

See discussions, stats, and author profiles for this publication at: <https://www.researchgate.net/publication/361824351>

KRIPTOGRAFİK BLOK ŞİFRELERİN MAKİSİMUM UZAKLIKLA AYRILABİLEN YAYILIM TABAKALARININ TASARIMI

Chapter · December 2020

CITATIONS

0

READS

1,913

2 authors:



Meltem Kurt Pehlivanoğlu

Kocaeli University

57 PUBLICATIONS 247 CITATIONS

[SEE PROFILE](#)



Elif Bilge Kavun

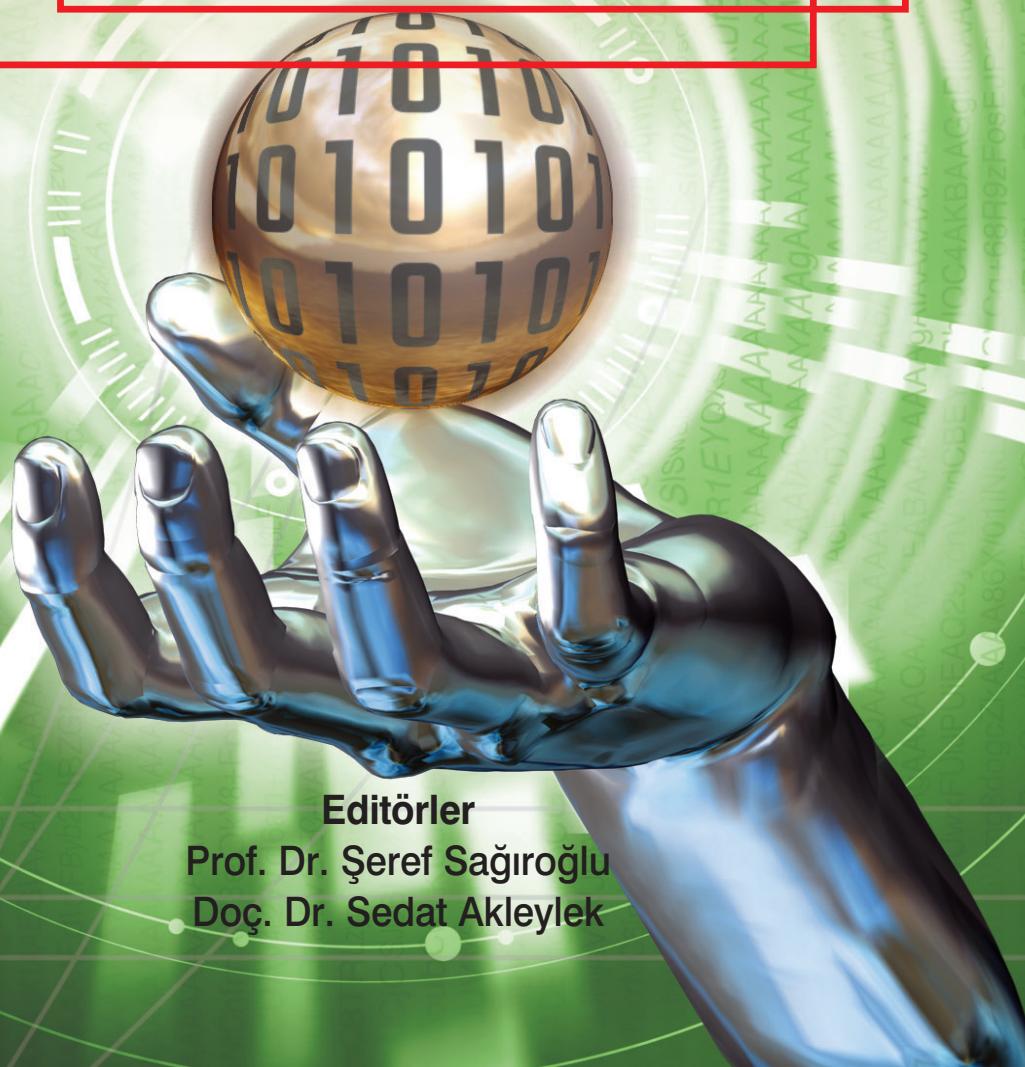
University of Passau

46 PUBLICATIONS 1,220 CITATIONS

[SEE PROFILE](#)

S i b e r Güvenlik ve Savunma

BİYOMETRİK VE KRIPTOGRAFİK UYGULAMALAR



Editörler

Prof. Dr. Şeref Sağıroğlu

Doç. Dr. Sedat Akleylek

SİBER GÜVENLİK VE SAVUNMA

Biyometrik ve Kriptografik Uygulamalar

Editörler: Prof. Dr. Şeref Sağıroğlu - Doç. Dr. Sedat Akleylek

Yayın No. : 3229
İktisat No. : 332
ISBN : 978-625-439-024-1
E-ISBN : 978-625-439-025-8
Basım Sayısı : 1. Basım, Aralık 2020

© Copyright 2020, NOBEL AKADEMİK YAYINCILIK EĞİTİM DANIŞMANLIK TİC. LTD. ŞTİ. SERTİFİKA NO.: 40340
Bu baskının bütün hakları Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic. Ltd. Şti.ne aittir. Bu kitap yayinevinin yazılı izni olmaksızın elektronik olarak dağıtılabilir, paylaşılabılır ve çoğaltılabılır. Bu kitap basılı olarak ya da herhangi bir usûl ile para karşılığı satılmaz.

Kitap içerisindeki bölümlerin akademik, etik ve doğabilecek herhangi hukuki sorumluluklar bölüm yazarlarına aittir.

Nobel Yayın Grubu, 1984 yılından itibaren ulusal ve 2011 yılından itibaren ise uluslararası düzeyde düzenli olarak faaliyet yürütmekte ve yayındığı kitaplar, ulusal ve uluslararası düzeyde yükseköğretim kurumları kataloglarında yer almaktadır.

Genel Yayın Yönetmeni: Nevzat Argun -nargun@nobelyayin.com-
Yayın Koordinatörü : Gülfem Dursun -gulfem@nobelyayin.com-

Redaksiyon : Buse Gamze Çeliktaş -buse@nobelyayin.com-
Sayfa Tasarım : Tarkan Kara -erdal@nobelyayin.com-
Kapak Tasarım : Grafiker
Baskı Sorumlusu : Yavuz Şahin -yavuz@nobelyayin.com-
Baskı ve Cilt : Sarıyıldız Ofset Amb. Kağı. Paz. San. ve Tic. Ltd Sertifika No.: 23593
İvedik Ağaç İşleri San. Sit. 1354. Cad. 1358. Sok. No.: 31 Ostim / ANKARA

Kütüphane Bilgi Kartı

Sağıroğlu, Şeref., Akleylek, Sedat.

Siber Güvenlik ve Savunma Biyometrik ve Kriptografik Uygulamalar / Şeref Sağıroğlu - Sedat Akleylek

1. Basım. XVIII + 508 s. 16x23,5 cm. Kaynakça ve dizin var.

ISBN: 978-625-439-024-1

E-ISBN: 978-625-439-025-8

1. Sis Bilişimi ve Uygulamalarında Veri Güvenliği 2. Saldırı Tespit Sistemleri ve LOG (Günlük) Analizi 3. Açık Kaynak İstihbaratı (Open Source Intelligence OsInt) 4. Biyolojik Biyometrik Sistemler, Biyometrik Veriler, Hukuk ve Güvenlik 5. Davranışsal Biyometrik Sistemler, Teknolojiler ve Güvenlik 6. Biyometride Yeni Nesil Davranış Modelleme Yaklaşımları, Riskler ve Öngörüler 7. Kafes Tabanlı Kriptografide Kullanılan Zor Problemlerin Kriptanalizi ve Yazılım Kütüphaneleri 8. Ağ Anomali Tespitinde Makine Öğrenmesi Algoritmalarının Kullanılması ve Sınıflandırma İçin Bir Uygulama Örneği 9. Kriptografik Blok Şifrelerin Maksimum Uzaklıklık Ayırılabilen Yayılm Tabakalarının Tasarımı 10. Güvenlik Uygulamalarını Hedefleyen Fiziksel Saldırılar ve Bunlara Karşı Alınabilecek Önlemler 11. Küresel Salgının Ulusal Bilişim Güvenliğine Etkileri 12. DevSecOps 13. Endüstriyel Kontrol Sistemlerinin Siber Güvenliği 14. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminde Karşılaşılan Uygulama Zorlukları 15. Siber Tehdit İstihbaratı ve Saldırı Tespit Sistemlerinde Büyük Veri Teknolojileri

Genel Dağıtım

ATLAS AKADEMİK BASIM YAYIN DAĞITIM TİC. LTD. ŞTİ.

