_h & 02_h \end{bmatrix} \bullet \begin{bmatrix} FC_h \\ DA_h \\ 25_h \\ 2A_h \end{bmatrix} = \begin{bmatrix} 99_h \\ 16_h \\ 12_h \\ B4_h \end{bmatrix}$$

şeklinde olur.

1.1.2.2.2. ARIA Blok Şifreleme Algoritmasında Doğrusal Dönüşüm

ARIA şifreleme algoritması (Chee vd., 2004, s. 432-445)'da verileri 128 bitlik bloklar şeklinde işleyen bir algoritmadır. Kullandığı anahtar uzunluğu 128, 196 ve 256 bit olarak değişebilir. ARIA doğrusal dönüşümünde 16×16 boyutunda involutif (tersi

kendisine eşit) bir MDBL matris kullanılır. Bu matris 16×16 ikili matrislerde olabilecek maksimum dallanma (branch) sayısı 8 değerine sahip bir matristir. Şifrelemek istenen veriler 16 bitlik dikey vektör olarak parçalara ayrılıp dönüşüm matrisiyle çarpılarak yeni veriler elde edilir. Bu dönüşüm matrisi (T) aşağıda gösterilmektedir. İşlemler $GF(2)$'de yapıldığı için doğrusal dönüşüm sonucunda her bir bit çıkışı, girişlerden bazılarının XOR toplamı olacak şekilde, bir doğrusal fonksiyon olarak ifade edilebilir.

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

1.2. Kriptanaliz

Kriptanaliz ile uğraşan bilim insanlarının (kriptanalist) amacı kripto sistemlerdeki zayıflıkları ve açıkları keşfedip, kripto sistemin güvenlik bariyerini kırmaktır. Kripto sistemler kayda değer bir kriptanalize karşı direnç göstermeden güvenli olarak düşünülmezler, bu nedenle profesyonel kriptanalistler, kripto sistemlerin oluşturulmasında ve gücünün değerlendirilmesinde önemli roller üstlenmiş olurlar.

Günümüzde ise teknolojinin gelişmesi ile kriptanalitik yöntemler de farklılaşmıştır. 19. yy başlarında Auguste Kerckhoff bir takım prensipler ortaya koyarak güvenli kripto sistem için belirli şartlardan bahsetmiştir. Bu prensiplere göre saldırganın kripto sistemin bazı özelliklerini bildiği kabul edilir. Saldırgan sahip olduğu bu bilgileri kullanarak, şifrenin oluşturulma mantığını çözmeye çalışır ve kriptanaliz için farklı yöntemler seçer. Saldırganın önceden sahip olabileceği bu bilgiler şunlar olabilir: şifreli metinlerin olduğu bir dizi, açık metinler ile bu metinlerin şifreli karşılıkları, açık metinlerden şifreli metinler oluşturabilme, şifreli metinlerden bu metinlerin açık hallerine erişebilme gibidir. Saldırgan aynı zamanda bir şifreleme algoritmasını çözebilmek için birden çok kriptanaliz yöntemi kullanabilir. Günümüzde kullanılan kriptanaliz yöntemlerinin en önemlilerinden ikisi diferansiyel ve doğrusal kriptanalizdir (Biham & Shamir, 1990, s. 3-72., Matsui, 1993).

1.2.1. Diferansiyel Kriptanaliz

Diferansiyel kriptanaliz 1990'da Eli Biham ve Adi Shamir tarafından keşfedilmiştir (Biham & Shamir, 1990, s. 3-72). Genellikle blok şifreleme algoritmalarına karşı uygulanmalarına rağmen akan şifreler ve hash (özet) fonksiyonlarına karşı da uygulanabilirler. Saldırgan, bu kriptanaliz yönteminde, kripto sisteme ait tüm açık metinlerin olduğu açık metin dizisinden istediği bir çift metni seçip, bu metinlerin şifreli karşılıklarını elde eder. Daha sonra seçtiği açık metinler arasında bulunan özel farkların, bu metinlerden elde edilen şifreli metin çiftinde ne kadar farklılık oluşturduğunu inceler. Bu işlem yapılırken, seçilen metin çiftleri arasında bulunan farklara karşılık son döngüden önceki durum bitleri farkı elde edilir. Daha sonra bütün açık-şifreli metin çiftlerine olası anahtar değerleri uygulanır. Uygun bir değer bulunursa sayaç değeri bir artırılarak, bu işlem bütün olası anahtarlar için tekrarlanır. Sayaç değeri en büyük olan olası anahtar orijinal anahtar olarak kabul edilir (Sakallı, 2006).

Blok şifrelerin tasarlanmasında kullanılan S-kutuları algoritmada kullanılan en önemli elemandır. Çünkü doğrusal dönüşüm benzeri işlemlerin aksine veriler doğrusal olmayan bir şekilde S-kutularının kullandığı fonksiyonlara göre karıştırılmaktadır. S-kutularının bazı özellikleri taşımaları gerekmektedir. Bu özelliklerden biri girişteki bitlerden yalnız 1 bit'in değişmesi halinde çıkıştaki tüm bitlerin yarısı değişmiş

olmalıdır (çığ etkisi) (Sakallı, 2006). S-kutularının giriş, çıkış bit uzunluğu mümkün olduğunca büyük olmalıdır fakat çok büyük S-kutuları uygulama açısından da büyük bir maliyet getireceğinden dikkatli olunmalıdır. S-kutusunun çıkış değerlerinin, kolaylıkla giriş değerlerinin bir doğrusal fonksiyonu olarak yazılabilmesinin önüne geçilmelidir. Çıkış değerleri kolaylıkla giriş değerlerinin bir doğrusal fonksiyonu olarak yazılabilen S-kutuları kullanan şifreler doğrusal kriptanaliz benzeri saldırılara karşı dirençli olamazlar (Stallings, 2005, s. 88).

1.2.2. Doğrusal Kriptanaliz

Doğrusal kriptanaliz ilk olarak 1992'de Mitsuru Matsui tarafından blok şifrelere karşı teorik bir saldırı olarak düşünülmüş daha sonra DES şifreleme algoritmasına karşı başarı ile uygulanmıştır (Matsui, 1993). Günümüzde blok şifrelere karşı en geniş kullanım alanına sahip yöntemdir. Doğrusal kriptanaliz temel olarak açık metin, şifreli metin ve anahtar bitleri arasındaki olabilecek doğrusal ilişkiyi istatistiksel olarak ortaya koymaya çalışır. Saldırganın elinde açık metin dizileri ve bunların oluşturduğu şifreli metin dizileri vardır. Saldırgan elindeki açık metindeki bazı bitlerle şifreli metindeki bazı bitlerin doğrusal olarak ifadesinden anahtar bitlerini elde etmeye çalışır. Bu işlem ise S-kutularının incelenmesi ile yapılır. Bu yöntemle S-kutusunun girdi ve çıktı bitleri arasındaki bütün mümkün eşitlikler bulunur. Bu eşitlikleri bulmak için, açık metin bitleri ile en son döngüden önceki durum bitleri arasındaki doğrusal ilişkinin tespit edilmesi gerekmektedir. Elde edilen bu bilgi anahtar bitlerinin tamamına uygulanarak bir sapma değeri elde edilir ve bu değer teorik sapma değeri ile kıyaslanır. Sapma değeri en yüksek olan aday hedeflenen anahtar olarak kabul edilir. Eğer bu sapma çok küçük ise seçilen anahtar doğru olmayacaktır (Sakallı, 2006).

1.3. MDS (Maximum Distance Separable-Maksimum Uzaklıkta Ayrılabilen) Matrisler

Birçok blok şifre tasarımında (ya da kriptografik yapıların tasarımında) doğrusal dönüşüm olarak MDS (Maximum Distance Separable-Maksimum Uzaklıkta Ayrılabilen) matrisler kullanılmaktadır. Örneğin, AES blok şifresi byte değerleri giriş olarak alan 4×4 boyutunda bir MDS matris kullanır. MDS matrislerin kullanıldığı diğer blok şifrelere örnek olarak Twofish (Ferguson vd., 1998), SHARK (Bosselaers, Daemen, Preneel, Rijmen & Win, 1996, s. 99-102), Square (Daemen, Knudsen &

Rijmen, 1997), Khazad (Barreto & Rijmen, 2000c) ve Clefia (Furuya, Preneel, Takaragi, Yoshida & Watanabe, 2002, s. 179-194) verilebilir. MDS matrislerin yayılımın sağlanması amacıyla kullanıldığı hash (özet) fonksiyonlarına örnek olarak ise Maelstrom (Schneier, 1996), Grøstl (Gauravaram vd., 2008) ve Photon hafif siklet hash fonksiyonları ailesi (Guo, Peyrin & Poschmann, 2011, s. 222-239) gibi hash (özet) fonksiyonları verilebilir.

1994 yılında Vaudenay iyi seviyede yayılım (diffusion) sağlanması için MDS matrislerin kullanılmasını önermiştir (Hong, Lin & Xuejia, 2014, s. 552-563). Ayrıca Vaudenay çoklu permütasyonlarla güçlendirilmeyen yayılım katmanlarının, nasıl kriptanalizle kolaylıkla kırılabileceğini de göstermiştir. Bu düşünce daha sonra Daemen tarafından geliştirilmiş ve dallanma sayısı olarak isimlendirilmiştir. Daemen, en kuvvetli yayılım katmanlarının, en fazla dallanma sayısına sahip matrislerle diğer bir deyişle MDS matrislerle sağlanabileceğini ileri sürmüştür.

MDS matris tasarımında dairesel (circulant) matrislerden ve Hadamard matrislerden faydalanılır. Donanım uygulamalarında dairesel matrisler kullanmanın en göze çarpan özelliği, matrislerin bütün satırlarının aynı elemanlardan oluşmasıdır. Matrisin ilk satırını oluşturduktan sonra bir sonraki satır için üsteki satırın bir sağa döndürülmesi yeterlidir. Böylelikle uygulama maliyetlerinde büyük avantaj sağlanabilir. MDS matrislerin tasarımında Hadamard matrisleri kullanmak involutif matris ($A = A^{-1}$) oluşturmak için büyük bir avantaj sağlar çünkü bu tip matrislerden kolaylıkla involutif matrisler elde edilebilir.

1.4. Tez Konusu ve Önemi

MDS matrislerin yayılım katmanında kullanılmasının şifrelerin gücünü artırdığından ve şifreleri doğrusal ve diferansiyel gibi çeşitli kriptanaliz saldırılarına karşı daha dirençli hale getirdiğinden MDS matrisler büyük bir önem kazanmıştır. Bundan dolayı MDS matris tasarlanması çok ilgi çeken bir alan olmuştur. Literatürde MDS matrislerin elde edilmesi için çeşitli yöntemler mevcuttur. Bu yöntemler aşağıdaki gibi verilebilir:

- (Bosselaers, Daemen, Preneel, Rijmen & Win, 1996, s. 99-102)'de Gabidulin kod teorisi uygulanarak MDS matrisler tasarlanmaktadır.

- (Guo, Peyrin & Poschmann, 2011, s. 222-239., Gupta & Ray, 2013, s. 29-43)'de eş (companion) matrislerden yoğun arama yapılarak hafif siklet MDS matrisler tasarlanmaktadır.
- (Augot & Finiasz, 2015, s. 3-17)'de kısaltılmış BCH (Bose-Chaudhuri-Hocquengham) kodlar kullanılarak MDS matrisler tasarlanmaktadır.
- (MacWilliams & Sloane, 1998, s. 299-316)'de kısaltılmış RS (Reed Solomon) kodlar kullanılarak MDS matrisler tasarlanmaktadır.
- (Dakhilalian, Mala, Omoomi & Sajadieh, 2012a, s. 1-22)'de Vandermonde matrisler kullanılarak MDS matrisler tasarlanmaktadır.
- (Mister, Tavares & Youssef, 1997, s. 40-48)'de Cauchy matrisler kullanılarak MDS matrisler tasarlanmaktadır.
- (Junod & Vaudenay, 2004, s. 84-99)'de heuristik yöntemler kullanılarak MDS matrisler tasarlanmaktadır.
- (Mister, Tavares & Youssef, 1997, s. 40-48)'de rastsal tasarım kullanılarak MDS matrisler tasarlanmaktadır.

Bu tezde $GF(2^m)$ üzerine tanımlı MDS matrisler ile $GF(2^{mt})$ ($t \geq 1$ ve $m > 1$) üzerine tanımlı MDS matrisler arasındaki otomorfizma ve izomorfizma ilişkisi incelenmektedir. Buna ek olarak $GF(2^m)$ üzerine tanımlı MDS matrislerden aynı boyutta $GF(2^{mt})$ ($t \geq 1$ ve $m > 1$) üzerine MDS matrislerin nasıl elde edilebileceği araştırılmaktadır. Sonlu cisim üzerine tanımlanan MDS matrisler için bu ilişkileri ifade edebilecek bir yöntemin geliştirilmesi var olan MDS matrislerden yenilerinin (uygulama anlamında farklı) elde edilmesini sağlayacaktır. Dolayısıyla bu yöntem, literatürde var olan tüm yöntemlerle elde edilecek MDS matrislerden farklı MDS matrislerin (herhangi bir tasarım ya da arama yöntemi olmaksızın) elde edilmesini sağlayacağından diğer yöntemleri tamamlayıcı bir yöntem olarak değerlendirilebilir.

BÖLÜM 2

2. MATEMATİK ALTYAPI

Bu bölümde tez konusu ile ilgili gerekli matematik altyapı sunulmaktadır. MDS matrisler, izomorfizma, otomorfizma gibi tez boyunca gerekli konular hakkında tanımlar yapılmakta, gerekli teorem ve önermeler verilmektedir.

2.1. Sonlu Cisimler

Tanım 2.1.1 (Nesin, 2013). x,y tamsayı ve n pozitif tamsayı olsun. Eğer n, $y-x$ i bölüyorsa $x \equiv y\,(mod\ n)$ şeklinde yazabiliriz. $x \equiv y\,(mod\ n)$ ifadesine denklik denir ve x, y'ye $mod\, n$'e göre denktir denir. Tamsayı n'ye de modulo denir.

Aritmetik modulo $n: Z_n$ $\{0,1,...,n-1\}$ kümesi ile iki işlem toplama ve çarpma tabanlı tanımlanabilir. Z_n'de toplama ve çarpma işlemleri gerçek toplama ve çarpma işlemleridir ve sadece sonuçlar modulo n'ye göre indirgenmektedir. Z_n'de toplama ve çarpma işleminde çeşitli aksiyomlar vardır. Bunlar aşağıdaki gibidir.

1- Toplamada kapalılık özelliği:

$x,y \in Z_n$ için $x+y \in Z_n$

2- Toplamada değişme özelliği:

$x,y \in Z_n$ için $x+y=y+x$

3- Toplamada geçişme özelliği:

$x,y,z \in Z_n$ için $(x+y)+z=x+(y+z)$

4- Toplama etkisiz eleman 0:

$x,y \in Z_n$ için $x+0=0+x=x$

5- Toplamaya göre ters eleman:

$x \in Z_n$ için x in toplamaya göre tersi $n - x$ 'dir.