Adres: Bahçekapı mh. 2465 sk. Oto Sanayi Sitesi No:7 Bodrum Kat Şaşmaz-ANKARA - siparis@nobelyayin.com-

Telefon: +90 312 278 50 77 - Faks: 0 312 278 21 65

E-Satış: www.nobelkitap.com - esatis@nobelkitap.com / www.atlaskitap.com - info@atlaskitap.com

Dağıtım ve Satış Noktaları: Alfa Basım Dağıtım, Arasta, Arkadaş Kitabevi, D&R Mağazaları, Dost Dağıtım, Ekip Dağıtım, Kida Dağıtım, Kitapsan, Nezih Kitabevleri, Pandora, Prefix, Remzi Kitabevleri

BÖLÜM YAZARLARI

Bölüm 1

Sis Bilişimi ve Uygulamalarında Veri Güvenliği

SEDAT AKLEYLEK - AYKUT KARAKAYA

Bölüm 2

Saldırı Tespit Sistemleri ve LOG (Günlük) Analizi

HİDAYET TAKCI

Bölüm 3

Açık Kaynak İstihbaratı (Open Source Intelligence Osint)

HÜSEYİN AKARSLAN

Bölüm 4

Biyolojik Biyometrik Sistemler, Biyometrik Veriler, Hukuk Ve Güvenlik

PELIN ÖZKAYA - REFİK SAMET

Bölüm 5

Davranışsal Biyometrik Sistemler, Teknolojiler ve Güvenlik

HANDE TUTUMLUER - REFİK SAMET

Bölüm 6

Biyometride Yeni Nesil Davranış Modelleme Yaklaşımları, Riskler ve Öngörüler

BİLGEHAN ARSLAN - ÇAĞLA AKSOY - ŞEREF SAĞIROĞLU

Bölüm 7

Kafes Tabanlı Kriptografide Kullanılan Zor Problemlerin Kriptanalizi ve Yazılım Kütüphaneleri

HAMİ SATILMIŞ - SEDAT AKLEYLEK

Bölüm 8

Ağ Anomali Tespitinde Makine Öğrenmesi Algoritmalarının Kullanılması ve Sınıflandırma İçin Bir Uygulama Örneği

HABİBE GÜLER - ŞEREF SAĞIROĞLU

Bölüm 9

Kriptografik Blok Şifrelerin Maksimum Uzaklıkla Ayrılabilen Yayılım Tabakalarının Tasarımı

MELTEM KURT PEHLİVANOĞLU - ELİF BİLGE KAVUN

Bölüm 10

Güvenlik Uygulamalarını Hedefleyen Fiziksel Saldırılar ve Bunlara Karşı Alınabilecek Önlemler

MELTEM KURT PEHLİVANOĞLU - ELİF BİLGE KAVUN

Bölüm 11

Küresel Salgının Ulusal Bilişim Güvenliğine Etkileri

ENSAR ŞEKER

Bölüm 12

DevSecOps

MURAT KAYA - TUĞCAN TUĞLULAR

Bölüm 13

Endüstriyel Kontrol Sistemlerinin Siber Güvenliği

İSMAİL ERKEK - ERDAL IRMAK

Bölüm 14

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sisteminde Karşılaşılan Uygulama Zorlukları

SAMİME MERAL - HALİL İBRAHİM BÜLBÜL

Bölüm 15

Siber Tehdit İstihbaratı ve Saldırı Tespit Sistemlerinde Büyük Veri Teknolojileri

YAVUZ CANBAY

BİLGİ GÜVENLİĞİ DERNEĞİ'NDEN

Bilgi Güvenliği Derneği (BGD); 22.07.2007 tarihinde, Bilgi Güvenliği ve Siber Güvenlik alanında toplumun her kesiminde bilgi ve bilinç düzeyini artırmak, bu konu ile ilgili teknolojik gelişmeleri izlemek, yerli ve milli teknolojilerin geliştirilmesine katkı sağlamak; bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak ve kamu-sektör-üniversite işbirliklerini geliştirmek amacıyla kurulmuştur.

BGD'nin vizyonu; “bilgi güvenliği alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olmaktır.” BGD amacı doğrultusunda; tüm paydaşlarla işbirliği yaparak mevzuatın oluşturulmasında ve geliştirilmesinde aktif rol almaktır, gerçekleştirdiği konferans, sempozum, çalıştay ve eğitimler, yayılmış olduğu rapor ve yazılar ile farkındalıkın oluşmasına ve bunun davranışa dönüştürülmesine katkılar sağlamaktadır.

Derneğimiz bu kapsamda; “Ulusal Siber Güvenlik Strateji Belgesi” ve “Ulusal Siber Güvenlik Eylem Planı” hazırlanmasına öncülük etmiş, hazırladığı taslak metinler kabul görmüş ve sonučta ülkemizin siber güvenlik stratejisi ve eylem planlarının gecikmeden yayımlanmasına katkı sağlamıştır. Aynı zamanda; bu alanda nitelikli insan kaynağı yetiştirmesi, mesleki yeterliliklerin belirlenmesi, kamu-endüstri-üniversite işbirliklerinin geliştirilmesi, kümelenme çalışmalarının başlaması gibi önemli politika ve stratejilerin oluşturulmasında etkin rol üstlenmektedir.

BGD, “Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı”, “Ulusal Siber Güvenlik Stratejisi Çalıştayı”, “Veri Merkezleri ve Siber Güvenlik Çalıştayı”, “Siber Güvenlik Hukuku Çalıştayı”, “Mobil Dünyada Çocuk ve Gençlerin Güvenliği Sempozyumu”, “IPv6 Konferansı”, “Kritik Enerji Altyapılarının Korunması Sempozyumu”, “Ulusal Siber Terör Konferansı”, “Siber Güvenlik Yaz Kampı” gibi etkinlikleri düzenleyerek ve destekleyerek bilgi güvenliğine ihtiyaç duyulan her alanda çalışmalar yürütmüştür. Cumhurbaşkanlığı, BTK, UAB, MEB, SGK, Üniversiteler gibi farklı paydaşlar ile çalışmalar yürütmektedir.

BGD, CyberMag Dergisi ile toplumun tüm kesimlerine ulaşmaya çalışmaktadır. 2020 yılında 13. sini düzenlediğimiz “Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı” kısaca ISCTurkey Konferansı olarak bilinen uluslararası etkinlik ile kurulduğu günden bu yana kamu kurumları, özel sektör ve üniversiteleri bir araya getirmeyi başarmıştır.

Bununla birlikte, bilgi güvenliği ve siber güvenlik alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olan Bilgi Güvenliği Derneği, bünyesinde oluşturulan BGD Genç ile; bireysel, kurumsal, ulusal ve evrensel boyutlarda bilgi ve iletişim güvenliği alanında teknik, bilimsel, sosyal ve kültürel faaliyetler yürütmek, orta ve yüksek öğrenim gören genç üyelerimizin mesleki gelişimini artırmak, siber güvenlik alanında farkındalık oluşturmak, ülkemizin siber güvenlik uzman kaynağını oluşturmak için gençlerimizin bu alana ilgisini artırmak için faaliyet göstermektedir.

ISCTurkey etkinlikleri, Gazi Üniversitesi, İstanbul Teknik Üniversitesi ve ODTÜ işbirliği ile düzenlenmekte ve Ulaştırma ve Altyapı Bakanlığı, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ile Bilgi Teknolojileri ve İletişim Kurumu tarafından sürekli desteklenmektedir. Bu etkinlik, Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) tarafından “Avrupa Siber Güvenlik Ayı” platformu etkinliklerine dahil edilen ilk ve tek etkinliktir. Ayrıca, düzenlendiği ilk yıldan beri ülkemizin siber güvenlik alanındaki bilimsel ve sektörel çalışmaların paylaşıldığı, üniversite-kamu-endüstri işbirliğinin geliştirildiği, kamunun bilgilendirildiği, paydaşların eğitildiği, tüm bilim insanları, araştırmacılar ve sektörel uygulayıcılar arasında bilgi alışverişini sağlayan ülkemizde bu alanındaki en önemli etkinliktir.

Bu kitabın hazırlanmasında katkı sağlayan başta editörlerimize, hiç bir beklenmedi içerisinde olmadan bölüm yazan ve bunu kamuoyu ile ücretsiz paylaşılması konusunda destek veren saygıdeğer yazarlarımıza, sponsorumuza ve bugüne kadar ülke bilgi güvenliği ve siber güvenliğinin gelişimine katkı sağlayan BGD yöneticilerimize ve üyelerimize bu vesile ile şükranlarımı sunarım.

Bu kitap serisinin, ülkemiz siber güvenlik ve savunma çalışmalarına katkılar sağlama dileğiyile.

Ahmet Hamdi ATALAY
Bilgi Güvenliği Derneği YK Başkanı

EDİTÖRLERDEN

Bilgi Güvenliği Derneği (BGD), kuruluşundan bugüne kadar ülkemizin bilgi ve siber güvenliği ile savunmasının gelişimine katkı sağlamakta, birikimini çevreye aktarmakta, bilgi güvenliği alanında açık kaynak yaklaşımını benimseyen ve bu kapsamda içerik üretilmesine ve geliştirilmesine destek vermektedir, bunları yaymakta, paylaşmakta ve kamuoyunun kullanımına sunmaktadır. Düzenlediği ulusal ve uluslararası etkinliklere ait bildiri kitapları serisi, hazırladığı raporlar, taslak strateji dokümları ve eylem planları vb. bunların başında gelmektedir. Siber Güvenlik ve Savunma Kitapları Serisi ise BGD'nin ülkemizin siber güvenliğine önemli bir katkısıdır.

Tehditlerin, saldırıların veya açıklıkların artması, boyut ve yön değiştirmesi, farklılaşması, siber tehdit ekosisteminin gittikçe güçlenmeye başlaması, kritik altyapıların hedef haline gelmesi, bilgi ve kaynak hırsızlıklarının çoğalması, yeraltı yapılarının etkinleşmesi, siber tehditlerin artık savaşa dönüşmesi, siber suç ve suçlarının çoğalması, siber terörün yaygınlaşması vb. olumsuzlukların hızla artması, yapılacak mücadele, alınacak önlem ve karşı koyulacak yaklaşımlara duyulan ihtiyacı artırmıştır. Kapsamlı bir mücadele için; ulusal strateji ve eylem planlarına, araştırma merkezlerine, gelişmiş altyapı ve araçlara, lisans ve lisansüstü programlara, nitelikli insan kaynağına, yerli ve milli ürünlerin geliştirilmesine, siber güvenlik ve savunma ekosisteminin oluşturulmasına, ulusal siber olaylara müdahale ekiplerinin sayısının ve niteliğinin artırılmasına, savunma sanayinin gelişmesine katkı sağlayacak yeni çalışma ve projelerin hayatı geçirilmesine mevcut sistem, yapı ve organizasyonların kapsamının büyütülmesine, yeni yapıların kurulmasına ihtiyaç vardır. Duyulan bu ihtiyacı bir nebze de olsa karşılamak için bu kitap serisi hazırlanmıştır. Bu kitap serisinde, 100'e yakın konu başlığı irdelenmektedir. Her bölümde, farklı bir konu siber güvenlik ve savunma kapsamında ele alınmakta, değerlendirilmekte ve alınması gereken önlemlere yer verilmektedir.

Bu kitap serisinde sunulan konu başlıklarını, ülkemizde bu alanda çalışan akademisyenler, uzmanlar ve çalışanlar ile paylaşılmış ve bu kitap serisine katkı sağlamaları istenilmiştir. Zamanı uygun olan, katkı vermek isteyen uzman veya akademisyenler belirlenen bir konuda bölüm yazarı olmaları için davet edilmişlerdir. Belirlenen süre içerisinde bölümlerini tamamlayan yazarlarımızın eserleri ise uygun olan ciltlerde basılmaktadır. Bundan sonraki süreçte, belirlenen diğer konular belirli sürelerde tamamlanıp takip eden ciltlerde yayımlanacaktır. Siber güvenlik ve savunmaya çok kapsamlı bir bakış sunmayı amaçlayan ve farklı başlıklarını bir araya toplayan bu kapsamlı eserin, ülke siber güvenliğimiz ve savunmasına katkı sağlama beklenmektedir.

Bu kitap serimizin dördüncü cildinde, 15 farklı bölüm sunulmuştur. Siber güvenliğin farklı açılardan irdelediği bu ciltte; siber güvenliğin kapsamı ve boyutu, yapılan saldırıların türleri, alınabilecek önlemler, karşılaşılan yeni riskler ve problemlere yer verilmiş, karşılaşılabilen risklere dikkat çekilmiş ve sonuçta alınması gereken önlemler ve yapılması gerekenler özetlenmiştir. Her bir bölüm; ülkemizde bu alana katkı sağlayan, bu alanda eğitim almış, tez hazırlamış, çalışmalar yapmış değerli akademisyen, kamu çalışanı ve üst düzey yöneticiler tarafından hazırlanmıştır. Her bir bölüm, birbirinden bağımsız olarak hazırlansa da konu bütünlüğü ve devamlılığının sağlanmasına mümkün olduğunda dikkat edilmiştir. Her bölüm tarafından değerlendirilmiş, yazarlara konu içeriği ve başlıklarla ilgili olarak bazı önerilerde bulunulmuş, düzeltmeler yapılması istenilmiştir ve sonuçta yapılan değişiklikler dikkate alınarak bu kitap hazırlanmıştır. Kitapta yazılan bölümler intihal taramasından geçirilmiş, tekrar tekrar kontrol edilmiş, yapılan çalışmalar ise her bölümün sonunda bölüm yazarları tarafından değerlendirilmiştir.

Bu kitabın, siber güvenlik ve savunma konusunda yapılacak çalışmalara ışık tutması, yeni çalışmaların yapılmasına katkı sağlama, bu konuda yapılacak olan işbirliklerini geliştirmesi, bu konunun boyutunun ve kapsamının daha iyi anlaşılmasına katkı sağlama ve en önemlisi ise bilgi güvenliği ve siber güvenlik alanında duyulan ihtiyacı bir nebze de olsa karşılaması, açık kaynak olarak sunulması ile de kaynaklara erişimi kolaylaştırıcı bir başvuru kitabı serisi olması beklenmektedir. Bu eser serisi açık kaynak olarak, Bilgi Güvenliği Derneği web sayfasında (www.bilgiguvenligi.org.tr) yayımlanmaktadır.

Bu kitapta yazarlarımız; alan uzmanlıklarına göre bölümleri hazırlamışlar, kişisel ve kurumsal bilgi birikimlerini hazırladıkları bölümlerde sunmuşlar, hazırladıkları bölümlerin açık kaynak olarak yayımlanmasını kabul etmişler ve bu kitabın basımı ve dağıtım ile ilgili olarak herhangi bir telif hakkı talep etmemişlerdir. Yazarlara, bu kitap serisinin editörleri olarak çok özel teşekkürlerimi ve şükranları sunarız.

Kitabın titizlikle hazırlanmasında, kontrolünde ve basılmasında başta yazarlarımız olmak üzere emeği geçen tüm paydaşlarımıza, bu fikri hayatı geçiren Bilgi Güvenliği Derneği YK üyelerimize ve özellikle de basılmasına maddi destek veren HAVELSAN A.Ş.'ye teşekkürlerimizi sunarız.