6- Çarpmada kapalılık özelliği:

$x, y \in Z_n$ için $x \cdot y \in Z_n$

7- Çarpmada değişme özelliği:

$x, y \in Z_n$ için $x \cdot y = y \cdot x$

8- Çarpmada geçişme özelliği:

$x, y, z \in Z_n$ için $(x \cdot y) \cdot z = x \cdot (y \cdot z)$

9- Çarpma işleminde etkisiz eleman 1'dir.

$x, y \in Z_n$ için $a \cdot 1 = 1 \cdot a = a$

10- Dağılma özelliği sağlanır.

$x, y, z \in Z_n$ olmak üzere $(x + y) \cdot z = x \cdot z + y \cdot z$ ve $x \cdot (y + z) = x \cdot y + x \cdot z$

Tanım 2.1.2 (Lidl & Niederreiter, 1986). Yukarıda verilen aksiyomlardan 1, 3, 4, 5 aksiyomlarını sağlayan Z_n cebirsel yapısına grup denir. Eğer bahsedilen aksiyomlarla beraber Z_n cebirsel yapısı 2'inci aksiyomu da sağlıyorsa abelian grup adını alır.

Tanım 2.1.3 (Lidl & Niederreiter, 1986). Yine verilen aksiyomlardan 1, 2,.., 10 aksiyomlarını sağlayan Z_n cebirsel yapısına halka denir. Örnek olarak tamsayılar, reel sayılar ve karmaşık sayılar halka örneklerindendir. Buna ek olarak bu örnekler sonsuz halka örneklerindendir.

Tanım 2.1.4 (Lidl & Niederreiter, 1986). Tanım 2.1.1'deki aksiyomlara ek olarak toplama ve çarpmaya göre ters alma işlemini sağlayan cebirsel yapıya cisim adı verilir.

Örneğin Z_5 'te toplama ve çarpma işlemini inceleyelim;

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Şekil 2.1 Z_5'te Toplama ve Çarpım İşlemleri

Z_5 cebirsel yapısı Tanım 2.1.1'de verilen 10 aksiyomun tamamını sağlamaktadır. Buna ek olarak 0 haricinde bütün elemanların tersinin olduğu görülmektedir. Bundan dolayı Z_5 cebirsel yapısı cisim oluşturur.

Teorem 2.1.1 (Lidl & Niederreiter, 1986). Eğer n bir asal sayı ise Z_n bir cisim oluşturur.

Teorem 2.1.2 (Forouzan, 2008). p asal sayı ve $\alpha \in Z_n$ olsun. O zaman $\frac{p-1}{q}$ olacak şekilde tüm asal q'lar için $\alpha^{\frac{p-1}{q}} \neq 1 mod\ p$ şeklinde ise $\alpha\ mod\ p$'ye göre ilkel elemandır.

Teorem 2.1.3 (Murphy, 2001, s. 27-29, s. 55-56). Sonlu sayıda elemanlardan oluşan cisimlere sonlu cisimler denir. q bir asal sayı ve $Zq = \{0,1,2,...q-1\}$ q tane elemandan oluşan bir kümede modulo q toplama ve çarpma işlemlerinin tanımlanmasıyla sonlu bir cisim elde edilir. Bu sonlu cisim $GF(q)$ sonlu Galois cismi olarak adlandırılır. Bir Galois cismi q taban olmak üzere $GF(q^n)$ olarak q^n elamandan oluşacak şekilde genişletilebilir. Böyle cisimleri $GF(q)$ nun genişletilmiş cismi denir.

2.1.1. Genişletilmiş Sonlu Cisimlerde Toplama, Çarpma İşlemleri

Şifreleme algoritmalarında genellikle genişletilmiş cisimler kullanıldığı için genişletilmiş cisimlerde işlemler anlatılmaktadır.

2.1.1.1. Genişletilmiş Sonlu Cisimlerde Toplama İşlemi

Sonlu cisimlerde toplama işlemi, normal polinomlarda olduğu gibidir ama birkaç farkı da beraberinde taşımaktadır. Sonlu cisimler belli bir tabanda ve bir indirgenemez polinomla tanımlı sonlu yapılardır. Sonlu cisimde işlemler, cismin tanımlı olduğu uzayın tabanına göre mod alarak gerçekleştirilir. Sonlu olmalarının gereği olarak belli bir yerden sonra indirgemeye tabi tutulmaktadırlar. Tanımlı oldukları polinomun derecesini geçen bir işlem değerine ulaşıldığı zaman o işlem, $mod(p(x))$'e (cismin tanımlı olduğu polinom) göre indirgemeye tabi tutulur. Örneğin, $GF(2^4)/(x^4+x+1)$ cisminde işlem yapılacaksa işlemler cismin tabanı 2 olduğu için modulo 2'ye göre yapılır ve cismin derecesi 4 olduğu için maksimum x^3'e kadar çıkan işlem sonuçları aynen korunur. x^3'ten sonraki işlem sonuçları için x^4 yerine $x+1$ yazılarak işleme devam edilir ($x^4+x+1=0$, $x^4=-x-1$, mod2 ye göre işlem yapıldığı için $-x-1$ ile $x+1$aynı şeyi ifade eder).

Örnek 2.1 $x^4+x^3+x^2+1$ ve $x^7+x^3+x^2$ ifadelerini $GF(2)$ ye göre toplanırsa,

$$(x^3 \oplus x^2 \oplus 1) \oplus (x^7 \oplus x^3 \oplus x^2) \oplus (x^7 \oplus x^3) = (2x^7 \oplus 3x^3 \oplus 2x^2 \oplus 1) = (x^3 \oplus 1)$$

İşlemler $GF(2)$'de yapıldığı için aynı dereceye sahip olan terimlerin toplanması sonucu oluşan terimlerin katsayısı modulo 2 işlemine tabi tutulur ve 0 veya 1 değerini alır. Aynı işlem $GF(3)$'e göre yapılırsa;

$$(x^3+x^2+1)+(x^7+x^3+x^2)+(x^7+x^3)=(2x^7+3x^3+2x^2+1)=(2x^7+2x^2+1)$$

yukarıda gösterildiği gibi toplama sonucu oluşan katsayılar modulo 3 işlemine tabi tutulur.

2.1.1.2. Genişletilmiş Sonlu Cisimlerde Çarpma İşlemi

Sonlu cisimlerde çarpma işlemi polinomsal ifadenin çarpımı olarak düşünülürse, çarpma ifadesinde yer alan iki terimin katsayıları birbiriyle normal aritmetik işlem kurallarına göre çarpılır. İşlem sonucu çıkan terimlerin katsayıları üzerinde işlem yapılan sonlu cismin tabanına göre modulo işlemine tabi tutulur. Terimlerin dereceleri genişletilmiş sonlu cisimlerde çarpma yapılıyorsa cisimde kullanılan polinoma göre modulo işlemine tabi tutulur (indirgenir). Örneğin $GF(2^4)/x^4+x+1$ genişletilmiş sonlu cisminde x^3+x^2+1 ve x^3+x+1 ifadeleri çarpılsın. Çarpma işlemi yapılırken, işlemler birkaç adıma ayrılır. Öncelikli olarak çarpma işlemine tabi ifadelerden bir tanesi sabit olarak alınır, diğer ifadenin bütün terimleriyle tek tek çarpılır. İşlem kolaylığı açısından terim sayısı çok olan ifade sabit olarak alınabilir. $GF(2)$'de genişletilmiş cisimlerde işlem yapıldığı için terimler ikili notasyon üzerinden gösterilebilir. Bu aşamadan itibaren örneğimize ikili notasyon gösterimi üzerinden devam edilecek.

İkili notasyonda,

$$x^3+x^2+1=1101$$

$$x^3+x+1=1011$$

olarak gösterilebilir. Örnekteki 1101 ifadesi sabit alınsın, 1011 ifadesinin bütün terimleriyle tek tek çarpılsın. Çarpmaya en küçük dereceli terimden başlayıp sırasıyla devam etmek kolaylık sağlayacaktır.

Önce derecesi 0 olan 1 terimiyle çarpılsın.

$$(1101)\cdot(1)=(1101)$$

$GF(2)$'de işlem yapıldığı için terimlerin katsayılarla ilgili bir indirgeme işlemine ihtiyaç duyulmamaktadır fakat $GF(2)$ haricinde başka cisim tabanlarında yapılırsa katsayılar çarpılıp işlem yapılan cismin tabanına göre modulo işlemine tabi tutulur.

İkinci adım olarak sabit terim derecesi 1 olan x terimiyle çarpılsın. Sonlu cisimde bir ifadeyi x ile çarpmak demek; o ifadeyi 1 sola döndürmek demektir, ayrıca döndürme sırasında kaybedilen en soldaki sayı 0 ise ilave bir işleme gerek duyulmaz, 1 ise bulunan

sonuç cismin tanımlı olduğu polinoma göre modulo işlemine tabi tutularak sonuç bulunur.

$(1101)\otimes(x)$

1101 bir sola döndürülürse 1010 sonucu bulunur, döndürme sırasında en soldaki 1 kaybedildiği için bulunan sonuç cisimde kullanılan polinomla cismin tabanında modulo işlemine tabi tutulur. Cismin polinomu x^4+x+1 olduğu için x^4 bulunur ve indirgeme işlemi buna göre yapılır.

$x^4=-x-1=x+1=0011$

Bir önceki adımda sola döndürme sonucu bulunan 1010 ile $x^4=-x-1=x+1=0011$ cismin tabanına göre modulo işlemine tabi tutulur. $GF(2)$'de işlem yapıldığı için cismin tabanı 2 dir. Modulo 2 ye göre işlem yapmak XOR işlemiyle aynı olduğu için işlem aşağıdaki gibi yazılıp,

$(1010)\oplus(0011)=(1001)$

$(1101)\otimes x=(1001)$

Daha sonra derecesi 2 olan, x^2'li terim ile çarpma işlemine geçilir. Sabit olarak ayırılan ifadenin x ile çarpım sonucu daha önce bulunduğu için bu x ile çarpılmasıyla edilen sonuç bir daha x ile çarpılmaya tabi tutularak ifadenin x^2 ile çarpımı bulunmuş olur.

$(1101)\otimes(x)=(1001)$

$(1101)\otimes(x)\otimes(x)=1001\otimes x$

Yukarıda x ile çarpım ile ilgili anlatılan aynen uygulanırsa ifade önce sola döndürülür, döndürmede en soldaki 1 kaybedildiği için x^4 $(x^4=-x-1=x+1=0011)$ ile indirgenir.

1001 sola döndürülürse 0010 bulunur,

x^4 ile indirgenirse

$(0010)\oplus(0011)=0001$

$(1101) \otimes x^2 = 0001$

Daha sonra derecesi 3 olan, x^3'lü terim ile çarpma işlemine geçilir. Sabit olarak ayırılan ifadenin x^2 ile çarpım sonucu daha önce bulunduğu için bu x^2 ile çarpılmasıyla edilen sonuç bir daha x ile çarpılmaya tabi tutularak ifadenin x^3 ile çarpımı bulunmuş olur. Daha yüksek dereceli terimlerin olduğu ifadelerin çarpımlarında bu şekilde devam edilir.

$(1101) \otimes (x) \otimes (x) = 0001$

$(1101) \otimes x^3 = (1101) \otimes (x) \otimes (x) \otimes (x) = 0001 \otimes x$

Çarpım işlemi için sola döndürme yapılır. Kayıp olmadığı için x^4 ile indirgemeye gerek olmaz.

$(1101) \otimes x^3 = 0001 \otimes x = 0010$

Çarpım işleminde sabit alınan 1101 ifadesini $x^3 + x + 1 = 1011$ ifadesinin bütün terimleriyle çarpıldığı için $(1101) \otimes x^3, (1101) \otimes x$ *ve* $(1101) \otimes 1$ sonuçları sonlu cismin tabanına göre modulo işlemine tabi tutulur. Örnek için ifade edilirse bulunan 3 sonuç XOR işlemine tabi tutulur.

$$((1101) \otimes x^3) \oplus ((1101) \otimes x) \oplus ((1101) \otimes 1)$$
$$= (0010) \oplus (1001) \oplus (1101)$$
$$= (0110)$$

sonucu bulunur.

Çarpma işleminde xtime ve table lookup işlemlerinden faydalanılabilir.

Xtime (β ile Çarpma) İşlemi :

xtime işlemi sonlu cisimlerde bir sayıyı β veya 02_h ile çarpma işlemidir. Çarpma işleminin $GF(2)$'de olduğu düşünülürse, sayılar ikili notasyonda yazılır. 02_h sayısı (10) şeklinde olacağı için diğer sayıyı (10) ile çarpmak demek onu bir sola kaydırmak demektir. Kaydırma işlemi sonucu en soldaki 1 kaybediliyorsa bölüm

2.1.1.2'de ayrıntılı olarak anlatıldığı üzere cismin tanımlı olduğu polinom üzerinden indirgeme işlemi yapılır.

Table Lookup (Tablo Okuma) ile Çarpma İşlemi :

Sonlu cisimlerde çarpma yapmanın diğer bir kolay yolu, öncelikli olarak cismin tablosunu oluşturulması daha sonra bu tablodan faydalanılarak çarpım işleminin yapılmasıdır. Cisimlerde eleman sayısı tanımlı oldukları polinomun derecesine göre değişir. $GF(2)$de işlem yaptığımızı düşünürsek n polinomun derecesi olmak üzere, toplam eleman sayısını 2^n dir. Cismin eleman sayısı kadar kolon ve satıra sahip bir tablo üzerinde bütün olası çarpım işlemlerinin sonuçları depolanır. Çarpmaya ihtiyaç duyulduğu zaman sonuçlar direkt bu tablodan bulunur. Cisim elemanları, cismin ilkel bir elemanının kuvvetleri şeklinde ifade edilebilir. Örnek olarak Şekil 3.1.1'de $GF(2^4)/x^4+x+1$cisminin elemanlarının üssel ve onaltılık (hexadecimal) gösterimi verilmektedir. Tablodan bütün elemanların x'in üssü şeklinde ifade edilebileceği görülebilir. Örneğin, cisim elemanlarından x^3+x $(1010_h = x^9)$ ile x^2+1 $(0100_h = x^8)$ elemanı çarpılmak istenirse elemanların üssel olarak çarpılması yeterlidir. $x^9 \times x^8 = x^{17}$ sonucu bulunur. Cisim $GF(2^4)$'de tanımlı olduğu için bulunan üs değerinin 15 (2^4-1)'e göre modu alınır. $x^{17\,mod(15)} = x^2$ olduğundan dolayı çarpım işleminin sonucu x^2 (0100_h) dir. Cismin tanımlı olduğu uzay büyükse cismin tablosunun oluşturulması çok maliyetli olabilir. Örneğin, $GF(2^{16})$'da tanımlı bir cismin tablosu oluşturulmak istenirse 65536 (2^{16}) elemanlı bir tablo oluşturulması gerekir.

2.2 MDS Matrisler ile İlgili Altyapı

Bu bölümde kriptografik uygulamalarda önemli bir yer teşkil eden MDS matrisler ile ilgili bir altyapı sunulmaktadır.

Tanım 2.2.1 (Daemen & Rijmen, 2002). $[nxn]$ boyutundaki bir A: $(GF(2^m))^n \rightarrow (GF(2^m))^n$ matrisinin diferansiyel dallanma sayısı aşağıda verildiği gibi tanımlanabilir:

$$\beta_d(A) = min\ \{wt(x)+wt(A \cdot x^T) \mid x \in (GF(2^m)^n, x \neq 0\}$$

Tanım 2.2.2 (Daemen & Rijmen, 2002). $[nxn]$ boyutundaki bir A: $(GF(2^m))^n \rightarrow (GF(2^m))^n$ matrisinin doğrusal dallanma sayısı aşağıda verildiği gibi tanımlanabilir:

$$\beta_l(A) = min\ \{wt(x)+wt(A^T \cdot x^T) \mid x \in (GF(2^m)^n, x \neq 0\}$$

Bu tez çalışmasında $GF(2^m)$ üzerine matrislerin dallanma sayılarının elde edilmesinde Magma yazılım paketi (Bosma, Cannon & Playoust, 1997, s. 235-265) kullanılmıştır. Örnek 2.2'de 8×8 boyutunda $GF(2^4)$ üzerine tanımlı bir matrisin dallanma sayısı değerinin elde edilmesi için Magma kodu verilmektedir.

Örnek 2.2 x^4+x+1 ile tanımlı $GF(2^4)$ cisminden 8×8 bir Hadamard matris aşağıdaki gibidir. Bu matris MDS bir matristir. Dolayısıyla dallanma sayısı değeri 9'dur

$$A = \begin{bmatrix} x & x^{12} & x^6 & x^8 & x^9 & x^2 & x^3 & x^4 \\ x^{12} & x & x^8 & x^6 & x^2 & x^9 & x^4 & x^3 \\ x^6 & x^8 & x & x^{12} & x^3 & x^4 & x^9 & x^2 \\ x^8 & x^6 & x^{12} & x & x^4 & x^3 & x^2 & x^9 \\ x^9 & x^2 & x^3 & x^4 & x & x^{12} & x^6 & x^8 \\ x^2 & x^9 & x^4 & x^3 & x^{12} & x & x^8 & x^6 \\ x^3 & x^4 & x^9 & x^2 & x^6 & x^8 & x & x^{12} \\ x^4 & x^3 & x^2 & x^9 & x^8 & x^6 & x^{12} & x \end{bmatrix} = \begin{bmatrix} 2_h & F_h & C_h & 5_h & A_h & 4_h & 8_h & 3_h \\ F_h & 2_h & 5_h & C_h & 4_h & A_h & 3_h & 8_h \\ C_h & 5_h & 2_h & F_h & 8_h & 3_h & A_h & 4_h \\ 5_h & C_h & F_h & 2_h & 3_h & 8_h & 4_h & A_h \\ A_h & 4_h & 8_h & 3_h & 2_h & F_h & C_h & 5_h \\ 4_h & A_h & 3_h & 8_h & F_h & 2_h & 5_h & C_h \\ 8_h & 3_h & A_h & 4_h & C_h & 5_h & 2_h & F_h \\ 3_h & 8_h & 4_h & A_h & 5_h & C_h & F_h & 2_h \end{bmatrix}$$

Aşağıda verilen Magma kodu yardımıyla MDS matris olma durumu doğrulanabilir.

```
P<z> := PolynomialRing(GF(2));

p := z^4+z+1;

F<x> := ext <GF(2) | p >;

A:=Matrix(F,8,8,[

x,x^3+x^2+x+1,x^3+x^2,x^2+1,x^3+x,x^2,x^3,x+1,

x^3+x^2+x+1,x,x^2+1,x^3+x^2,x^2,x^3+x,x+1,x^3,

x^3+x^2,x^2+1,x,x^3+x^2+x+1,x^3,x+1,x^3+x,x^2,

x^2+1,x^3+x^2,x^3+x^2+x+1,x,x+1,x^3,x^2,x^3+x,

x^3+x,x^2,x^3,x+1,x,x^3+x^2+x+1,x^3+x^2,x^2+1,

x^2,x^3+x,x+1,x^3,x^3+x^2+x+1,x,x^2+1,x^3+x^2,

x^3,x+1,x^3+x,x^2,x^3+x^2,x^2+1,x,x^3+x^2+x+1,

x+1,x^3,x^2,x^3+x,x^2+1,x^3+x^2,x^3+x^2+x+1,x]);

I := IdentityMatrix(F,8);

C := LinearCode(HorizontalJoin(I,A));

MinimumWeight(C);
```

Tanım 2.2.3 (Mister, Tavares & Youssef, 1997, s. 40-48., Nakahara & Abrahao, 2009, s. 109-116). Bir $GF(2^m)$ üzerine bir $[n,k,d]$ kod, vektör uzayı $(GF(2^m))^n$'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 $[kxn]$ boyutunda bir matristir. Bir doğrusal $[n,k,d]$-kod $d \leq n-k+1$ Singleton sınırını karşılıyorsa bu koda MDS kod adı verilir.

Tanım 2.2.4 (Mister, Tavares & Youssef, 1997, s. 40-48., Nakahara & Abrahao, 2009, s. 109-116). $[nxn]$ boyutunda bir matris için MDS matris olma şartı, satır ve sütunlarından oluşturulan tüm alt kare matrislerinin determinantının 0'dan farklı olmasıdır. Alt kare matrisler bulunurken $2 \le i \le n-1$ aralığında tüm i ler için, i sayıda satır ve i sayıda sütun silinerek alt kare matrisler elde edilir.

Açıklama 2.2.1 Bir MDS matrisin bütün elemanları sıfırdan farklı olmalıdır.

Açıklama 2.2.2 $[nxn]$ boyutunda bir A matrisi MDS ise A'nın dallanma sayısı (branch number) $n+1$ dir.

Önerme 2.2.1 $GF(2^m)$ üzerine bir A matrisi MDS ise A'nın bir satırının (veya kolonunun) sabit bir $c \in GF(2^m)$ sayısıyla çarpımından veya satırların (veya sütünların) permütasyonundan elde edilen A' matrisi, MDS matristir. Buna ek olarak, A bir MDS matris ise, A^T de bir MDS matristir.

Tanım 2.2.5 Bir A kare matrisi, $A^2 = I$ şartını sağlıyorsa yani A'nın tersi kendisine eşitse $(A = A^{-1})$ A involutif matris olarak isimlendirilir.

Tanım 2.2.6 Bir A kare matrisi, $A \cdot A^T = I$ şartını sağlıyorsa A ortogonal matris olarak isimlendirilir.

Tanım 2.2.7 Aralarında asal iki sayı n ve q olsun. q'nun mod n' ye göre siklotomik koseti (i'yi içerecek şekilde)

$$C_i = \left\{ (i.q^j (mod\ n)) \in Z_n : j = 0,1,..... \right\}$$

şeklinde tanımlanabilir. Z_n'in bir alt seti $\{i_1,.....,i_t\}$, $C_{i_1},.....,C_{i_t}$ birbirlerinden farklı ve $U_{j=1}^{t} C_{i_j} = Z_n$ ise $q\ mod\ n$'in siklotomik koset temsilcilerinin toplam seti olarak adlandırılır.

Örnek 2.3 2'nin mod 15'e göre siklotomik kosetlerini aşağıdaki gibi elde edilebilir.

Tanım 2.3.7 yi kullanarak aşağıdaki gibi bulunabilir.

$1\cdot 2^0 (mod\,15) \equiv 1 \qquad 3\cdot 2^0 (mod\,15) \equiv 3 \qquad 7\cdot 2^0 (mod\,15) \equiv 7 \qquad 5\cdot 2^0 (mod\,15) \equiv 5$

$1\cdot 2^1 (mod\,15) \equiv 2 \qquad 3\cdot 2^1 (mod\,15) \equiv 6 \qquad 7\cdot 2^1 (mod\,15) \equiv 14 \qquad 5\cdot 2^1 (mod\,15) \equiv 10$

$1\cdot 2^2 (mod\,15) \equiv 4 \qquad 3\cdot 2^2 (mod\,15) \equiv 12 \qquad 7\cdot 2^2 (mod\,15) \equiv 13$

$1\cdot 2^3 (mod\,15) \equiv 8 \qquad 3\cdot 2^3 (mod\,15) \equiv 9 \qquad 7\cdot 2^3 (mod\,15) \equiv 11$

$C_0 = \{0\}, \qquad C_1 = \{1,2,4,8\}, \qquad C_3 = \{3,6,9,12\}$
$C_5 = \{5,10\}, \qquad C_7 = \{7,11,13,14\}$

Yukarıdan da anlaşılacağı gibi $C_1 = C_2 = C_4 = C_8$ şeklindedir. O zaman $\{0,1,3,5,7\}$ kümesi 2'nin mod 15'e göre siklotomik kosetlerinin temsilcilerinin toplam bir kümesidir.

Tanım 2.2.8 $a_m \in GF(2^k)$ ve $k \in Z^+$ olmak üzere mxm dairesel matris aşağıdaki gibidir.

$$circ(a_1, a_2, ..., a_m) = \begin{bmatrix} a_1 & a_2 & . & . & . & a_{m-1} & a_m \\ a_m & a_1 & . & . & . & a_{m-2} & a_{m-1} \\ a_{m-1} & a_m & . & . & . & a_{m-3} & a_{m-2} \\ . & . & . & & & . & . \\ . & . & & . & & . & . \\ . & . & & & . & . & . \\ a_2 & a_3 & . & . & . & a_m & a_1 \end{bmatrix}$$

Matrisin birinci satırından diğer satırlar elde edilir. Matrisin 2. satırını elde etmek için 1. satır elemanları bir sağa döndürülür ve 1. satırın sonundaki elemanda 2. satırın başına getirilir. Sonraki satırlar içinde bir önceki satır elemanları bir sağa döndürülür ve önceki satırın son elemanı sonraki satırın başına getirilir.

Tanım 2.2.9 (Nakahara & Abrahao, 2009, s. 109-116). $A \;\; 2^t x 2^t$ Hadamard matris aşağıdaki formda düzenlenebilir.

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

U ve V $2^{t-1}x2^{t-1}$ formunda Hadamard matrislerdir.

Örnek 2.4 $\{a,b,c,d\}$ elemanlarından 4×4 boyutunda bir Hadamard matris aşağıdaki gibi verilebilir.

Tanım 2.2.9'dan U ve V olarak iki elemana ihtiyaç var. U ve V nin tanın gereği örnekte 2×2 matrislerden oluşması gerekmektedir. İşlem ikiye ayrılıyor, öncelikle ilk iki elemandan (a,b) bir Hadamard matris oluşturulmakta, bu sonraki adım için U matrisini oluşturmaktadır. Daha sonra diğer iki elemanı (c,d) kullanarak başka bir Hadamard matris oluşturulmaktadır, bu matris de sonraki adımda V matrisini oluşturmaktadır.

$$U=\begin{bmatrix} a & b \\ b & a \end{bmatrix} \qquad V=\begin{bmatrix} c & d \\ d & c \end{bmatrix}$$

Şimdi bu U ve V elemanlarını $had(U,V)=\begin{bmatrix} U & V \\ V & U \end{bmatrix}$ formatında olacak şekilde birleştirilirse,

$$Had(a,b,c,d)=\begin{bmatrix} U & V \\ V & U \end{bmatrix}=\begin{bmatrix} \begin{bmatrix} a & b \\ b & a \end{bmatrix} & \begin{bmatrix} c & d \\ d & c \end{bmatrix} \\ \begin{bmatrix} c & d \\ d & c \end{bmatrix} & \begin{bmatrix} a & b \\ b & a \end{bmatrix} \end{bmatrix}$$

şeklinde elde edilir. 8 elemandan Hadamard matris oluşturulursa da yapılması gereken elemanları dörderli iki gruba ayırmak, her biri için yukarıda gösterilen işlemleri yapmaktır. Bu işlemlerde U ve V elemanları 4×4 matrislerden oluşmaktadır.

2.3. İzomorfizma

İzomorfizm, iki nesne kümesi veya nesnelerle kavramlar arasında, birebir eşleşmeyi mümkün kılacak biçimde var olan denklik olarak tanımlanabilir.

Örnek 2.5 İki tane grup G_1 ve G_2 aşağıdaki gibi verilsin. Bu gruplar $G_1=\{a,b,c,d,e\}$, $G_2=\{1,2,3,4,5\}$olsun. G_1'e ait $*$ ve G_2'ye ait $\bullet$ işlem tabloları aşağıda verildiği gibi olsun.

$*$	A	B	C	D	E
A	E	A	D	C	B
B	D	B	C	A	E
C	B	C	A	E	D
D	A	D	E	C	B
E	C	E	B	A	D

$\bullet$	1	2	3	4	5
1	5	1	4	3	2
2	4	2	3	1	5
3	2	3	1	5	4
4	1	4	5	3	2
5	3	5	2	1	4

Bu tablolardan, birinci tablodan ikinci tabloya, a,b,c,d,e elemanları yerine sırasıyla $1,2,3,4,5$ haritalaması yapılırsa ve $*$ işlemi yerine de $\bullet$ işlemi yapılırsa, birinci tablodan ikinci tablo elde edilmiş olur. Tersi yapılırsa, ikinci tabloda $1,2,3,4,5$ elemanları yerine sırasıyla a,b,c,d,e haritalaması yapılırsa ve $\bullet$ işlemi yerine $*$ işlemi yazılırsa ikinci tablodan birinci tablo elde edilmiş olur. Başka bir deyişle $E(a)=1, E(b)=2, E(c)=3, E(d)=4, E(e)=5$ ile tanımlanan $E: G_1 \to G_2$ fonksiyonu bire-bir ve örten olup her $\alpha, \beta \in G_1$ için

$$E(\alpha * \beta) = E(\alpha) \bullet E(\beta)$$

özelliğine sahiptir. Örnek $\alpha = a \ ve \ \beta = c$ olsun. Yukarıdaki denklemde yerine konulursa

$$E(\alpha * \beta) = E(a) \bullet E(c)$$

$$E(a * c) = E(a) \bullet E(c)$$

$$E(d) = 1 \bullet 3$$

$$4 = 4$$

denklemin sağlandığını gözlenebilir. Buradan $*$ işlemiyle tanımlanan G_1 ve $\bullet$ işlemiyle tanımlanan G_2 gruplarının aynı özellikler gösterdiği söylenebilir bundan dolayı bu gruplardan birinin özellikleri bilindiği zaman diğeri de bilinebilir (Nesin, 2013).

Tanım 2.3.1 (Nesin, 2013). A ve B iki grup $Q: A \to B$ bir fonksiyon olsun.

1. Q bire-bir ve örtendir.

2. Her $x,y \in A$ için $Q(xy) = Q(x)Q(y)$

Yukarıdaki iki koşul sağlanıyorsa A ve B arasında bir izomorfizma var denir, A ve B

izomorf gruplardır ve $A \cong B$ şeklinde yazılır.

Tanım 2.3.1'deki ikinci özelliğe $Q : A \to B$ fonksiyonunun işlem koruma özelliği denir. Burada gruplar çarpımsal grup gibi düşünülmüştür fakat çarpımsal grup olmasa da yapılacak işlem benzerdir. A'nın ikili işlemi $*$ ve B'nin ikili işlemi $\bullet$ ise $Q : A \to B$ nin işlem koruma özelliği

Her $x,y \in A$ için $Q(x * y) = Q(x) \bullet Q(y)$

olarak ifade edilebilir. Burada haritalama işlemi yaparken A'da tanımlı x'in B'de karşılığını bulmak için $Q(x)$e yani A'daki x'e karşılık gelecek sıradaki elemana, y için B'deki y ye karşılık gelen elemana bakılır. Eleman haritalaması yapıldıktan sonra işlem haritalaması yapılmaktadır. $*$ işlemi yerine bunun B'deki karşılığı olan $\bullet$ işlemi kullanılır.