Prof. Dr. Şeref SAĞIROĞLU

BGD Kurucu Üyesi ve II. Başkanı
Gazi Üniversitesi Mühendislik Fakültesi Dekanı
FutureTech Genel Müdürü



Doç. Dr. Sedat AKLEYLEK

BGD Ulusal Bilim Kurulu Üyesi,
Ondokuz Mayıs Üniversitesi Mühendislik Fakültesi
Bilgisayar Mühendisliği Bölümü Öğretim Üyesi
SdataM Bilişim Teknolojileri ve Güvenliği
Ltd. Şti. Kurucu Ortağı

İÇİNDEKİLER

Bölüm Yazarları.....	iii
Bilgi Güvenliği Derneği'nden.....	V
Editörlerden	VII

Bölüm 1 **SİS BİLİŞİMİ VE UYGULAMALARINDA VERİ GÜVENLİĞİ1**

Sedat Akleylek - Aykut Karakaya

1.1. Giriş	2
1.2. Sis Bilişimin Özellikleri	7
1.3. Sis, Kenar ve Bulut Bilişim	9
1.3.1. Sybil Saldırısı	13
1.3.2. Wormhole Saldırısı.....	14
1.3.3. Fiziksel Saldırılar.....	15
1.3.4. Dağıtık Hizmet Reddi (Distributed Denial of Service - DDoS).....	16
1.4. IoT Uygulamalarında Sis Bilişim Kullanımında Güvenlik İhtiyaçları	18
1.5. IoT Uygulamalarında Sis Bilişim Kullanımı	22
1.5.1. Bağlantılı Araçlar (Connected Vehicles).....	23
1.5.2. Kablosuz Sensör Ağları (Wireless Sensor Networks - WSN)	24
1.5.3. Akıllı Şebeke (Smart Grid).....	24
1.6. Sonuç ve Değerlendirmeler	25
Kaynaklar.....	26

Bölüm 2 **SALDIRI TESPİT SİSTEMLERİ VE LOG (GÜNLÜK) ANALİZİ.....29**

Hidayet Taşçı

2.1. Giriş	29
2.2. Saldırı Tespit Sistemleri.....	33
2.2.1. Host Tabanlı Saldırı Tespiti.....	35
2.2.2. Ağ Tabanlı Saldırı Tespiti.....	36
2.3. Saldırı Tespitinde Kullanılan Yöntemler.....	38
2.3.1. İmza Tabanlı Saldırı Tespiti	39
2.3.2. Anormallilik Tabanlı Saldırı Tespiti	40
2.4. Veri Madenciliği ile Saldırı Tespiti	45
2.4.1. Saldırı Tespit Sistemleri ve Web Kullanım Madenciliği	46
2.4.2. Web Miner Tasarımı	47
2.5. Sonuç ve Değerlendirmeler	51
Kaynaklar.....	53

Bölüm 3

AÇIK KAYNAK İSTİHBARATI (Open Source Intelligence Osint).....**55**

Hüseyin Akarslan

3.1. Giriş	55
3.2. Açık kaynak İstihbaratı.....	56
3.2.1. Açık Kaynak İstihbaratının Sınıflandırılması.....	58
3.2.2. Açık Kaynak İstihbaratının Avantajları ve Dezavantajları.....	62
3.2.3. 21. Yüzyılda Açık Kaynak İstihbaratı	63
3.3. Açık Kaynak İstihbaratı Toplama Süreci	65
3.3.1. Açık Kaynak İstihbaratı Toplama Öncesi Hazırlık.....	66
3.3.2. Açık Kaynak İstihbaratı Döngüsü.....	68
3.3.3. Açık Kaynak İstihbaratı Araçları ve Teknikleri	70
3.3.3.1. Metin Madenciliği (Text Mining).....	72
3.3.3.2. Sosyal Ağ Analizi (Social Network Analysis)	74
3.3.3.3. Mekânsal Analiz (Geospatial Analysis).....	76
3.4. Derin Web ve Karanlık Web Açısından Açık Kaynak İstihbaratı	78
3.5. Büyük Veri ve Açık Kaynak İstihbaratı	82
3.6. Yapay Zekâ ve Açık Kaynak İstihbaratı	84
3.7. Standartlar ve Platformlar	86
3.8. Açık Kaynak İstihbaratı Projeleri	88
3.9. Tehdit İstihbaratının Tehdit ve Fırsatları	90
3.10. Sonuç ve Değerlendirmeler	92
Kaynaklar.....	94

Bölüm 4

BİYOLOJİK BİYOMETRİK SİSTEMLER, BİYOMETRİK VERİLER, HUKUK VE GÜVENLİK.....**103**

Pelin Özkaya - Refik Samet

4.1. Giriş	104
4.2. Biyolojik Biyometrik Sistem Çeşitleri	107
4.2.1. Parmak İzi	108
4.2.2. Yüz Tanıma	113
4.2.3. İris Tanıma	119
4.2.4. Retina Tanıma	122
4.2.5. DNA Kimlik Teknolojisi.....	124
4.2.6. El Geometrisi.....	126
4.2.7. Avuç İçi Tanıma	131
4.3. Biyometrik Verilerin Karşılaştırılması	135
4.4. Biyometri ve Kamu Güvenliği	138
4.5. Biyometri ve Sivil Kimlik	140
4.6. Biyometri ve Özel Veri Güvenliği.....	141
4.7. Biyometrik Korsanlık	143
4.8. Hukuki Düzenlemeler.....	146
4.8.1. GDPR (General Data Protection Regulation - AB Genel Veri Koruma Tüzüğü) ..	148
4.8.2. Kişisel Verilerin Korunması Kanunu (KVKK)	151
4.8.3. Türk Ceza Kanunu (TCK)	154
4.9. Sonuç ve Değerlendirmeler	155
Kaynaklar.....	157

Bölüm 5

DAVRANIŞSAL BİYOMETRİK SİSTEMLER, TEKNOLOJİLER VE GÜVENLİK 163

Hande Tutumluer - Refik Samet

5.1. Giriş	164
5.2. Kaynak Tabanlı Davranışsal Biyometri.....	166
5.2.1. Metin Yazarlığı.....	167
5.2.2. E-posta Yazarlığı.....	168
5.2.3. Eskiz Stili	169
5.2.4. Boyama Stili.....	169
5.3. İnsan - Bilgisayar Etkileşimi Tabanlı Davranışsal Biyometri.....	170
5.3.1. Tuş Vuruşu Dinamikleri.....	171
5.3.2. Fare Dinamiği	172
5.3.3. Komut Satırı Girdileri	173
5.3.4. Grafiksel Kullanıcı Arayüzü (Graphical User Interface - GUI)	174
5.4. Motor Beceriye Dayalı Davranışsal Biyometri	174
5.4.1. Dudak Hareketleri.....	175
5.4.2. Göz Kırpması	176
5.4.3. Yürüyüş	176
5.4.4. Dinamik Yüz Özellikleri.....	178
5.4.5. Dokunsal Biyometri / Haptik (Mobil Etkileşimler).....	179
5.4.6. İmza / El Yazısı	180
5.4.7. Ses	182
5.5. Saf Davranışsal Biyometri	184
5.5.1. Araba Sürüş Stili.....	184
5.5.2. Oyun Stratejileri	185
5.5.3. Kredi Kartı Kullanımı	185
5.5.4. Çağrı Alışkanlıkları.....	186
5.5.5. Programlama (Kodlama) Stilleri	186
5.6. Davranışsal Biyometri Karşılaştırılmaları.....	187
5.7. Davranışsal Biyometri ve Adli Bilişim.....	189
5.8. Davranışsal Biyometrinin Hukuki Dayanağı	191
5.9. Sonuç ve Değerlendirmeler	192
Kaynaklar	198

Bölüm 6

BİYOMETRİDE YENİ NESİL DAVRANIŞ MODELLEME YAKLAŞIMLARI, RİSKLER VE ÖNGÖRÜLER 205

Bilgehan Arslan - Çağla Aksoy - Şeref Sağıroğlu

6.1. Giriş	206
6.2. Biyometrinin Tanımı, Tarihçesi ve Gelişim Süreci	207
6.3. Biyometrik Karakteristikler ve Veri Türleri	210
6.4. Sosyal Davranış Biyometrikleri ve Yumuşak Biyometrikler	218
6.5. Sonuç ve Değerlendirmeler	222
Kaynaklar	228

Bölüm 7

KAFES TABANLI KRIPTOGRAFİDE KULLANILAN ZOR PROBLEMLERİN KRIPTANALİZİ VE YAZILIM KÜTÜPHANELERİ.....**233**

Hami Satılmış - Sedat Akleylek

7.1.	Giriş	233
7.2.	Literatür Özeti	235
7.2.1.	Eleme Algoritmaları ve Uygulamaları	235
7.2.2.	Numaralandırma Algoritmaları ve Uygulamaları.....	236
7.2.3.	Kriptanaliz Yazılım Kütüphaneleri.....	238
7.3.	Kriptanaliz Algoritmaları.....	239
7.3.1.	Eleme Tabanlı Algoritmalar.....	239
7.3.1.1.	GaussSieve ve ProGaussSieve Eleme Algoritmaları	239
7.3.1.2.	HashSieve Eleme Algoritması.....	241
7.3.1.3.	Eleme Algoritmalarının Özelliklerinin Karşılaştırılması.....	243
7.3.2.	Numaralandırma Tabanlı Algoritmalar.....	243
7.3.2.1.	ENUM Numaralandırma Algoritması.....	244
7.3.2.2.	Schnorr ve Euchner'in BKZ İndirgeme Algoritması.....	245
7.4.	Uygulamalar ve Yazılım Kütüphaneleri.....	247
7.4.1.	Kriptanaliz Algoritmalarına Ait Uygulamalar.....	247
7.4.2.	Yazılım Kütüphaneleri	249
7.5.	Sonuç ve Değerlendirmeler	251
	Kaynaklar	253