2.4. Otomorfizma

Nesne kümesinin kendi içerisinde olan izomorfizm, otomorfizma olarak tanımlanabilir.

Tanım 2.4.1 (Nesin, 2013). A bir grup olsun. A'dan A'ya bir izomorfizmaya A'nın bir otomorfizması denir.

Örnek 2.6 A bir değişmeli grup ise, $Q : A \to A$, $Q(x) = x\text{-}1$ ile tanımlanan dönüşüm, A nın bir otomorfizmasıdır. Gerçekten $x,y \in A$ için

$$Q(x) = Q(y) \Rightarrow x\text{-}1 = y\text{-}1 \Rightarrow x = y, Q(y\text{-}1) = y$$

olduğundan, Q bire-bir ve örtendir. Ayrıca,

$$Q(xy) = (xy)-1 = (yx)-1 = (x-1)(y-1) = Q(x)Q(y)$$

olur.

BÖLÜM 3

3. $GF(2^m)$'DE TANIMLI MDS MATRİSLERDEN $GF(2^{mt})$'DE TANIMLI MATRİSLER ÜRETME

Bu bölümde, $GF(2)$'den genişletilmiş $GF(2^m)$ cisminde tanımlı MDS matrislerden, $GF(2^{mt})$ cisminde tanımlı yeni MDS matrisler (uygulama anlamında) üretmemizi sağlayacak farklı fonksiyonların üretimi ile ilgili detaylı bilgi verilmektedir. Bu fonksiyonlar üretilirken, MDS matrislerdeki otomorfizma ve izomorfizma ilişkilerinden faydalanılmaktadır. Bölüm 3.1'de aynı ikili genişletilmiş cisim üzerinde yeni MDS matrisler üretmek için otomorfizm ve bu otomorfizmalara ilişkin farklı fonksiyonların tanımlanması üzerine çalışma yapılmaktadır. Bölüm 3.2'de Bölüm 3.1'de kullanılan fikir genelleştirilerek, aynı dereceyle genişletilmiş cisimlerdeki MDS matrislerde izomorfizmalar tanımlanmaktadır. Bölüm 3.3'de $GF(2^m)$ de tanımlı elemanlardan oluşan MDS matrislerden, $GF(2^{mt})$ $(t \geq 1 \; ve \; m > 1)$de tanımlı elemanlardan oluşan MDS matrisler üretebilmek için gerekli izomorfizmalar ve bu izomorfizmalarla ilişkili farklı fonksiyonlar elde edebilmek için yeni bir yöntem geliştirilmektedir. Ayrıca $GF(q^m)(q = 2$ ve $m > 1)$'de tanımlı elemanlardan oluşan MDS matrislere odaklanılmaktadır. β, $GF(2^m)$'de tanımlı bir cisim oluşturmak için gerekli ilkel eleman olarak belirlensin. O zaman karakteristiği 2 olan bir sonlu cisim elemanı $\alpha_{m-1}\beta_{m-1} + \alpha_{m-2}\beta_{m-2} + ... + \alpha_1\beta + \alpha_0$ $(\alpha_i \in \{0,1\})$ veya bitlerin onaltılık (hexadecimal) formu $(\alpha_{m-1}\alpha_{m-2}...\alpha_1\alpha_0)$ ile ifade edilebilir. Bu tez çalışması boyunca, sonlu cisim elemanlarını ifade etmek için onaltılık notasyon veya ilkel bir elemanın kuvvetleri kullanılmaktadır.

3.1. MDS Matris Otomorfizmaları

Bu bölüm, Bölüm 2.2'deki önerme, tanım ve açıklamalar kullanılarak, genişletilmiş ikili cisimlerde MDS matrislerin otomorfizmalarının ve bu

otomorfizmalarla ilgili farklı fonksiyonların tanımlanması üzerinedir. Genişletilmiş ikili cisimlerde herhangi bir MDS matris üzerinde bu otomorfizmalar ve otomorfizmalarla ilgili fonksiyonlar kullanılarak yeni MDS matrisler üretilebilir. Önerme 3.1.1'de otomorfizmalarının alt determinantlarının 0'dan farklı olma durumunu (nonsingularity) incelenmektedir.

Teorem 3.1.1 (Lidl & Niederreiter, 1986). $GF(q)$ üzerine $GF(q^m)$'in farklı otomorfizmaları $r_0, r_1, ..., r_{m-1}$ haritalamalarıdır. Bu haritalamalar $r_j(\alpha) = \alpha^{q^j}$ ($\alpha \in GF(q^m)$ ve $0 \le j \le m-1$) fonksiyonu ile tanımlanabilir.

Önerme 3.1.1 A, $GF(q^m)$ ($GF(q^m)$ cismi indirgenemez bir $p(x)$ polinomla tanımlı) üzerine tanımlı $n \times n$ boyutunda bir matris olsun. O zaman β ilkel bir eleman olmak üzere $f_i : b \to b^{2^i}$ $(0 \le i \le m-1)$ üs fonksiyonları $GF(q^m)$ üzerinden, $GF(q^m)$ üzerine otomorfizma oluşturur. A matrisinin determinantı 0 ise $GF(q^m)$ in herhangi bir farklı otomorfizmasını uygulayarak elde ettiğimiz bir matrisin determinantı da 0'dır. A matrisinin determinantı 0 dan farklı ise elde ettiğimiz matrisin de determinantı 0 dan farklıdır.

İspat. Teorem 3.1.1'e göre $GF(2)$ üzerine $GF(2^m)$'in farklı otomorfizmaları b^{2^i} ($b \in GF(q^m)$ ve $0 \le i \le m-1$) otomorfik üs fonksiyonlarıyla sağlanabilir. Bu fonksiyonları kullanarak yapılacak haritalamalarda, her bir eleman diğer başka bir elemana haritalanır. Başka bir deyişle $GF(2^m)$ elemanları kendi üzerine haritalanır ve birebir ilişki vardır. A matrisine, $GF(q)$ üzerinde $GF(q^m)$'in herhangi bir farklı otomorfizması uygulayarak elde ettiğimiz bir matrisin (A') determinantı, A matrisinin determinantı ile aşağıdaki gibi ilişkilendirilebilir:

$$\text{Eğer } det(A) = 0 \quad \text{ise} \quad det(A') = 0$$

$$\text{Eğer } det(A) \neq 0 \quad \text{ise} \quad det(A') \neq 0$$

Otomorfizma uygulandıktan sonra Önerme 3.1.1'de değinilen durumlar sağlanacaktır. Ek olarak otormorfizma tanımı gereği, otomorfizma toplama ve çarpma işlemlerinde de

korunur. $GF(q)$ üzerinde $GF(q^m)$'in farklı otomorfizmalarının sayısı m olur. Diğer taraftan bu m tane otomorfizma, $GF(q^m)$'deki sabit elemanlarla çarpılarak ($f_{i,c} : \beta \to (\beta^{2^i}) \cdot c, 0 \le i \le m-1 \quad c \in GF(2^m)^*$), $m \cdot (2^m - 1)$ tane farklı, birebir ve örten üs fonksiyonu elde edilebilir. Bu üs fonksiyonlarını kullanarak yeni MDS matrisler üretilebilir.

Teorem 3.1.2 β, $GF(2^m)$'de herhangi bir ilkel eleman, $c \in GF(2^m)$, $0 \le i \le m-1$ olmak üzere $f_{i,c} : \beta \to (\beta^{2^i}) \cdot c$ formundaki otomorfizmalarla ilişkili olmak üzere $m \cdot (2^m - 1)$ tane farklı, birebir ve örten üs fonksiyonu vardır. Bu fonksiyonlar var olan matrislerden yeni matrisler üretirken, aynı ikili genişletilmiş cisimde kare matrisin MDS matris olma özelliğini de yeni oluşturulan matrise taşımaktadır.

İspat. Burada var olan bir MDS matris elemanlarına farklı otomorfik üs fonksiyonları uygulayarak elde edilen elemanlardan oluşturulan matrisin, MDS matris olma özelliğini koruduğunun gösterilmesi gerekmektedir. $p(x)$, $GF(2)$'de m. dereceden indirgenemez bir polinom ve $\beta \in GF(2^m)$ olsun. $0 \le i \le m-1$ ve $c \in GF(2^m)$ koşullarında $p(\beta) = p(\beta^{2^i}) \cdot c = 0$ olduğu için ($p(\beta^{2^i}) = p(\beta)^{2^i}$) β ve $(\beta^{2^i}) \cdot c$ aynı minimal polinomlara sahiptirler. Otomorfik üs fonksiyonlarını kullanarak elde ettiğimiz elemanlardan oluşan yeni matrisin bütün alt kare determinantlarının tersinin alınabildiğini, matrisin her bir satırının ve sütununun doğrusal olarak bağımsız olduğunu ve MDS matris olma özelliğinin korunduğunu görebiliriz.

Örnek 3.1'de, $GF(2^4)$'de Hadamard formunda, otomorfik ve involutif bir MDS matris gösterilmektedir.

Örnek 3.1 $GF(2^4)/(x^4 + x + 1)$ cisminde $(x^4 + x + 1)$ ilkel bir polinom olduğu için ilkel elemanı α olarak seçilsin. Teorem 3.1.2 gereği 4 farklı otomorfik üs fonksiyonu sırasıyla

$f_{0,1} : \alpha \to \alpha$

$f_{1,1} : \alpha \to \alpha^2$

$f_{2,1} : \alpha \to \alpha^4$

$f_{3,1} : \alpha \to \alpha^8$

şeklindedir. Çizelge 3.1'de $GF(2^4)/(x^4 + x + 1)$cisminde tanımlı MDS matrislerden yeni MDS matrislerin kolaylıkla elde edilebilmesi için $f_{2,1} : \alpha \to \alpha^4$ fonksiyonu (cisim elemanları arasındaki birebir ve örten fonksiyon) onaltılık gösterim ile verilmektedir.

Çizelge 3.1 $GF(2^4)/(x^4+x+1)$ Cisminde Otomorfik Fonksiyon $f_{2,1}:\alpha \to \alpha^4$

$GF(2^4)$ Cisim Elemanları (hexadecimal gösterim)	f_2	$GF(2^4)$ Cisim Elemanları (hexadecimal gösterim)
1_h	$\to$	1_h
2_h	$\to$	3_h
3_h	$\to$	2_h
4_h	$\to$	5_h
5_h	$\to$	4_h
6_h	$\to$	6_h
7_h	$\to$	7_h
8_h	$\to$	F_h
9_h	$\to$	E_h
A_h	$\to$	C_h
B_h	$\to$	D_h
C_h	$\to$	A_h
D_h	$\to$	B_h
E_h	$\to$	9_h
F_h	$\to$	8_h

Örnek 3.2 $p(x)=x^4+x+1$ ile tanımlı $GF(2^4)$ cisminden 4×4 Hadamard involutif bir MDS matris aşağıdaki gibi olsun:

$$A=\begin{bmatrix} 1 & x & x^2 & x^5 \\ x & 1 & x^5 & x^2 \\ x^2 & x^5 & 1 & x \\ x^5 & x^2 & x & 1 \end{bmatrix}=\begin{bmatrix} 1_h & 2_h & 4_h & 6_h \\ 2_h & 1_h & 6_h & 4_h \\ 4_h & 6_h & 1_h & 2_h \\ 6_h & 4_h & 2_h & 1_h \end{bmatrix}.$$

A Hadamard matrisi elemanlarına $f_{2,1}:\alpha\to\alpha^4$ otomorfik üs fonksiyonu uygulayarak oluşturduğumuz yeni elemanları sırasıyla kullanarak elde ettiğimiz matris A' matrisidir ve aşağıda gösterilmektedir.

$$A'=\begin{bmatrix} 1 & x^4 & x^8 & x^5 \\ x^4 & 1 & x^5 & x^8 \\ x^8 & x^5 & 1 & x^4 \\ x^5 & x^8 & x^4 & 1 \end{bmatrix}=\begin{bmatrix} 1_h & 3_h & 5_h & 6_h \\ 3_h & 1_h & 6_h & 5_h \\ 5_h & 6_h & 1_h & 3_h \\ 6_h & 5_h & 3_h & 1_h \end{bmatrix}.$$

A' matrisine, A matrisinin $f_{2,1}:\alpha\to\alpha^4$ üs fonksiyonu altında bir otomorfizması denir ve Teorem 3.1.2 gereği MDS matris olma özelliğini koruduğu görülür.

Not: Yine Teorem 3.1.2 gereği A matrisinden kendisi hariç 59 yeni MDS matris oluşturabiliriz $(m\cdot(2^m-1)-1=4\cdot(2^4-1)-1=59)$.

3.2. MDS Matris İzomorfizmaları

Bu bölüm, Bölüm 2.2'deki önerme, tanım ve açıklamalar kullanılarak, genişletilmiş ikili cisimlerde MDS matrislerin izomorfizmalarının ve bu izomorfizmalarla ilgili farklı fonksiyonların tanımlanması üzerinedir. İkili cisimlerde herhangi bir MDS matris üzerinde bu izomorfizmaları ve bu izomorfizmalarla ilgili farklı fonksiyonları kullanarak $GF(2^m)$ üzerine tanımlı MDS matrislerden $GF(2^{mt})$ $(m>1 ve t\geq1)$ üzerine tanımlı yeni MDS matrisler üretebilmek için yeni bir yöntem geliştirilmektedir. Geliştirilen yöntem aynı derecede genişletilmiş fakat farklı indirgenemez polinomlarla tanımlı cisimler arasında elemanların yer değiştirmesine dayanır.

Önerme 3.2.1 $GF(2^m)/p_1(x)$ ve $GF(2^m)/p_2(x)$ iki cisim olsun**.** Bu cisimlere ait ilkel elemanlar sırasıyla β_1 ve β_2 olsun. A matrisi $GF(2^m)/p_1(x)$ cisminde tanımlı $k \times k$ boyutunda bir matris olsun. A matrisinden $f_{s_u} : \beta_1 \to \beta_2^{s_u}$ (β_2 $GF(2^m)/p_2(x)$ cisminde ilkel bir eleman ve $0 \le s_u \le m-1$) izomorfik üs fonksiyonları kullanarak yeni A' ($GF(2^m)/p_2(x)$ cisminde tanımlı) matrisleri üretilebilir. A matrisinin alt kare matrislerinin determinantlarının 0 veya 0 olmama durumu A' matrisinde de aynen korunmaktadır.

İspat. Önerme 3.2.1'de değinildiği üzere, MDS matrisin elemanlarına herhangi bir izomorfik üs fonksiyonları uygulayarak elde ettiğimiz bütün elemanlar önceki elemanlar gibi sıfırdan farklıdır. s_u üs değerlerini kullanarak elde edeceğimiz f_{s_u} haritalamalarında $GF(2)$'deki her bir eleman diğer bir elemana haritalanır.

Teorem 3.2.1 $GF(2^m)/p_1(x)$ ve $GF(2^m)/p_2(x)$ iki cisim olmak üzere, bu cisimlere ait ilkel elemanlar sırasıyla β_1 ve β_2 olsun. $GF(2^m)/p_2(x)$ üzerine $GF(2^m)/p_1(x)$ üzerinden $f_{s_u} : \beta_1 \to \beta_2^{s_u}$ $(0 \le s_u \le m-1)$ formunda m tane izomorfizma vardır. Bu izomorfizmalara ilave olarak her bir izomorfizma, üzerine geçiş yaptığımız sonlu cismin 0 dan farklı sabit elemanlarıyla çarpılarak $m \cdot (2^m - 1)$ ($s_u = e \cdot 2^i$, $1 \le e \le 2^m - 2$, $gcd(e, 2^m - 1) = 1$, $0 \le u$, $i \le m-1$) tane fonksiyon bulunur ve bu fonksiyonlar yardımıyla $GF(2^m)/p_1(x)$ cismindeki elemanlara, $GF(2^m)/p_2(x)$ cisminde karşılık gelen elemanlar bulunur ve bu elemanlar aynı sırayla kullanılarak $GF(2^m)/p_1(x)$ cismindeki elemanlardan oluşturulan bir MDS matristen $GF(2^m)/p_2(x)$ cismindeki elemanlardan oluşan yeni bir matris elde edilmiş olur. Yeni oluşan matris, MDS matris olma özelliğini muhafaza eder.

İspat. β, $GF(2^m)$' de ilkel bir eleman olsun. $\beta, \beta^2, \beta^3, \ldots, \beta^{2^{m-1}}$ minimal polinom seti m en küçük pozitif tamsayı değerini aldığı zaman, $\beta^{2^m} = \beta$ eşitliği sağlanmaktadır.

$0 \le i \le m-1$ ve $c \in GF(2^m)$ olmak koşuluyla $p(\beta)=0=p(\beta^{2^i})\cdot c$ $(p(\beta^{2^i})=p(\beta)^{2^i})$ eşitliği sağladığı için β ve $(\beta^{2^i})\cdot c$, aynı minimal polinomlara sahiptirler. Her bir s_u üs değerinin $gcd(s_u, 2^{m-1})=1$ denklemini sağlayan s_u değerlerinin içinde bulunduğu siklotomik kosetlerden birinin üyesi olduğu görülür.

Algoritma 3.2.1, Teorem 3.2.1'deki izomorfizmaları tanımlamak için gerekli s_u değerlerinin nasıl hesaplanacağını göstermekte ve sadece ilkel polinomu girdi olarak almaktadır. Algoritma 3.2.1'in ana fikri bütün elemanları ilkel elemanların kuvveti olarak gösterebilmektir. Bu şekilde gösterilmesi, aynı ikili genişletilmiş cisimler arasında izomorfizma kurulmasına yardımcı olmaktadır. Algoritmada, verilen ilkel elemanın kuvvetlerinin, üzerine geçiş yapılan cismin indirgenemez polinomunun $(p_1(x))$ bir kökü olup olmadığı kontrol edilir. Yapılan işlemler sonlu cisimlerde ikili tabanda yapılan işlemlerdir ve indirgeme işlemi (mod işlemi), üzerinden geçiş yapılan cismin indirgenemez polinomu olan $p_2(x)$ üzerinden yapılır.

Algoritma 3.2.1: Önerme 3.2.1'deki izomorfizmaları tanımlamak için gerekli s_u değerlerini hesaplama

---

Input: $p_1(\beta_1), \beta_2$ ve $p_2(x)$

Output: $s_u = e \cdot 2^i, gcd(e, 2^m - 1) = 1, \ (0 \le u, \ i \le m-1)$

1: for $s_u = 1$ to $2^m - 2$ **do**

2: $y_1 \leftarrow p_1(\beta_2^{su}) \ (mod \ p_2(x))$

3: if $y_1 = 0$ **then**

4: Return (s_u)

5: **end if**

6: **end for**

Örnek 3.3 $GF(2^4)$, $p_1(x) = x^4 + x^3 + x^2 + x + 1$ indirgenemez polinomu ile tanımlı olsun. α, $p_1(x)$'in bir kökü ve β_1 $(\beta_1 = \alpha + 1)$, $GF(2^4)/p_1(x)$ de ilkel bir eleman olsun. $GF(2^4)/p_1(x)$'de tanımlı 4×4 involutif bir Hadamard MDS matris aşağıdaki gibidir:

$$M_2 = \begin{bmatrix} 1_h & 2_h & 4_h & 6_h \\ 2_h & 1_h & 6_h & 4_h \\ 4_h & 6_h & 1_h & 2_h \\ 6_h & 4_h & 2_h & 1_h \end{bmatrix} = \begin{bmatrix} 1 & \beta_1^{12} & \beta_1^{9} & \beta_1^{13} \\ \beta_1^{12} & 1 & \beta_1^{13} & \beta_1^{9} \\ \beta_1^{9} & \beta_1^{13} & 1 & \beta_1^{12} \\ \beta_1^{13} & \beta_1^{9} & \beta_1^{12} & 1 \end{bmatrix}.$$

$p_1(\alpha)=\alpha^4+\alpha^3+\alpha^2+\alpha+1$ polinomu, β_1 ilkel elamanı kullanılarak $p_1(\beta_1)=\beta_1^4+\beta_1^3+1$ şeklinde yazılabilir. $GF(2^4)/p_2(x)$ $(p_2(x)=x^4+x+1)$ ikinci sonlu cisim ve $p_2(x)=x^4+x+1$'in ilkel elemanı β_2 $(\beta_2=\alpha)$olsun. $GF(2^4)/p_1(x)$ üzerinden $GF(2^4)/p_2(x)$ üzerine, algoritma 3.2.1'i kullanarak 4 farklı izomorfizma elde edilebilir. Algoritmayı kullanarak elde edeceğimiz s_u değerleri şunlardır: $s_0=7,\ s_1=11,\ s_2=13,\ s_3=14.$ Bu s_u değerlerini yerine yazarak elde edilecek izomorfizmalar: $f_{7,1}:\beta_1\to\alpha^7$, $f_{11,1}:\beta_1\to\alpha^{11}$, $f_{13,1}:\beta_1\to\alpha^{13}$, $f_{14,1}:\beta_1\to\alpha^{14}$, olur. Örnek olarak $f_{7,1}:\beta_1\to\alpha^7$, izomorfizmasını kullanarak, $GF(2^4)/p_1(x)$'deki 4×4 involutif bir M_2 matrisinden, $GF(2^4)/p_2(x)$ üzerine 4×4 involutif bir M_2' matrisi aşağıdaki gibi elde edilebilir.

$$M_2=had(1_h,2_h,4_h,6_h)=had(1,\beta_1^{12},\beta_1^{9},\beta_1^{13})$$

$$M_2=\begin{bmatrix}1&\beta_1^{12}&\beta_1^{9}&\beta_1^{13}\\ \beta_1^{12}&1&\beta_1^{13}&\beta_1^{9}\\ \beta_1^{9}&\beta_1^{13}&1&\beta_1^{12}\\ \beta_1^{13}&\beta_1^{9}&\beta_1^{12}&1\end{bmatrix}=\begin{bmatrix}1_h&2_h&4_h&6_h\\ 2_h&1_h&6_h&4_h\\ 4_h&6_h&1_h&2_h\\ 6_h&4_h&2_h&1_h\end{bmatrix}.$$

$$M_2'=had(1_h,C_h,F_h,3_h)=had(1,\alpha^6,\alpha^{12},\alpha^4)$$

$$M_2'=\begin{bmatrix}1&\alpha^6&\alpha^{12}&\alpha^4\\ \alpha^6&1&\alpha^4&\alpha^{12}\\ \alpha^{12}&\alpha^4&1&\alpha^6\\ \alpha^4&\alpha^{12}&\alpha^6&1\end{bmatrix}=\begin{bmatrix}1_h&C_h&F_h&3_h\\ C_h&1_h&3_h&F_h\\ F_h&3_h&1_h&C_h\\ 3_h&F_h&C_h&1_h\end{bmatrix}.$$

M_2' matrisine M_2 matrisinin $f_{7,1}:\alpha+1\to\alpha^7$ haritalama fonksiyonu altında bir izomorfizması denir ve Teorem 3.2.1 gereği MDS matris olma özelliğini koruduğu görülür.

Not: Yine Teorem 3.2.1 gereği $GF(2^4)/p_1(x)$'den $GF(2^4)/p_2(x)$'e, M_2 matrisinden kendisi hariç 59 ($m\cdot(2^m-1)-1=4\cdot(2^4-1)-1=59$) yeni MDS matris oluşturulabilir. Örnek 3.3'deki s_u üs değerlerinin $C_1=\{1,2,4,8\}$ ve $C_7=\{7,11,13,14\}$ siklotomik kosetlerinden birinin üyesi olduğu görülür. Bunun için Algoritma 3.2.1'de s_u değerlerini bulmak için işlem yapılırken, sadece bu iki tane siklotomik kosetin liderlerinin ($s_u=1$ ve $s_u=7$) işleme tabi tutulması yeterli olacaktır.

3.3. MDS Matris İzomorfizmalarının Genelleştirilmesi için Yöntem

Bu bölümde $GF(2^m)$ sonlu cisminde tanımlı bir MDS matristen, $GF(2^{mt})$ $(t\geq 1 \text{ ve } m>1)$'de tanımlı MDS matrislerin elde edilmesini sağlayacak bir yöntem sunulmaktadır (Diğer bir deyişle bu cisimler arası izomorfizmalar elde edilmektedir). Böylelikle $GF(2^m)$'de tanımlı sonlu cismin bütün elemanlarının $GF(2^{mt})$'de karşılıkları bulunmuş olmaktadır. Önerme 3.2.1, Teorem 3.2.1 ve Algoritma 3.2.1'de anlatılan yöntem biraz daha geliştirilerek, izomorfizmalar ve izomorfizmalarla ilgili farklı fonksiyonların elde edilmesine yönelik genelleştirilmiş bir yöntem elde edilmektedir. Bu yöntemin kullanılması için oluşturulan sözde kod aşağıdaki gibi verilebilir:

Adım 1. m. dereceden $p_1(x)$ ilkel polinomunu seç. Sonlu cisimler $GF(2^m)/p_1(x)$, $GF(2^{mt})/p_2(x)$ için sırasıyla ilkel elemanlar β_1 ve β_2 yi seç.

Adım 2. Algoritma 3.3.1 i kullanarak s_u değerlerini hesapla ve bu değerleri de kullanarak m tane izomorfizma üret.

Adım 3. Adım 2'de üretilen izomorfizmaları, $GF(2^{mt})$ cismindeki 0 hariç bütün sabit elemanlarla ($c\in GF(2^{mt})$) çarparak $m\cdot(2^{mt}-1)$ tane, bu izomorfizmalarla ilgili farklı fonksiyonları hesapla.

Açıklama 3.3.1 Adım 1'deki $p_1(x)$ polinomu ilkel değil sadece indirgenemez polinom ise, ilkel eleman β_1 kullanılarak ifade edilecek şekilde ($p_1(\beta_1)$) bir ilkel polinomu seçilip, seçilen eleman Algoritma 3.3.1'de girdi olarak kullanılacaktır.

Algoritma 3.3.1: $GF(2^{mt})$'deki MDS matrislerle $GF(2^m)$'deki MDS matrisler arasındaki izomorfizmaları tanımlamak için gerekli s_u değerlerini hesaplama

---

Input: $p_1(\beta_1), \beta_2$ ve $p_2(x)$

Output: s_u ($0 \le u \le m-1$)

1: for $s_u = 1$ to $2^{mt} - 2$ **do**

2: $y_1 \leftarrow p_1(\beta_2^{su})$ $(mod\ p_2(x))$

3: if $y_1 = 0$ **then**

4: Return (s_u)

5: **end if**

6: **end for**

Açıklama 3.3.2 Genel yöntemle elde edilen s_u üs değerleri $gcd(s_u, 2^{mt}-1) = \frac{2^{mt}-1}{2^m-1} = (2^m)^{t-1} + (2^m)^{t-2} + ... + 1$ $(t \ge 1)$ olacak şekilde 2'nin mod $2^{mt}-1$ ile elde edilen siklotomik kosetlerinden birinin üyesidir. $2^m - 1$ tane $GF(2^m)$ elemanı, $2^m - 1$ tane $GF(2^{mt})$ elemanına haritalanır böylelikle izomorfizmanın gereği olan birebir ve örten yapı sağlanmış olur.

Örnek 3.4 $GF(2^4)$, $p_1(x) = x^4 + x + 1$ ilkel polinomu ile tanımlı olsun. α $p_1(x)$'in bir kökü ve β_1 $(\beta_1 = \alpha + 1)$ $GF(2^4)/p_1(x)$'de ilkel bir eleman olsun. $GF(2^4)/p_1(x)$'de tanımlı 4×4 involutif bir MDS matris aşağıdaki gibidir:

$$M_3 = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^4 \\ 1 & 1 & \alpha^3 & \alpha^2 \\ 1 & \alpha^2 & 1 & \alpha \\ \alpha & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1_h & 2_h & 4_h & 3_h \\ 1_h & 1_h & 8_h & 4_h \\ 1_h & 4_h & 1_h & 2_h \\ 2_h & 1_h & 1_h & 1_h \end{bmatrix}.$$

$GF(2^8)$, $p_2(x) = x^8 + x^4 + x^3 + x + 1$ ilkel polinomu ile tanımlı olsun. α , $p_2(x)$'in bir kökü ve β_2 $(\beta_2 = \alpha + 1)$ $GF(2^8)/\ p_2(x)$ de ilkel bir eleman olsun.

$GF(2^4)/\ p_1(x)$'den $GF(2^8)/\ p_2(x)$'e, Algoritma 3.3.1 i kullanarak elde edilecek s_u değerlerinden faydalanarak 4 farklı izomorfizma elde edilebilir. Algoritmayı kullanarak elde edilecek s_u değerleri şunlardır: $s_0 = 17$, $s_1 = 34$, $s_2 = 68$, $s3 = 136$. Bu s_u değerlerini yerine yazarak elde edilecek izomorfizmalar: $f_{17,1} : \alpha \to \beta_2^{17}$, $f_{34,1} : \alpha \to \beta_2^{34}$, $f_{68,1} : \alpha \to \beta_2^{68}$, $f_{136,1} : \alpha \to \beta_2^{136}$ dır. Örnek olarak $f_{17,1} : \alpha \to \beta_2^{17}$ izomorfizmasını kullanarak, $GF(2^4)/\ p_1(x)$'den $GF(2^8)/\ p_2(x)$'e, 4×4 bir MDS matris M_3' elde edilsin.

$$M_3' = \begin{bmatrix} 1 & \beta_2^{17} & \beta_2^{34} & \beta_2^{68} \\ 1 & 1 & \beta_2^{51} & \beta_2^{34} \\ 1 & \beta_2^{34} & 1 & \beta_2^{17} \\ \beta_2^{17} & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 01_h & E1_h & 5C_h & E0_h \\ 01_h & 01_h & 0C_h & 5C_h \\ 01_h & 5C_h & 01_h & E1_h \\ E1_h & 01_h & 01_h & 01_h \end{bmatrix}.$$

M_3' ne M_3 ün $f_{17,1} : \alpha \to \beta_2^{17}$ üs fonksiyonu altında bir izomorfizması denir ve Teorem 3.2.1 gereği MDS matris olma özelliğini koruduğu görülür.