Bölüm 8

AĞ ANOMALİ TESPİTİNDE MAKİNE ÖĞRENMESİ ALGORİTMALARININ KULLANILMASI VE SINIFLANDIRMA İÇİN BİR UYGULAMA ÖRNEĞİ ..**257**

Habibe Güler - Şeref Sağıroğlu

8.1.	Giriş	258
8.2.	Ağlarda Anomali Tespiti ve Saldırı Tespit Sistemleri	259
8.2.1.	Anomali Türleri.....	260
8.2.2.	Anomali Tespit Tekniklerinin Çıktıları.....	261
8.2.3.	Anomali Tespitinde Kullanılan Yöntemler.....	262
8.2.4.	Anomali Tespitinin Uygulama Alanları	264
8.2.5.	Saldırı Türleri	264
8.2.6.	Ağ Saldırı Tespit Sistemleri.....	266
8.2.7.	Ağ Anomali Tespitinde Karşılaşılan Zorluklar.....	267
8.3.	Uygulamada Kullanılan Araç ve Yöntemler	268
8.3.1.	Araçlar	268
8.3.2.	Sınıflandırma Algoritmaları.....	269
8.4.	Uygulamanın Gerçekleştirilmesi	273
8.4.1.	Veri Setinin İncelenmesi	273
8.4.2.	Veri Setinin Görselleştirilme İşlemleri	276
8.4.3.	Veri Seti Üzerinde Uygulanan İşlemler.....	280
8.4.4.	Algoritmaların Uygulanması	281
8.5.	Testler ve Karşılaştırmalar.....	289
8.5.1.	Performans Metrikleri.....	289

8.5.2. Algoritmaların Karşılaştırılması.....	290
8.6. Sonuç ve Değerlendirmeler	291
Kaynaklar.....	293

**Bölüm 9
KRİPTOGRAFİK BLOK ŞİFRELERİN MAKSİMUM UZAKLIKLA AYRILABİLEN
YAYILIM TABAKALARININ TASARIMI 295**

Meltem Kurt Pehlivanoglu - Elif Bilge Kavun

9.1. Giriş	295
9.2. MDS Matrisler İçin Matematiksel Altyapı	298
9.3. (Tersi Kendisine Eşit) MDS Matris Tasarım Yöntemleri	305
9.3.1. (Tersi Kendisine Eşit) MDS Matrisler için Özyinelemeli ve Özyinelemeli - Olmayan Tasarım Yöntemleri	306
9.3.2. (Tersi Kendisine Eşit) MDS Matrisler için Doğrudan Tasarım, Arama ve Hibrit Tasarım Yöntemleri	310
9.4. (Tersi kendisine eşit) MDS Matrisler İçin Yerel ve Genel Optimizasyon Yöntemleri	316
9.4.1. (Tersi Kendisine Eşit) MDS Matrisler için Yerel Optimizasyon Yöntemleri.....	317
9.4.2. (Tersi Kendisine Eşit) MDS Matrisler için Genel Optimizasyon Yöntemleri.....	320
9.5. Sonuç ve Değerlendirmeler	324
Kaynaklar	325

**Bölüm 10
GÜVENLİK UYGULAMALARINI HEDEFLEYEN FİZİKSEL SALDIRILAR
VE BUNLARA KARŞI ALINABİLİR ÖNLEMLER 331**

Meltem Kurt Pehlivanoglu - Elif Bilge Kavun

10.1. Giriş	331
10.2. Fiziksel Saldırılar	333
10.2.1. Bozucu Saldırılar	333
10.2.2. Bozucu Olmayan Saldırılar.....	335
10.2.3. Yarı Bozucu Saldırılar.....	343
10.3. Fiziksel Saldırı Güvenlik Değerlendirmeleri ve Önlemleri.....	345
10.3.1. Bozucu Saldırı Önlemleri.....	346
10.3.2. Bozucu Olmayan Saldırı Önlemleri	347
10.3.3. Yarı Bozucu Saldırı Önlemleri	351
10.4. Sonuç ve Değerlendirmeler	354
Kaynaklar	355

**Bölüm 11
KÜRESEL SALGININ ULUSAL BİLİŞİM GÜVENLİĞİNE ETKİLERİ 361**

Ensar Şeker

11.1. Giriş	361
11.2. Yeni Çalışma Düzeni; Uzaktan İş Gücü.....	362
11.3. Pandemi ve Bilgi Güvenliği	363
11.4. COVID-19 Salgınının Ortasında Siber Tehditler.....	363
11.4.1. Sahte Alan Adları ve Web Sayfaları	367
11.4.2. Oltalama Saldırıları	368

11.4.3. Uç-Nokta Saldırıları	368
11.4.4. Uzaktan Eğitim Sistemlerine Saldırılar	368
11.4.5. Sağlık Bakanlıkları, Araştırma Laboratuvarları ve Hastanelere DDoS ve Fidye Yazılım Saldırıları	369
11.4.6. DarkWeb'de Sahte Kit, Sahte İlaç ve Plazma Satışları	370
11.4.7. Telekonferans Uygulamalarına Yapılan Saldırılar	371
11.4.8. COVID-19 Kötüçül Yazılımı	371
11.4.9. VPN Saldırıları	372
11.5. Saldırılara Karşı Tedbirler	372
11.5.1. Kullanıcılara Yönelik Sorumluluklar	373
11.5.2. Organizasyonlara Yönelik Sorumluluklar	373
11.5.3. Siber Operasyon ve Siber Olaylara Müdahale Merkezleri	373
11.6. Ulusal Bilişim Güvenliği	374
11.7. Sonuç ve Değerlendirmeler	378
Kaynaklar	379

Bölüm 12 **DEVSECOPS** 381

Murat Kaya - Tuğkan Tuğlular

12.1. Giriş	381
12.2. DevOps	383
12.3. DevSecOps	388
12.3.1. DevSecOps'un Genel Tanımı	388
12.3.2. DevSecOps Neden Bu Kadar Önemli?	389
12.3.3. DevSecOps'un Faydaları	390
12.4. DevSecOps Temelleri	391
12.4.1. Temel İlkeler	391
12.4.2. DevSecOps Yaşam Döngüsü	392
12.4.3. DevSecOps'ta Katmanlar	393
12.5. DevSecOps Hattı	399
12.6. DevSecOps Araçları	403
12.7. Sonuç ve Değerlendirmeler	410
Kaynaklar	411

Bölüm 13 **ENDÜSTRİYEL KONTROL SİSTEMLERİNİN SİBER GÜVENLİĞİ** 413

Ismail Erkek - Erdal Irmak

13.1. Giriş	414
13.2. SCADA Sistemi Güvenlik Açıkları	416
13.2.1. Kaynak Kodu Tasarımı ve Uygulaması	419
13.2.2. Bellek Taşırma (Buffer Overflow)	420
13.2.3. SQL Enjeksiyonu	421
13.2.4. XSS (Cross Site Scripting) Açığı	422
13.2.5. Gereksiz Portlar ve Servisler	422
13.2.6. Etkili Yama Yönetimi Uygulaması	423
13.2.7. Haberleşme Kanalı Güvenlik Açıkları	424
13.2.8. Haberleşme Protokollerinin Açıklıkları	424

13.2.8.1. DNP3 Açıklıkları ve Saldırıları	424
13.2.8.2. Modbus Açıklıkları ve Saldırıları	425
13.2.8.3. Profinet Açıklıkları ve Saldırıları	426
13.3. SCADA Güvenlik Testi Araçları	427
13.3.1. Shodan Arama Motoru	427
13.3.2. Wireshark Ağ Analiz Programı	429
13.3.3. Nmap Ağ Tarama Aracı	431
13.3.4. Plcscan Aracı	431
13.3.5. Snmpcheck	432
13.3.6. Metasploit Framework	433
13.3.6.1. Modbusdetect Modülü	434
13.3.6.2. Modbusclient Modülü	435
13.4. Literatürdeki Kritik Altyapılara Yönelik Siber Saldırılar	437
13.4.1. Sibirya Boru Hattı Patlaması	438
13.4.2. The Salt River Proje (SRP) Ele Geçirme Olayı	438
13.4.3. Houston Limanı Sistem Arızası	439
13.4.4. Slammer Solucanı	439
13.4.5. Kaliforniya Kanal Sisteminin Hacklenmesi	439
13.4.6. ABD'de Elektrik Şebekesi Casusluk İhlali	440
13.4.7. Nitro Saldırıları	440
13.4.8. Stuxnet Solucanı	441
13.4.9. Duqu Truva Atı	442
13.4.10. Shamoon Zararlı Yazılımı	442
13.4.11. Flame Zararlı Yazılımı	443
13.4.12. Doğalgaz Boru Hattı Firmalarına Siber Saldırılar	444
13.4.13. Ukrayna Elektrik Kesintisi	444
13.4.13.1. BlackEnergy'nin 2015'teki Gelişimi	445
13.4.13.2. Killdisk Bileşeni	446
13.5. Sonuç ve Değerlendirmeler	448
Kaynaklar	449
 Bölüm 14	453
ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNDE KARŞILAŞILAN UYGULAMA ZORLUKLARI	453
Samime Meral - Halil İbrahim Bülbül	
14.1. Giriş	454
14.2. BGYS Kapsamında Yapılması Gereken Çalışmalar	457
14.3. BGYS Kapsamında Geniş Tutulmasındaki Uygulama Zorlukları	459
14.4. Sonuç ve Değerlendirmeler	467
Kaynaklar	471
 Bölüm 15	473
SİBER TEHDİT İSTİHBARATI VE SALDIRI TESPİT SİSTEMLERİNDE BÜYÜK VERİ TEKNOLOJİLERİ	473
Yavuz Canbay	
15.1. Giriş	473
15.2. Siber Tehdit İstihbaratı	476

15.3. Saldırı Tespit Sistemleri.....	479
15.4. Büyük Veri ve Teknolojileri.....	481
15.5. Saldırı Tespit Sistemleri ve Siber Tehdit İstihbaratına Yönelik Yapılan Çalışmalar	484
15.5.1. Büyük Veri Teknolojileri Kullanılarak Geliştirilen Saldırı Tespit Sistemleri	484
15.5.2. Büyük Veri Teknolojileri Kullanılarak Geliştirilen Siber Tehdit İstihbarat Sistemleri	487
15.5.3. Siber Tehdit İstihbarat Sistemleri Üzerine Yapılan Çalışmalar	488
15.6. Sonuç ve Değerlendirmeler	489
Kaynaklar.....	491
DİZİN.....	495
YAZARLAR.....	497

Bölüm 9

KRIPTOGRAFİK BLOK ŞİFRELERİN MAKSİMUM UZAKLIKLA AYRILABİLEN YAYILIM TABAKALARININ TASARIMI

Meltem Kurt Pehlivanoğlu - Elif Bilge Kavun

Bu bölümde, kriptografideki blok şifreleme algoritmalarının en önemli bileşenlerinden biri olan yayılım tabakalarının ayrıntılı incelemesine yer verilmiştir. Kriptografik açıdan güvenli yayılım tabakalarının tasarımında kullanılan yöntemler ve bu yöntemlerin dayandırıldığı yapılar kapsamlı olarak sunulmuştur. Blok şifreleme algoritmalarında çoğunlukla yayılım tabakası olarak kullanılan ve maksimum yayılma sağlayan MDS (Maximum Distance Separable - Maksimum Uzaklıkla Ayrılabilen) matrislerin üretimi için geliştirilen farklı tasarım yöntemleri ve bu yöntemlere ait matematiksel altyapı verilmiştir. Bunun yanı sıra literatürde yer alan yerel (local) ve genel (global) optimizasyon teknikleri karşılaştırmalı olarak sunulmuştur.

9.1. GİRİŞ

Kerckhoffs'un Prensibi'ne göre [1] bir kriptosistemin güvenliği, kullanılan algoritmanın veya parametrelerin gizliliğine dayanmaz. Bu ilke güvenliğin sadece kriptosistemde kullanılan anahtarın gizliliğine bağlı olacağı anlamına gelir. Blok şifreler, seçilen gizli anahtar yardımıyla, sabit uzunluktaki bloklar (bit dizileri) kümesine şifreleme/şifre çözme işlemi uygulayan algoritmalarıdır. Blok şifrelerin tasarım prensibi Shannon'un önerdiği karıştırma (confusion) ve yayılma (diffusion) tekniklerine dayanır. Bu teknikler bir şifreyi istatis-

tiksel saldırılardan korumaya yarar. Karıştırma, gizli anahtar ile şifreli metin arasındaki ilişkiyi gizlemeyi amaçlar. Diğer bir ifadeyle; gizli anahtar öyle bir şekilde kullanılır ki, bir saldırgan açık metnin istatistiksel dağılımını bilse veya çok sayıda düz metin/şifreli metin çiftlerine sahip olsa bile, gizli anahtarı hâlâ çıkaramaz. Yayılma ise açık metinle şifreli metin arasındaki ilişkiyi gizler. Şifreli metnin her bir parçası mümkün olduğunca açık metne bağlı olmalıdır ki; açık metinde yapılacak çok küçük bir değişim (örneğin 1 bit değişim) şifreli metin üzerinde olabildiğince fazla değişim sağlamalı, diğer bir ifadeyle bu değişim maksimum yayılmalıdır [2]. Blok şifreler, temelde doğrusal olmayan tabaka (confusion layer), yayılım tabakası (diffusion/permuation layer) ve anahtar planlama algoritmasının (key scheduling algorithm) yer aldığı döngü (round) adı verilen yapılardan oluşurlar. Her döngüde farklı döngü anahtarı (alt anahtarlar) kullanılır ve bu anahtarlar anahtar planlama algoritması kullanılarak üretilir. Karıştırmanın sağlandığı doğrusal olmayan tabakada şifrenin tek doğrusal olmayan yapısı olarak yer değiştirme kutuları (Substitution-boxes – S-kutuları) kullanılırken, yayılmayı sağlayan yayılım tabakasında ise doğrusal dönüşümler kullanılır. Açık metin üzerinde yapılan bit değişimlerinden olabildiğince fazla saydaki S-kutusunun etkilenmesi beklenir. Bu bit değişiminden etkilenen S-kutusu sayısı, aktif S-kutusu olarak bilinir ve minimum aktif S-kutusu sayısının maksimum olması beklenir. S-kutuları ile ilgili literatürdeki çalışmalar incelendiğinde bu alanın iyi çalışıldığı görülebilir ancak kriptografik açıdan güclü ve verimli yayılım tabakalarının tasarımı hâlâ açık bir problemdir [3].

Blok şifreler farklı tasarım mimarileri kullanılarak tasarlanabilir, en temel iki tasarım mimarisini Feistel Ağları (Feistel Networks) ile Yer değiştirme ve Permutasyon Ağlarıdır (Substitution Permutation Networks–SPN). Feistel mimarisinde döngü bloğu ikiye bölünerek dallara ayrılır ve bu mimaride dalaın yarısı işlenirken, SPN mimarisinde döngü bloğunun tamamı işlenir. Her iki mimariye ilişkin karşılaşmalı kapsamlı bilgiye [2]’den erişilebilir.

Kriptografik açıdan güvenli ve verimli yayılım tabakalarının tasarımı önemlidir. İyi yayılımın sağlanması için bilinen iki genel tasarım yaklaşımı vardır; ad – hoc (geçici) [4] ve wide–trail (geniş–iz) [5]. Geçici yaklaşımda optimum izlerin bulunması için bilgisayar destekli araçlar gereklidir. Geniş–iz yaklaşımında ise doğrusal ve diferansiyel saldırılara [6] karşı dayanıklı tasarım sağlanması için; kaynakların büyük boyutlu S-kutuları için kullanımını yerine, yüksek yayılımın sağlanacağı doğrusal dönüşümlere (diğer bir ifadeyle yayılım taba-

kalarına) harcanması amaçlanır. Kaynakların kriptografik açıdan güvenli ve verimli yayılım tabakalarının tasarımını için kullanımı, aktif S-kutusu sayısını da artıracaktır. Aktif S-kutularının hesaplanması ile ilgili kapsamlı bilgiye [7]'den erişilebilir. Geniş-iz tasarım yaklaşımı yayılım tabakalarının tasarımının önemini vurgulasa da uygun sayıda aktif S-kutusu ile verimli ve güvenli yayılım tabakalarının nasıl tasarılanması gerektiği önemli bir araştırma problemidir. Bunun yanında kaynak kısıtlı cihazlar (kısıtlı hesaplama gücü, bellek kapasitesi, güç kaynağı) için önerilen hafif sıklet (lightweight) kripto sistemlerin yayılım tabakalarının tasarımını da literatürde yer alan bir diğer açık problemdir [8].