Not: Yine Teorem 3.2.1 gereği $GF(2^4)/\ p_1(x)$'den $GF(2^8)/\ p_2(x)$'e, M_3 matrisinden kendisi hariç 1019 yeni MDS matris oluşturabiliriz $(m \cdot (2^m - 1) - 1 = 8 \cdot (2^8 - 1) - 1 = 1019)$.

Açıklama 3.3.3 Açıklama 3.3.2'de değinildiği üzere, Örnek 3.4'deki her bir s_u üs değeri $gcd(s_u, 2^{mt}-1) = gcd(s_u, 2^{4\cdot 2}-1) = \frac{2^{mt}-1}{2^m-1} = \frac{2^{4\cdot 2}-1}{2^4-1} = 17$ eşitliğini sağlamak zorundadır. Bu eşitliği sağlayacak s_u üs değerlerinin $C_{119} = \{119, 187, 221, 238\}$ ve $C_{17} = \{17, 34, 68, 136\}$ siklotomik kosetlerinden birinin üyesi olduğu görülür. Bunun için Algoritma 3.3.1 de s_u değerlerini bulmak için işlem yapılırken, sadece bu iki tane siklotomik kosetin liderlerinin ($s_u = 17$ ve $s_u = 119$) işleme tabi tutulması yeterli olacaktır.

Algoritma 3.3.1 kullanılarak elde edilen s_u değerlerini kullanarak yapılan haritalamalarla var olan MDS matrislerden yeni MDS matrisler üretilmesine diğer bir örnek (8×8 bir MDS matris için) Örnek 3.5'de verilmektedir.

Örnek 3.5 $p_1(x) = x^4 + x + 1$ ilkel polinomu ile tanımlı $GF(2^4)$ cisminden 8×8 bir Hadamard MDS matris aşağıdaki gibi olsun:

$$M_5 = \begin{bmatrix} \alpha & \alpha^{12} & \alpha^6 & \alpha^8 & \alpha^9 & \alpha^2 & \alpha^3 & \alpha^4 \\ \alpha^{12} & \alpha & \alpha^8 & \alpha^6 & \alpha^2 & \alpha^9 & \alpha^4 & \alpha^3 \\ \alpha^6 & \alpha^8 & \alpha & \alpha^{12} & \alpha^3 & \alpha^4 & \alpha^9 & \alpha^2 \\ \alpha^8 & \alpha^6 & \alpha^{12} & \alpha & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^9 \\ \alpha^9 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha & \alpha^{12} & \alpha^6 & \alpha^8 \\ \alpha^2 & \alpha^9 & \alpha^4 & \alpha^3 & \alpha^{12} & \alpha & \alpha^8 & \alpha^6 \\ \alpha^3 & \alpha^4 & \alpha^9 & \alpha^2 & \alpha^6 & \alpha^8 & \alpha & \alpha^{12} \\ \alpha^4 & \alpha^3 & \alpha^2 & \alpha^9 & \alpha^8 & \alpha^6 & \alpha^{12} & \alpha \end{bmatrix} = \begin{bmatrix} 2_h & F_h & C_h & 5_h & A_h & 4_h & 8_h & 3_h \\ F_h & 2_h & 5_h & C_h & 4_h & A_h & 3_h & 8_h \\ C_h & 5_h & 2_h & F_h & 8_h & 3_h & A_h & 4_h \\ 5_h & C_h & F_h & 2_h & 3_h & 8_h & 4_h & A_h \\ A_h & 4_h & 8_h & 3_h & 2_h & F_h & C_h & 5_h \\ 4_h & A_h & 3_h & 8_h & F_h & 2_h & 5_h & C_h \\ 8_h & 3_h & A_h & 4_h & C_h & 5_h & 2_h & F_h \\ 3_h & 8_h & 4_h & A_h & 5_h & C_h & F_h & 2_h \end{bmatrix}$$

Verilen MDS matrise karşılık ilkel polinom $p_2(x) = x^{16} + x^{14} + x^{13} + x^9 + x^5 + x^4 + 1$ ile tanımlı $GF(2^{16})$ cisminden denk bir MDS matris elde edilmek istensin. $GF(2^4)/p_1(x)$ ve $GF(2^8)/p_2(x)$ cisimlerinin ilkel elemanları sırasıyla α ve β olsun.

Aşağıda verilen Magma kodu kullanılarak $f_i : \alpha \to \beta^{s_u}$ $(i \in (1,2,3,4))$ için s_u üs değerleri bulunur.

```
P<z> := PolynomialRing(GF(2));

p := z^16 + z^14 + z^13 + z^9 + z^5 + z^4 + 1;

F<x> := ext <GF(2) | p >;

for c:= 1 to 65535 do

y1:=(x ^ c) ^ 4 + (x ^ c) ^ 1 + 1;

if (y1 eq 0) then PrintFile ("Us.txt",c);

end if;

end for;
```

Magma kodu yardımıyla $f_{s_u,i} : \alpha \to \beta^{s_u}$ haritalamasındaki s_u değerleri 30583, 48059, 56797 ve 61166 olarak elde edilebilir. $p_2(x) = x^{16} + x^{14} + x^{13} + x^9 + x^5 + x^4 + 1$ ile tanımlı $GF(2^{16})$ cisminde $f_1 : \alpha \to \alpha^{30583}$ izomorfik üs fonksiyonu kullanılarak yukarıda verilen MDS matristen aşağıdaki MDS matris (M_5') elde edilebilir.

$$M_5' = \begin{bmatrix} (\alpha^{30583}) & (\alpha^{30583})^{12} & (\alpha^{30583})^6 & (\alpha^{30583})^8 & (\alpha^{30583})^9 & (\alpha^{30583})^2 & (\alpha^{30583})^3 & (\alpha^{30583})^4 \\ (\alpha^{30583})^{12} & (\alpha^{30583}) & (\alpha^{30583})^8 & (\alpha^{30583})^6 & (\alpha^{30583})^2 & (\alpha^{30583})^9 & (\alpha^{30583})^4 & (\alpha^{30583})^3 \\ (\alpha^{30583})^6 & (\alpha^{30583})^8 & (\alpha^{30583}) & (\alpha^{30583})^{12} & (\alpha^{30583})^3 & (\alpha^{30583})^4 & (\alpha^{30583})^9 & (\alpha^{30583})^2 \\ (\alpha^{30583})^8 & (\alpha^{30583})^6 & (\alpha^{30583})^{12} & (\alpha^{30583}) & (\alpha^{30583})^4 & (\alpha^{30583})^3 & (\alpha^{30583})^2 & (\alpha^{30583})^9 \\ (\alpha^{30583})^9 & (\alpha^{30583})^2 & (\alpha^{30583})^3 & (\alpha^{30583})^4 & (\alpha^{30583}) & (\alpha^{30583})^{12} & (\alpha^{30583})^6 & (\alpha^{30583})^8 \\ (\alpha^{30583})^2 & (\alpha^{30583})^9 & (\alpha^{30583})^4 & (\alpha^{30583})^3 & (\alpha^{30583})^{12} & (\alpha^{30583}) & (\alpha^{30583})^8 & (\alpha^{30583})^6 \\ (\alpha^{30583})^3 & (\alpha^{30583})^4 & (\alpha^{30583})^9 & (\alpha^{30583})^2 & (\alpha^{30583})^6 & (\alpha^{30583})^8 & (\alpha^{30583}) & (\alpha^{30583})^{12} \\ (\alpha^{30583})^4 & (\alpha^{30583})^3 & (\alpha^{30583})^2 & (\alpha^{30583})^9 & (\alpha^{30583})^8 & (\alpha^{30583})^6 & (\alpha^{30583})^{12} & (\alpha^{30583}) \end{bmatrix}$$

$$M_5' = \begin{bmatrix} \alpha^{30583} & \alpha^{39321} & \alpha^{52428} & \alpha^{48059} & \alpha^{13107} & \alpha^{61166} & \alpha^{26214} & \alpha^{56797} \\ \alpha^{39321} & \alpha^{30583} & \alpha^{48059} & \alpha^{52428} & \alpha^{61166} & \alpha^{13107} & \alpha^{56797} & \alpha^{26214} \\ \alpha^{52428} & \alpha^{48059} & \alpha^{30583} & \alpha^{39321} & \alpha^{26214} & \alpha^{56797} & \alpha^{13107} & \alpha^{61166} \\ \alpha^{48059} & \alpha^{52428} & \alpha^{39321} & \alpha^{30583} & \alpha^{56797} & \alpha^{26214} & \alpha^{61166} & \alpha^{13107} \\ \alpha^{13107} & \alpha^{61166} & \alpha^{26214} & \alpha^{56797} & \alpha^{30583} & \alpha^{39321} & \alpha^{52428} & \alpha^{48059} \\ \alpha^{61166} & \alpha^{13107} & \alpha^{56797} & \alpha^{26214} & \alpha^{39321} & \alpha^{30583} & \alpha^{48059} & \alpha^{52428} \\ \alpha^{26214} & \alpha^{56797} & \alpha^{13107} & \alpha^{61166} & \alpha^{52428} & \alpha^{48059} & \alpha^{30583} & \alpha^{39321} \\ \alpha^{56797} & \alpha^{26214} & \alpha^{61166} & \alpha^{13107} & \alpha^{48059} & \alpha^{52428} & \alpha^{39321} & \alpha^{30583} \end{bmatrix}$$

$$M_5' = \begin{bmatrix} 34DA_h & E242_h & D699_h & 4321_h & A163_h & 4320_h & 95B9_h & 34DB_h \\ E242_h & 34DA_h & 4321_h & D699_h & 4320_h & A163_h & 34DB_h & 95B9_h \\ D699_h & 4321_h & 34DA_h & E242_h & 95B9_h & 34DB_h & A163_h & 4320_h \\ 4321_h & D699_h & E242_h & 34DA_h & 34DB_h & 95B9_h & 4320_h & A163_h \\ A163_h & 4320_h & 95B9_h & 34DB_h & 34DA_h & E242_h & D699_h & 4321_h \\ 4320_h & A163_h & 34DB_h & 95B9_h & E242_h & 34DA_h & 4321_h & D699_h \\ 95B9_h & 34DB_h & A163_h & 4320_h & D699_h & 4321_h & 34DA_h & E242_h \\ 34DB_h & 95B9_h & 4320_h & A163_h & 4321_h & D699_h & E242_h & 34DA_h \end{bmatrix}$$

Açıklama 3.2.1 gereği;

$$gcd(s_u, 2^{4.4}-1) = gcd(30583,65535) = gcd(48059,65535) = gcd(56797,65535)$$
$$= gcd(61166,65535) = \frac{2^{16}-1}{2^4-1} = 4369$$

olarak elde edilir. Ayrıca s_u üs değerleri 2'nin mod $(2^{16}-1)$ ile elde edilebilecek siklotomik kosetlerinden $C_{30583} = \{30583, 48059, 56797, 61166\}$ kosetinin üyeleridir. C_{30583} koseti dışında $C_{4369} = \{4369, 8738, 17476, 34952\}$ koseti de karşılaşılabilecek üs değerlerinin üyelerini içermektedir. Çünkü bu koset elemanları da Açıklama 3.2.1'de verilen $gcd(s_u, 2^{mt}-1) = \frac{2^{mt}-1}{2^m-1}$ dolayısıyla $gcd(C_{4369}, 2^{4\cdot4}-1) = \frac{2^{16}-1}{2^4-1} = 4369$ şartını sağlamaktadır.

Açıklama 3.3.3 $GF(2^4)/(x^4+x+1)$cisminde tanımlı MDS matrislerden $GF(2^{16})/(x^{16}+x^{14}+x^{13}+x^9+x^5+x^4+1)$ cisminde tanımlı MDS matrislerin elde edilebilmesi için üretilebilecek toplam üs fonksiyonlarının sayısı (Açıklama 3.2.2 gereği) $N_{\sum f}=m\cdot(2^{mt}-1)=4\cdot(2^{4\cdot4}-1)=4\cdot65535=262140$ 'dır.

Örnek 3.6 $p_1(x)=x^8+x^4+x^3+x^2+1$ ilkel polinomu ile tanımlı $GF(2^8)$cisminden 4×4 bir Hadamard MDS matris aşağıdaki gibi olsun:

$$M_7=\begin{bmatrix} 1 & \alpha^{50} & \alpha^{224} & \alpha^{129} \\ \alpha^{50} & 1 & \alpha^{129} & \alpha^{224} \\ \alpha^{224} & \alpha^{129} & 1 & \alpha^{50} \\ \alpha^{129} & \alpha^{224} & \alpha^{50} & 1 \end{bmatrix}=\begin{bmatrix} 1_h & 5_h & 12_h & 17_h \\ 5_h & 1_h & 17_h & 12_h \\ 12_h & 17_h & 1_h & 5_h \\ 17_h & 12_h & 5_h & 1_h \end{bmatrix}.$$

Verilen MDS matrise karşılık ilkel polinom

$$p_2(x)=x^{32}+x^{31}+x^{29}+x^{27}+x^{25}+x^{23}+x^{22}+x^{20}+x^{17}+x^{16}+x^{12}+x^5+x^4+x^3+1$$

ile tanımlı $GF(2^{32})$ cisminden denk bir MDS matris elde edilmek istensin. $GF(2^8)/p_1(x)$ ve $GF(2^{32})/p_2(x)$ cisimlerinin ilkel elemanları sırasıyla β_1 ve β_2 olsun. β_1 ve β_2 ilkel elemanları, her iki polinom da ilkel olduğu için α olarak seçilsin. Aşağıda verilen Magma kodu kullanılarak $f_i:\alpha\to\alpha^{s_u}$ $(i\in(1,2,3,4,5,6,7,8))$ için s_u üs değerleri bulunur.

```
P<z> := PolynomialRing(GF(2));

p := z^32 + z^31 + z^29 + z^27 + z^25 + z^23 + z^22 + z^20
+ z^17 + z^16 + z^12 + z^5 + z^4 + z^3 + 1;

F<x> := ext <GF(2) | p >;

for c:= 1 to 2^32-1 do

y1:=(x ^ c) ^ 8 + (x ^ c) ^ 4 +(x ^ c) ^ 3 + (x ^ c) ^ 2 +
1;

if (y1 eq 0) then PrintFile ("Us.txt",c);

end if;

end for;
```

Magma kodu yardımıyla $f_{s_u,i} : x \to x^{s_u}$ haritalamasındaki s_u değerleri aşağıdaki gibi elde edilir.