Bir blok şifrede yayılım tabakaları farklı yapılar kullanılarak oluşturulabilir; bit permütasyonlarının kullanımı, dalların karıştırılması (the shuffle of the branches), doğrusal cebir tabanlı (linear algebra based) yapıların kullanılması [2] bu yapılara örnek olarak gösterilebilir. Bit permütasyonlarında S-kutusu çıktı bitleri, bit permütasyonları kullanılarak karıştırılır. Bit permütasyonları, düşük maliyetli (low-cost) donanım hedefli blok şifreler için uygundur. Bu yapılarda bir çıkış biti bir sonraki katmanın yalnızca (en fazla) tek bir giriş bitini etkiler, bu nedenle yayılım oldukça yavaştır ve fazla sayıda döngüye ihtiyaç duyulur. PRESENT [9], PRINTcipher [10], Khazad [11], Anubis [12], ICE-BERG [13] blok şifreleri yayılım tabakalarında bit permütasyonu kullanırlar. Dalların karıştırılması Feistel mimarisindeki blok şifreler için kullanılan yöntemlerden biridir ve dalların dairesel olarak kaydırılması işlemidir. DES [14], SAFER family [15], [16] ve FROG [17] blok şifreleri yayılım tabakalarında bu yöntemi kullanırlar. Doğrusal cebir tabanlı yayılım tabakaları, elemanları sonlu cisim üzerinde tanımlı matrisler olarak ifade edilebilir [2]. Shark [18], SQUARE [19], AES [20], Twofish [21], Camellia [22] blok şifreleri yayılım tabakası olarak doğrusal cebir tabanlı yayılım matrislerini kullanırlar.

Blok şifrelerde kullanılan yayılım tabakalarının tasarımındaki hedef en iyi yayılmayı (perfect diffusion) sağlamaktır. Cebirsel yayılım tabakaları ele alındığında, bir blok şifredeki en iyi yayılma; çoklu permütasyonu sağladığı için MDS matrislerin kullanımıyla elde edilir [23]. Bu nedenle maksimum yayılmayı sağlayan MDS matrislerin tasarımını literatürde çalışılan önemli açık problemlerden biridir [24].

Bu bölümde blok şifrelerde kullanılan en önemli yayılım tabakası tasarımlarından biri olan MDS matrislere ait matematiksel altyapı ve bu matrislerin

tasarım yöntemleri verilmiştir. Ayrıca bu yöntemler yerel ve genel optimizasyon teknikleri açısından karşılaştırmalı olarak sunulmuştur.

Çalışmanın ilerleyen bölümleri şu şekilde düzenlenmiştir; Bölüm 9.2'de MDS matrisler için matematiksel altyapı verilmiştir. Bölüm 9.3'te ise MDS matrisler için geliştirilen farklı tasarım yöntemleri sunulmuştur. Bölüm 9.4'te, Bölüm 9.3'te verilen tasarım yöntemleri yerel ve genel optimizasyon açısından değerlendirilmiştir. Son bölümde ise çalışmada verilen kapsamlı bilgiler değerlendirilerek özetlenmiştir.

9.2. MDS MATRİSLER İÇİN MATEMATİKSEL ALTYAPI

Bu bölümde MDS matrislerin dayandığı matematiksel tanımlar ve önermeler yer verilmiştir. MDS matrislerle ilgili detaylı tanımlamalara ve önermelere [25]'ten erişilebilir.

Tanım 9.1. (Sonlu Cisim): Sonlu sayıda elemanı olan cisim sonlu cisim olarak ifade edilir. \mathbb{F} sonlu cisim ve m pozitif sayı olmak üzere \mathbb{F}_{2^m} sonlu cismi, elemanları $\{0, 1\}$ 'den oluşan \mathbb{F}_2 sonlu cisminin m . dereceden genişletilmiş bir cismidir ve 2^m elemana sahiptir.

\mathbb{F}_{2^m} sonlu cisminin her bir elemanı katsayıları \mathbb{F}_2 cisminde tanımlı ve derecesi $m-1$ olan bir polinom şeklinde ifade edilebilir. α ilkel eleman ve $x \in \mathbb{F}_{2^m}$ olmak üzere; x elemanın polinom tabanlı gösterimi Eşitlik (9.1)'deki gibidir.

$$x_{m-1}\alpha^{m-1} + x_{m-2}\alpha^{m-2} + \dots + x_1\alpha + x_0 \quad (9.1)$$

Önerme 9.2. (Singleton Sınırı): Bir doğrusal kod C $[n, k, d]$ için Singleton sınırı $d \leq n - k + 1$ 'dir.

Tanım 9.3. (MDS Kod): C $[n, k, d]$ kodu için $d = n - k + 1$ ise C MDS koddur denir.

Önerme 9.4. (MDS Matris): C $[n, k, d]$ kodu, I $k \times k$ boyutlu birim matris, A $k \times (n-k)$ boyutlu matris ve $G = [I \mid A]$ üreteç matris olmak üzere, C ancak ve ancak A matrisinin satır ve sütunlarını oluşturan tüm alt kare matrislerin determinantı sıfırdan farklı (tekil olmayan matris) ise MDS koddur ve bu durumda A matrisi MDS matristir denir.

Bir blok şifrede iyi yayılma istenirken bir taraftan da şifrenin hızlı olması beklenir. Bu nedenle bu iki metrik arasında denge sağlamak amaçlı, optimum yayılmayı (optimal diffusion) hedefleyen yayılım matrislerinin kullanılması

gerekir. Daemen [5] optimum yayılmayı dal sayısı (branch number) metriğiyle ifade etmiştir ve dal sayısı β gösterimi ile tanımlanabilir. θ tersi alınabilir (invertible) doğrusal dönüşüm olmak üzere, θ 'nın dal sayısı β_θ Eşitlik (9.2)'deki gibidir.

$$\beta_\theta = \min_{\alpha \neq 0} \{wt(\alpha) + wt(\theta(\alpha))\} \quad (9.2)$$

$wt(\alpha)$; α 'nın Hamming ağırlığını (1 'e eşit olan elemanların sayısı) ifade eder. $wt(\alpha) \leq n$, her θ için, eğer $wt(\alpha) = 1$ ise bu da $\beta_\theta \leq n + 1$ olduğu anlaşıma gelir. θ tersi alınabilir bir doğrusal dönüşümü için optimum dal sayısı $\beta_\theta = n + 1$ 'dir [5].

Dal sayısı, bir matrisin ifade ettiği doğrusal dönüşümün yayılma gücünü tanımlar. Matrisin kendisinin dal sayısı (β_d) diferansiyel yayılmayı ölçerken, matrisin devriğinin (transpose) dal sayısı (β_l) doğrusal yayılmayı ölçer. Dal sayısı, en kötü durumdaki (worst-case) yayılmayı ölçer, şöyle ki iki ardışık döngüdeki aktif S-kutusu sayısı için alt sınır değerini (en kötü durumdaki minimum aktif S-kutusu sayısı) verir [2]. Tanım 9.5'te diferansiyel dal sayısı, Tanım 9.6'da ise doğrusal dal sayısı eşitlikleri verilmiştir.

Tanım 9.5. (Diferansiyel Dal Sayısı): $n \times n$ boyutlu A matrisinin diferansiyel dal sayısı;

$$\beta_d = \min \{wt(x) + wt(A \cdot x^T) \mid x \in (\{0,1\}^m)^n, x \neq 0\} \quad (9.3)$$

olarak ifade edilmektedir.

Tanım 9.6. (Doğrusal Dal Sayısı): $n \times n$ boyutlu A matrisinin doğrusal dal sayısı;

$$\beta_l = \min \{wt(x) + wt(A^T \cdot x^T) \mid x \in (\{0,1\}^m)^n, x \neq 0\} \quad (9.4)$$

olarak ifade edilmektedir.

Bir doğrusal dönüşüm için optimum dal sayısı $\beta_\theta = n + 1$ olduğundan, $\beta_d(A)$ ve $\beta_l(A)$ dal sayılarının maksimum değeri $n + 1$ 'dir. Bu değer MDS kodlarla oluşturulan doğrusal dönüşümlerle sağlanabilir, bu da MDS matrislerin optimum yayılma sağladığını kanıtlar [5].