Sıra	s_u Değerleri	Haritalama Fonksiyonu
1	724249387	$f_{1,1} : \alpha \to \alpha^{724249387}$
2	1448498774	$f_{2,1} : \alpha \to \alpha^{1448498774}$
3	1499027801	$f_{3,1} : \alpha \to \alpha^{1499027801}$
4	1701143909	$f_{4,1} : \alpha \to \alpha^{1701143909}$
5	2509608341	$f_{5,1} : \alpha \to \alpha^{2509608341}$
6	2896997548	$f_{6,1} : \alpha \to \alpha^{2896997548}$
7	2998055602	$f_{7,1} : \alpha \to \alpha^{2998055602}$
8	3402287818	$f_{8,1} : \alpha \to \alpha^{3402287818}$

$$p_2(x) = x^{32} + x^{31} + x^{29} + x^{27} + x^{25} + x^{23} + x^{22} + x^{20} + x^{17} + x^{16} + x^{12} + x^5 + x^4 + x^3 + 1$$

ilkel polinomu ile tanımlı $GF(2^{16})$cisminde $f_{1,1}:\alpha \to \alpha^{724249387}$ izomorfik üs fonksiyonu kullanılarak yukarıda verilen M_7 MDS matrisinden aşağıdaki MDS matris (M_7') elde edilir:

$$M_7' = \begin{bmatrix} (1)^{724249387} & (\alpha^{50})^{724249387} & (\alpha^{224})^{724249387} & (\alpha^{129})^{724249387} \\ (\alpha^{50})^{724249387} & (1)^{724249387} & (\alpha^{129})^{724249387} & (\alpha^{224})^{724249387} \\ (\alpha^{224})^{724249387} & (\alpha^{129})^{724249387} & (1)^{724249387} & (\alpha^{50})^{724249387} \\ (\alpha^{129})^{724249387} & (\alpha^{224})^{724249387} & (\alpha^{50})^{724249387} & (1)^{724249387} \end{bmatrix}$$

$$M_7' = \begin{bmatrix} 1 & \alpha^{1852730990} & \alpha^{3318072773} & \alpha^{3233857728} \\ \alpha^{1852730990} & 1 & \alpha^{3233857728} & \alpha^{3318072773} \\ \alpha^{3318072773} & \alpha^{3233857728} & 1 & \alpha^{1852730990} \\ \alpha^{3233857728} & \alpha^{3318072773} & \alpha^{1852730990} & 1 \end{bmatrix}$$

$$M_7' = \begin{bmatrix} 00000001_h & 4556972D_h & 2C77FEFE_h & 692169D3_h \\ 4556972D_h & 00000001_h & 692169D3_h & 2C77FEFE_h \\ 2C77FEFE_h & 692169D3_h & 00000001_h & 4556972D_h \\ 692169D3_h & 2C77FEFE_h & 4556972D_h & 00000001_h \end{bmatrix}$$

Açıklama 3.2.1 gereği;

$$gcd(s_u, 2^{8\cdot 4}-1) = gcd(724249387, 2^{32}-1) = gcd(1448498774, 2^{32}-1) = gcd(1499027801, 2^{32}-1)$$
$$= gcd(1701143909, 2^{32}-1) = gcd(2509608341, 2^{32}-1) = gcd(2896997548, 2^{32}-1)$$
$$= gcd(2998055602, 2^{32}-1) = gcd(3402287818, 2^{32}-1) = \frac{2^{32}-1}{2^8-1} = 16843009$$

olarak elde edilir. Ayrıca s_u üs değerleri 2'nin mod $(2^{32}-1)$ ile elde edilebilecek siklotomik kosetlerinden

$$C_{724249387} = \{724249387,\ 1448498774,\ 1499027801,\ 1701143909,$$
$$2509608341,\ 2896997548,\ 2998055602,\ 3402287818\}$$

kosetinin üyeleridir. $C_{724249387}$ koseti dışında

$$C_{16843009} = \{16843009,\ 33686018,\ 67372036,\ 134744072,\ 269488144,\ 538976288,\ 1077952576,\ 2155905152\}$$

koseti de karşılaşılabilecek üs değerlerinin üyelerini içermektedir. Çünkü bu koset elemanları da Açıklama 3.2.1'de verilen $gcd(s_u,\ 2^{mt}-1) = \dfrac{2^{mt}-1}{2^m-1}$ dolayısıyla

$gcd(C_{16843009}\ ,2^{8\cdot 4}-1) = \dfrac{2^{32}-1}{2^8-1} = 16843009$ şartını sağlamaktadır.

Açıklama 3.3.4 $GF(2^8)/\ x^8+x^4+x^3+x^2+1$ cisminde tanımlı MDS matrislerden

$$GF(2^{16})/\ x^{32}+x^{31}+x^{29}+x^{27}+x^{25}+x^{23}+x^{22}+x^{20} + x^{17}+x^{16}+x^{12}+x^5+x^4+x^3+1$$

cisminde tanımlı MDS matrislerin elde edilebilmesi için üretilebilecek toplam üs fonksiyonlarının sayısı (Açıklama 3.2.2 gereği)

$N_{\sum f} = m\cdot(2^{mt}-1) = 8\cdot(2^{8\cdot 4}-1) = 8\cdot 4294967295 = 34359738360$'dır.

BÖLÜM 4

4. GELİŞTİRİLEN YÖNTEMİN BAZI ÖNEMLİ ÖZELLİKLERİ ve UYGULAMA AVANTAJLARI

Bu bölümde, geliştirilen yöntemin bazı önemli özellikleri ışığında, şifreleme uygulamalarında getirebileceği yararlara değinilmektedir.

4.1. Geliştirilen Yöntemin Önemli Özellikleri

Bölüm 3'de var olan bir MDS matrisi alarak, o matrisin tanımlı olduğu $GF(2^m)$ cisminden veya $GF(2^{mt})$ cisminde tanımlı yeni MDS matrisler üreten bir yöntem tanıtılmıştır. Bu açıdan değerlendirildiğinde bu yöntem, var olan MDS matrislerden daha iyi kriptografik uygulama özelliklerine sahip MDS matrisler üretebilme imkanı sunacağından, diğer MDS matris tasarlama yöntemlerinin etkinliğini artıracaktır. $GF(2^m)$ ve $GF(2^{mt})$'de tanımlı MDS matrisler arasındaki ilişkilerden yola çıkılarak geliştirilen yöntemin bazı önemli özellikleri aşağıdaki gibi sıralanabilir:

- Bu yöntem, literatürde var olan MDS matrislerden yeni MDS matrisler üretmek için kullanılabilir.
- Bu yöntem günümüzde kullanılan MDS matris tasarım yöntemlerine, uygulama açısından daha iyi MDS matrisler bulabilme imkanı sağlayacağından, bu yöntemleri tamamlayıcı bir işlev görecektir.
- Bu yöntem $GF(2^m)$ de $k \times k$ MDS matrislerin, izomorfik üs fonksiyonlarıyla haritalanıp $GF(2^{mt})$ de $k \times k$ MDS matrislerin elde edilebilmesini sağlar.
- $GF(2^m)$'deki var olan MDS matrislerden izomorfik üs fonksiyonlarının kullanımıyla elde edilecek $GF(2^{mt})$'deki MDS matrisler, yazılım uygulamalarında az sayıda lookup (arama) avantajını kullanırlar ve sadece XOR işlemleri kullanılarak uygulanabilirler. (Bölüm 3.2 ye bakınız).

- Literatürde bilinen MDS matris üretmek için kullanılan birçok yöntem, uygulamada kullanılacak $GF(2^{mt})$'de MDS matrisler üretirken, mt çok büyük olduğu zaman, çok fazla zaman tüketen bazı arama işlemleri gerektirirler. Geliştirilen yöntem mt'nin büyük olduğu durumlarda bile var olan $GF(2^{m})$ deki matrislerden, $GF(2^{mt})$'de matrisler üretme işinde çok iyi sonuçlar verir. (Bu konuda detaylı bir örnek olan, $GF(2^{m})$'de 8×8 involutif bir MDS matristen, $GF(2^{16})$'da 8×8 involutif bir MDS matris üreten Örnek 3.5'e bakınız.)
- A, $k\times(n-k)$ bir matris ve $G=[I \setminus A]$ üreteç matris olsun. C bir $[n,k,d]$ kod olarak düşünülürse, C'nin minimum uzaklığı olan d, Bölüm 3.2'de gösterilen farklı fonksiyonların uygulanması sonucu korunur.

4.2. MDS Matris Üretmek için Geliştirilen Yöntemin Uygulama Özellikleri

Bu bölümde, 8 bitlik platformlardaki yazılım uygulamalarında hızlı ve etkin olarak çalışacak MDS matrislerin üretiminde kullanılan yeni yöntemin iki önemli özelliği anlatılmaktadır. Ayrıca çeşitli şifreleme algoritmalarında kullanılan veya çeşitli tasarım modelleriyle üretilen MDS matrislerin karşılaştırılması yapılmaktadır. Bu matrisler: ANUBIS (Barreto & Rijmen, 2000b), AES (çok bilinen literatürde şifreleme standardı olarak yer bulmuş olan AES şifreleme algoritmasında kullanılan (AES MixColumns dönüşümü olarak isimlendirilen)) ve (Dakhilalian, Mala, Omoomi & Sajadieh, 2012, s. 287-308)'de tasarlanan MDS matrislerdir.

Literatürde şifreleme algoritmalarının doğrusal dönüşümlerinde kullanılan MDS matrislerin çarpım işlemlerinin uygulanması için iki farklı işlem sırasıyla lookup tabloları (table lookups) ve xtime işlemleridir. Tez sırasında $GF(2^{m})$ üzerinde tanımlı matrislerden $GF(2^{mt})$ üzerine tanımlı matrisler üretmek için geliştirilen yöntem az sayıda lookup tablosu işlemi kullanmanın avantajını taşır. Buna ek olarak, geliştirilen yöntem MDS matris tasarlama yöntemlerine verimliliklerini artırma noktasında yardımcı olabilir. Bu yardım, tasarlanan matrislerin, doğrusal dönüşümlerindeki çarpımlarda xtime işlemleri kullanan şifreleme algoritmalarında kullanılması durumunda daha belirgin olacaktır.

Örnek 3.4'de $GF(2^4)$'de tanımlı bir involutif MDS matristen (M_3), $GF(2^8)$ de tanımlı involutif bir MDS matris (M_3') üretilmektedir. M_3' matrisi, $GF(2^4)$'de tanımlı M_3 matrisinden türetildiği için yazılım uygulamalarında az sayıda lookup tablosu kullanarak gerçekleştirilme avantajını beraberinde taşır. M_3' matrisiyle bir çarpım işlemi 12 xor ve 10 lookup tablosu ile uygulanabilir. Bunun uygulaması aşağıdaki gibi verilebilir:

$$y[0] = x[0] \oplus table[x[1] \oplus table[x[2] \oplus table[table[x[3]]]]]$$

$$y[1] = x[0] \oplus x[1] \oplus table[table[table[x[2]] \oplus x[3]]]$$

$$y[2] = x[0] \oplus x[2] \oplus table[table[x[1]] \oplus x[3]]$$

$$y[3] = table[x[0]] \oplus x[1] \oplus x[2] \oplus x[3]$$

Yukarıdaki uygulamada 4 bitlik giriş biti $x[0...3]$, 4 bitlik çıkış biti $y[0...3]$, olarak alınmaktadır. Burada β_2^{17} lookup tablosu kullanılarak, β_2^{17} ile bir çarpma işlemi sadece bir lookup tablo işlemi ile gerçekleştirilmektedir.

Örnek 4.1'de $GF(2^8)$'de tanımlı bir MDS matris (M_4') üretilmektektedir. M_4' matrisiyle bir çarpım işlemi 15 xor ve 4 lookup tablosu ile uygulanabilmektedir. Ayrıca aynı örnekte M_4 dairesel MDS matrisinin tersinden $((M_4)^{-1})$ aynı izomorfik üs fonksiyonu kullanılarak $GF(2^8)$ de $((M_4')^{-1})$ MDS matrisi elde edilmektedir. $((M_4')^{-1})$ ile bir çarpma işlemi aşağıda görüldüğü gibi 12 xor ve 16 lookup tablosu (iki tablo kullanarak) ile uygulanabilmektedir.

$$y[0] = table2[table2[x[0]] \oplus x[2]] \oplus table1[table1[x[3]] \oplus x[1]]$$

$$y[1] = table2[table2[x[1]] \oplus x[3]] \oplus table1[table1[x[0]] \oplus x[2]]$$

$$y[2] = table2[table2[x[2]] \oplus x[0]] \oplus table1[table1[x[1]] \oplus x[3]]$$

$$y[3] = table2[table2[x[3]] \oplus x[1]] \oplus table1[table1[x[2]] \oplus x[0]]$$

Yukarıdaki uygulamada 4 bitlik giriş biti $x[0...3]$, 4 bitlik çıkış biti $y[0...3]$, olarak alınmaktadır. Burada $\beta_2{}^{119}$ ve $(\beta_2{}^{119})^4((\beta_2{}^{119})^4 = \beta_2{}^{221})$ ile bir çarpma işlemi iki farklı lookup tablosu (table1 ve table2) kullanılarak uygulanabilmektedir.

Örnek 4.2'de M_6 matrisinden $GF(2^8)$'de involutif bir MDS matris ($M_6{}'$) üretilmektedir. $M_6{}'$ matrisiyle bir çarpım işlemi 14 xor ve 12 xtimes işlemi ile uygulanabilmektedir. M_6 matrisiyle bir çarpım işlemi 16 xor ve 12 xtimes işlemi ile uygulanabilmektedir.

Çizelge 4.1 $GF(2^8)$'de, 4×4 MDS Matrislerin Karşılaştırılması

MDS Matris	*# XOR*	*#lookup tabloları veya # xtimes*	*#temp*	*involutif*
$M_3{}'$	12	10	-	Evet
$M_4{}'$	15	4	3	Hayır
$(M_4{}')^{-1}$	12	16	-	Hayır
$M_6{}'$	14	12	-	Evet
M_6	16	12	4	Evet
ANUBIS	12	6	4	Evet
AES	15	4	3	Hayır

Çizelge 4.1'de incelenen bazı MDS matrisler için kaynaklar aşağıda verilmektedir.

M_6 (Dakhilalian, Mala, Omoomi & Sajadieh, 2012, s. 287-308).

ANUBIS (Barreto & Rijmen, 2000b).

AES (Daemen & Rijmen, 2002., Junod & Vaudenay, 2004, s. 84-99).

Çizelge 4.1'de geliştirilen yeni yöntemle üretilen $GF(2^8)$'de 4×4 MDS matrislerin uygulama maliyetleriyle literatürde iyi olarak bilinen 4×4 bazı MDS matrislerin, maliyet karşılaştırmaları yapılmaktadır. Bu tablodaki *temp* sütunu geçici değişkenlere ayrılmaktadır.

Örnek 4.1 $GF(2^4)$**,** $p_1(x)=x^4+x+1$ ilkel polinomu ile tanımlı olsun. α $p_1(x)$'in bir kökü ve β_1 $(\beta_1=\alpha+1)$ $GF(2^4)/\,p_1(x)$ de ilkel bir eleman olsun. $GF(2^4)/\,p_1(x)$ 'de tanımlı 4×4 dairesel bir MDS matris aşağıdaki gibidir:

$$M_4=\begin{bmatrix}\alpha & \alpha^4 & 1 & 1\\ 1 & \alpha & \alpha^4 & 1\\ 1 & 1 & \alpha & \alpha^4\\ \alpha^4 & 1 & 1 & \alpha\end{bmatrix}=\begin{bmatrix}2_h & 3_h & 1_h & 1_h\\ 1_h & 2_h & 3_h & 1_h\\ 1_h & 1_h & 2_h & 3_h\\ 3_h & 1_h & 1_h & 2_h\end{bmatrix}.$$

$GF(2^8)/(\,p_2(x)=x^8+x^4+x^3+x+1)$ cisminde, Örnek 3.4'te bulunan izomorfik üs fonksiyonlarından $f_{17,1}:\alpha\rightarrow\beta_2{}^{17}$ kullanarak, M_4 dairesel MDS matrisinden yeni bir MDS matris üretilsin. Üretilecek dairesel MDS matris $(M_4{}')$ aşağıdaki gibi olur.

$$M_4{}'=\begin{bmatrix}\beta_2{}^{17} & \beta_2{}^{68} & 1 & 1\\ 1 & \beta_2{}^{17} & \beta_2{}^{68} & 1\\ 1 & 1 & \beta_2{}^{17} & \beta_2{}^{68}\\ \beta_2{}^{68} & 1 & 1 & \beta_2{}^{17}\end{bmatrix}=\begin{bmatrix}E1_h & E0_h & 01_h & 01_h\\ 01_h & E1_h & E0_h & 01_h\\ 01_h & 01_h & E1_h & E0_h\\ E0_h & 01_h & 01_h & E1_h\end{bmatrix}.$$

M_4 dairesel MDS matrisinin tersi $(M_4{}^{-1})$ elde edilip bu matris $GF(2^8)/(\,p_2(x)=x^8+x^4+x^3+x+1)$ cismine haritalanırsa $(M_4{}')^{-1}$ elde edilir.

$$M_4^{-1} = \begin{bmatrix} \alpha^{11} & \alpha^{7} & \alpha^{13} & \alpha^{14} \\ \alpha^{14} & \alpha^{11} & \alpha^{7} & \alpha^{13} \\ \alpha^{13} & \alpha^{14} & \alpha^{11} & \alpha^{7} \\ \alpha^{7} & \alpha^{13} & \alpha^{14} & \alpha^{11} \end{bmatrix} = \begin{bmatrix} E_h & B_h & D_h & 9_h \\ 9_h & E_h & B_h & D_h \\ D_h & 9_h & E_h & B_h \\ B_h & D_h & 9_h & E_h \end{bmatrix}.$$

$$(M_4')^{-1} = \begin{bmatrix} \beta_2^{187} & \beta_2^{119} & \beta_2^{221} & \beta_2^{238} \\ \beta_2^{238} & \beta_2^{187} & \beta_2^{68} & \beta_2^{221} \\ \beta_2^{221} & \beta_2^{238} & \beta_2^{187} & \beta_2^{68} \\ \beta_2^{68} & \beta_2^{221} & \beta_2^{238} & \beta_2^{187} \end{bmatrix} = \begin{bmatrix} B1_h & EC_h & 51_h & 0D_h \\ 0D_h & B1_h & EC_h & 51_h \\ 51_h & 0D_h & B1_h & EC_h \\ EC_h & 51_h & 0D_h & B1_h \end{bmatrix}.$$

Örnek 4.2 $GF(2^8)$**,** $p_1(x) = x^8 + x^4 + x^3 + x^2 + 1$ ilkel polinomu ile tanımlı olsun. α $p_1(x)$'in bir kökü ve β_1 $(\beta_1 = \alpha + 1)$ $GF(2^4)/\, p_1(x)$'de ilkel bir eleman olsun. $GF(2^8)/\, p_1(x)$'de tanımlı 4×4 involutif Hadamard bir MDS matris aşağıdaki gibidir:

$$M_6 = \begin{bmatrix} 1 & \alpha^{50} & \alpha^{224} & \alpha^{129} \\ \alpha^{50} & 1 & \alpha^{129} & \alpha^{224} \\ \alpha^{224} & \alpha^{129} & 1 & \alpha^{50} \\ \alpha^{129} & \alpha^{224} & \alpha^{50} & 1 \end{bmatrix} = \begin{bmatrix} 01_h & 05_h & 12_h & 17_h \\ 05_h & 01_h & 17_h & 12_h \\ 12_h & 17_h & 01_h & 05_h \\ 17_h & 12_h & 05_h & 01_h \end{bmatrix}.$$

$GF(2^8)$**,** $p_2(x) = x^8 + x^4 + x^3 + x + 1$ ilkel polinomu ile tanımlı olsun. α, $p_2(x)$'in bir kökü ve β_2 $(\beta_2 = \alpha + 1)$ $GF(2^8)/\, p_2(x)$ de ilkel bir eleman olsun.

$GF(2^8)/\, p_1(x)$'den $GF(2^8)/\, p_2(x)$'e, Algoritma 3.3.1 i kullanarak elde edilecek s_u değerlerinden faydalanarak 8 farklı izomorfizma elde edilebilir. Bu s_u değerlerini yerine yazarak elde edilecek izomorfizmalar: $f_{1,1} : \alpha \to \beta_2^{\,1}$, $f_{2,1} : \alpha \to \beta_2^{\,2}$, $f_{4,1} : \alpha \to \beta_2^{\,4}$, $f_{8,1} : \alpha \to \beta_2^{\,8}$, $f_{16,1} : \alpha \to \beta_2^{\,16}$, $f_{32,1} : \alpha \to \beta_2^{\,32}$, $f_{64,1} : \alpha \to \beta_2^{\,64}$, $f_{128,1} : \alpha \to \beta_2^{\,128}$ dır. Örnek olarak $f_{1,1} : \alpha \to \beta_2^{\,1}$ izomorfizmasını kullanarak, $GF(2^8)/\, p_1(x)$'den $GF(2^8)/\, p_2(x)$'e, 4×4 bir MDS matris M_6' elde edilsin.

$$M_6{}' = \begin{bmatrix} 1 & \beta_2{}^{50} & \beta_2{}^{224} & \beta_2{}^{129} \\ \beta_2{}^{50} & 1 & \beta_2{}^{129} & \beta_2{}^{224} \\ \beta_2{}^{224} & \beta_2{}^{129} & 1 & \beta_2{}^{50} \\ \beta_2{}^{129} & \beta_2{}^{224} & \beta_2{}^{50} & 1 \end{bmatrix} = \begin{bmatrix} 01_h & 04_h & 12_h & 16_h \\ 04_h & 01_h & 16_h & 12_h \\ 12_h & 16_h & 01_h & 04_h \\ 16_h & 12_h & 04_h & 01_h \end{bmatrix}.$$

BÖLÜM 5

5. SONUÇ

Bu tez çalışmasında var olan MDS matrislerden yeni MDS matrislerin elde edilmesini sağlayacak yeni bir yöntem için çalışmalar yapılmıştır. Daha özel olarak ise tez çalışması $GF(2^m)$ (ilkel veya indirgenemez bir polinomla tanımlı) sonlu cismi üzerine MDS matrislerden $GF(2^{mt})$ $(t \geq 1 \; ve \; m > 1)$ (ilkel veya indirgenemez bir polinomla tanımlı) üzerine yeni MDS matrislerin elde edilebilmesini sağlayan bir yöntem sunmaktadır. Dolayısıyla yöntem, $GF(2^m)$ cismi üzerine MDS matrislerden $GF(2^{mt})$ $(t \geq 1 \; ve \; m > 1)$ üzerine tanımlı yeni MDS matrislerin elde edilmesini sağlayacak izomorfik fonksiyonlara odaklanmaktadır.

Bu çalışmada var olan MDS matrislerden ilgili cisimlerdeki otomorfik ve izomorfik üs fonksiyonları kullanılarak kendi üzerlerine veya gerekli koşulu sağlayan diğer cisimler üzerine MDS matrisler elde edilmiştir. Sonuç olarak geliştirilmekte olan yöntemin literatürde MDS matrislerin tasarımı için geliştirilmiş olan tüm yöntemler için tamamlayıcı bir yöntem olması planlanmaktadır. Literatürde MDS matrislerden yenilerinin elde edilmesini sağlayan genel bir yöntem bulunmaması tezin önemini daha iyi ortaya çıkarmaktadır. Tez çalışmasının alt cisim (sub-field) Hadamard tasarımı (Sim, Khoo, Oggier & Peyrin, 2015, s. 471-493) ile ilişkilendirilmesi ve hafif siklet 4×4 $GF(2^8)$ üzerine MDS matrislerin üretilmesi için revizyonu ileriki çalışmalarda gerçekleştirilebilir.

KAYNAKLAR

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

Biham, E., Shamir, A. (1990). *Differential Cryptanalysis of DES-like Cryptosystems.* Journal of Cryptology. Vol. 4, s. 3-72.

Akleylek, S., Rijmen, V., Sakallı M. T., Öztürk E. (2017). *Efficient Methods to Generate Cryptographically Significant Binary Diffusion Layers*. IET Information Security, Vol.11, No.4, s.177-187, doi: 10.1049/iet-ifs.2016.0085.

Akleylek, S., Sakallı, M. T., Öztürk E., Mesut A, Tuncay G. (2016). *Generating Binary Diffusion Layers with Maximum/High Branch Numbers and Low Search Complexity.* Security and Communication Networks, Vol.9, No.16, s.3558-3569, doi: 10.1002/sec.1561.

Augot, D., Finiasz M. (2015). *Direct construction of recursive MDS diffusion layers using shortened BCH codes.* FSE, Vol. 8540, s. 3-17.

Aumasson, J. P., Fischer, S., Khazaei, S., Meier, W., Rechberger C. (2007). *New features of Latin dances: analysis of Salsa, ChaCha, and Rumba.* http://eprint.iacr.org/2007/472.

Barreto, P. S. L. M., Filho, G.D., Rijmen, V. (2006). *The Maelstrom-0 Hash Function.* Proceedings of the 6th Brazilian Symposium on Information and Computer Systems.

Barreto, P. S. L. M., Rijmen, V. (2000a). *The ANUBIS legacy-level block cipher*.. First open NESSIE Workshop, Leuven.

Barreto, P. S. L. M., Rijmen, V. (2000b). *The ANUBIS Block Cipher.* Submission to the NESSIE Project. http://cryptonessie.org

Barreto, P. S. L. M., Rijmen, V. (2000c). *The Khazad Legacy-Level Block Cipher*. First Open NESSIE Workshop.

Bosma W., Cannon J., Playoust C. (1997). *The Magma Algebra System I: The User Language.* Journal of Symbolic Computation, s. 235-265.

Bosselaers, A., Daemen, J., Preneel, B., Rijmen, V., Win, E. D. (1996). *The cipher SHARK.* Gollmann, D. (Ed.) FSE. LNCS , Springer, Heidelberg. Vol. 1039, 99–112.

Britannica, *Cryptology*, Adres: https://www.britannica.com/topic/cryptology. Erişim Tarihi: 18.12.2017

Cannière, C. D., Preneel B. (2005). *The Stream Cipher Trivium, eSTREAM*. The ECRYPT Stream Project.

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

Daemen, J., Knudsen, L.R., Rijmen, V. (1997). *The block cipher SQUARE*. Biham, E. (Ed.) FSE. LNCS Springer, Heidelberg, Vol. 1267, s. 149–165.

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

Dakhilalian, M., Mala, H., Omoomi, B. Sajadieh, M. (2012a). *On construction of involutory MDS matrices from Vandermonde Matrices in GF (2q).* Design, Codes Cryptography, s. 1–22.

Dakhilalian, M., Mala, H., Omoomi, B., Sajadieh, M. (2012b). *On construction of involutory MDS matrices from Vandermonde Matrices in GF (2q).* Design, Codes and Cryptography 64(3), s. 287-308.

Ferguson, N., Hall, C., Kelsey, J., Schneier, B., Wagner, D., Whiting, D. (1998). *Twofish: A 128-bit block cipher.* The first AES Candidate Conference. National Institute for Standards and Technology.

Forouzan A. (2008). *Cryptography and Network Security.*.

Furuya, S., Preneel, B., Takaragi, K., Yoshida, H., Watanabe, D. (2002). *A new keystream generator MUGI.* Daemen, J (Ed.)., Rijmen, V. (Ed.) FSE. LNCS, Springer, Heidelberg. Vol. 2365, s. 179–194.

Gauravaram, P., Knudsen, L.R., Matusiewicz, K., Mendel, F., Rechberger, C., Schlaffer, M., Thomsen, S. (2008). *Grφstl a SHA-3 Candidate.* Submission to NIST, http://www.groestl.info.

Guo I., Peyrin T., Poschmann A. (2011). *The PHOTON Family of Lightweight Hash Functions.* In CRYPTO, s. 222–239.

Gupta, K. C., Ray I. G. (2013). *On constructions of MDS matrices from companion matrices for lightweight cryptography.* CD-ARES Work shops:MoCrySEn, s. 29-43.

Hong X., Lin T., Xuejia L. (2014). *On the Recursive Construction of MDS Matrices for Lightweight Cryptography Chapter Information Security Practice and Experience.* The series Lecture Notes in Computer Science. Vol. 8434, s. 552-563.

Junod, P., Vaudenay S. (2004). *Perfect Diffusion Primitives for Block Ciphers-Building Efficient MDS Matrices*. In Proceedings of Selected Areas in Cryptology. Lecture Notes in Computer Science, Springer-Verlag. Vol. 3357, s. 84-99.

Kozaczuk, W. (2004). *Enigma.*

Lidl, R., Niederreiter, H. (1986). *Introduction to Finite Fields and Their Applications*. Cambridge University Press.

MacWilliams F. J.& Sloane, N.J.A. (1998). *The Theory of Error-Correcting Codes*. North-Holland, s. 299-316.

Matsui, M. (1993). *Linear Cryptanalysis Method for DES Cipher, in Advances in Cryptology.* EUROCRYPT 93, s. 386-397.

Mister, S., Tavares, S.E. Youssef, A. M. (1997). *On the Design of Linear Transformations for Substitution Permutation Encryption Networks.* Workshop on Selected Areas in Cryptography, s. 40–48.

Murphy, T. (2001). *Finite Fields.* Course 373: University of Dublin School of Mathematics, Ireland, s. 27-29, s. 55-56.

Nakahara, J., Abrahao, E. (2009). *A New Involutory MDS Matrix for the AES.* International Journal of Network Security, s. 109-116.

Nesin, A. (2013). *Cebir 1, Temel Grup Teorisi.*

NIST, (1999). *Data Encryption Standard*. https://csrc.nist.gov/csrc/media/publications/fips/46/3/archive/1999-10-25/documents/fips46-3.pdf

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

Schneier, B. (1996). *Applied Cryptography - Protocols, Algorithms, and Source code in C.*

Sim, S.M., Khoo, K., Oggier, F., Peyrin, T. (2015). *Lightweight MDS involution matrices.* Fast Software Encryption (FSE), LNCS 9054, s.471-493.

Stallings, W. (2005). *Cryptography and Network Security Principles and Practices.* (4. Baskı), s. 88

Wu, H. (2005). *The Stream Cipher HC-256, eSTREAM.* The ECRYPT Stream Project.

ÖZGEÇMİŞ

Kemal AKKANAT, 07 Ocak 1980 yılında Besni'de doğdu. Lise öğrenimini Bayrampaşa Sabit Büyükbayrak Lisesi'nde tamamladı. 1997 yılında girdiği İstanbul Üniversitesi İşletme Fakültesi İşletme (İng) Bölümü'nden, 2002 yılında mezun oldu. Daha sonra Sakarya Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü'ne 2010 yılında giriş yapıp 2014 yılında mezun oldu. 2015 yılında Trakya Üniversitesi Bilgisayar Mühendisliği Bölümünde Yüksek Lisans çalışmalarına başladı. 2015 yılından beri Trakya Üniversitesi Bilgisayar Mühendisliği Bölümünde Araştırma Görevlisi olarak çalışmaktadır.