MDS matrisler için önemli özellikler aşağıdaki gibi verilebilir;

- $n \times n$ boyutlu M matrisi ancak ve ancak satır ve sütunlarını oluşturan tüm alt kare matrisleri tekil olmayan matris ise ve M matrisinin elemanları 0 'dan farklı ise MDS matristir.

- $n \times n$ boyutlu M matrisi MDS matris ise, M matrisinin tüm alt kare matrislerinin rank'ı tam (full) rank'tır.
- $n \times n$ boyutlu M matrisi MDS matris ise, M matrisinin tüm alt kare matrisleri de MDS matristir.
- $n \times n$ boyutlu M matrisi MDS matris ise, M matrisinin devriği (transpose) M^T MDS matristir.
- $n \times n$ boyutlu M matrisi MDS matris ise, M matrisinin tersi M^{-1} matrisi MDS matristir.
- $n \times n$ boyutlu M MDS matrisinin herhangi bir satır veya sütunu herhangi bir c ($c \in \mathbb{F}_{2^m}, c \neq 0$) sabitiyle çarpıldığında MDS özelliği korunur.
- $n \times n$ boyutlu M MDS matrisinin diferansiyel $\beta_d(M)$ ve doğrusal $\beta_l(M)$ dal sayıları $n+1$ 'dir.

Bunun yanında tersi kendisine eşit (involutory) ve ortogonal (orthogonal) yapılar, MDS matrislerin tasarıımı için önemlidir. Tersi kendisine eşit ve ortogonal MDS matrisler kullanılarak blok şifrelerin verimli donanım ve yazılım uygulamaları gerçekleştirilebilir. Bu nedenle tersi kendisine eşit veya ortogonal verimli MDS matrislerin bulunması önemli bir çalışma alanıdır [26]. Tersi kendisine eşit ve ortogonal matris tanımları sırasıyla Tanım 9.7 ve Tanım 9.8'de verilmiştir.

Tanım 9.7. (Tersi Kendisine Eşit Matris): I $n \times n$ boyutlu birim matris olmak üzere, $n \times n$ boyutlu A matrisi eğer $A^2 = I$ yani $A^{-1} = A$ koşulunu sağlıyorsa bu matrisin tersi kendisine eşittir.

Tanım 9.8. (Ortogonal Matris): I $n \times n$ boyutlu birim matris olmak üzere, $n \times n$ boyutlu A matrisi eğer $AA^T = I$ yani $A^{-1} = A^T$ koşulunu sağlıyorsa bu matris ortogonal matristir.

Verimli yayılım matris tasarımıyla, bir yayılım matrisinin özellikle donanım uygulaması maliyetinin azaltılması amaçlanır. Donanım maliyeti iki önemli metrikle ölçülebilir; XOR (Exclusive Or) [27] sayısı ve derinlik [24]. Yayılım matrisinin donanım uygulamasında kullanılacağı devredeki XOR sayısının azaltılması; devrenin alanını (chip area) ve güç tüketimini (power consumption) azaltırken, devre derinliğinin azaltılması ise gecikmeyi azaltarak (low latency) daha hızlı devrelerin tasarımını sağlar [28]. Azaltılmış devre alanı, azaltılmış güç tüketimi ve hızlı devre tasarımlına sahip yayılım matrisleri; ha-

fif sıklet kriptosistemlerin yayılım tabakaları için gereklidir. XOR sayısı ve derinlik metrikleri tanımları sırasıyla, Tanım 9.9 ve Tanım 9.10'da verilmiştir.

Tanım 9.9. (XOR Sayısı): $p(x) \in \mathbb{F}_{2^m}$ sonlu cismi üzerinde indirgenemez polinom, $a \in \mathbb{F}_{2^m} / p(x)$ ve $b \in \mathbb{F}_{2^m} / p(x)$ olmak üzere, $\text{XOR}(a)$, a elemanını keyfi bir b elemanıyla çarpmak için gereken XOR sayısı olarak ifade edilir. ■

Örnek 9.10: \mathbb{F}_{2^4} sonlu cismi üzerinde, α ilkel eleman ve $p(x) = x^4 + x + 1$ (0×13) indirgenemez polinomu olmak üzere, $\mathbb{F}_{2^4} / (0 \times 13)$ sonlu cismi üzerinde herhangi bir $x \in \mathbb{F}_{2^4}$ elemanı için Eşitlik (9.1)'den faydalananlarak $x = (x_3, x_2, x_1, x_0)$ olmak üzere, $x_3\alpha^3 + x_2\alpha^2 + x_1\alpha + x_0$ şeklinde yazılabilir ve bu sonlu cisim üzerinde $9_h (= \alpha^3 + 1)$ elemanın herhangi bir x elemanı ile çarpımı;

$$x_3\alpha^3 + x_2\alpha^2 + x_1\alpha + x_0 \rightarrow (\alpha^3 + 1)(x_3\alpha^3 + x_2\alpha^2 + x_1\alpha + x_0) \bmod (0 \times 13)$$

$= x_3\alpha^6 + x_3\alpha^3 + x_2\alpha^5 + x_2\alpha^2 + x_1\alpha^4 + x_1\alpha + x_0\alpha^3 + x_0$, burada (0×13) indirgenemez polinomu altında $\alpha^6 = \alpha^3 + \alpha^2$, $\alpha^5 = \alpha^2 + \alpha$, $\alpha^4 = \alpha + 1$ olduğundan;

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

$$= \cancel{x_3\alpha^3} + x_3\alpha^2 + \cancel{x_3\alpha^3} + \cancel{x_2\alpha^2} + x_2\alpha + \cancel{x_2\alpha^2} + \cancel{x_1\alpha} + x_1 + \cancel{x_1\alpha} + x_0\alpha^3 + x_0$$

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

$$= (x_0)\alpha^3 + (x_3)\alpha^2 + (x_2)\alpha + (x_1 \oplus x_0)$$

olarak elde edilir. Buradan $(\alpha^3 + 1)$ elemanın herhangi bir x elemanı ile çarpımı için gereken XOR sayısı $\text{XOR}(\alpha^3 + 1) = 1$ 'dir.

$p(x) \in \mathbb{F}_{2^m}$ sonlu cismi üzerinde bir indirgenemez polinom, $a \in \mathbb{F}_{2^m} / p(x)$ sonlu cismi üzerinde tanımlı herhangi bir eleman olmak üzere, a elemanı \mathbb{F}_2 sonlu cismi üzerinde karşılığı olan ikili matrisle ifade edilebilir. Bu gösterim sayesinde blok şifrelerin yayılım tabakalarında kullanılacak yayılım matrisi elemanlarının \mathbb{F}_2 sonlu cismi üzerinde ikili matris karşılıkları kullanılarak, matrisin donanım devresinin giriş (x_0, x_1, \dots, x_k) ve çıkış (y_0, y_1, \dots, y_k) haritalaması elde edilir.

$\mathbb{F}_{2^4} / (0 \times 13)$ sonlu cismi üzerinde tanımlı $(\alpha^3 + 1)$ elemanı, 4×4 ikili matris karşılığıyla \mathbb{F}_2 cismi üzerinde Eşitlik (9.5)'teki gibi ifade edilebilir;

$$\begin{aligned}
 &= \underbrace{(x_0)}_{y_3} \alpha^3 + \underbrace{(x_3)}_{y_2} \alpha^2 + \underbrace{(x_2)}_{y_1} \alpha + \underbrace{(x_1 \oplus x_0)}_{y_0} \rightarrow \\
 &\quad \begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} \rightarrow \begin{array}{l} y_0 = x_0 \oplus x_1 \\ y_1 = x_2 \\ y_2 = x_3 \\ y_3 = x_0 \end{array} \tag{9.5}
 \end{aligned}$$

Örnek 9.11: \mathbb{F}_{2^4} sonlu cismi üzerinde, α ilkel eleman ve $p(x) = x^4 + x + 1$ (0×13) indirgenemez polinomu olmak üzere, $\mathbb{F}_{2^4} / (0 \times 13)$ sonlu cismi üzerinde 4×4 boyutlu

$$A = \begin{bmatrix} 3_h & 2_h & 1_h & 3_h \\ 8_h & 9_h & 2_h & 2_h \\ 9_h & 8_h & 3_h & 2_h \\ 2_h & 2_h & 3_h & 1_h \end{bmatrix} = \begin{bmatrix} \alpha^4 & \alpha & 1 & \alpha^4 \\ \alpha^3 & \alpha^{14} & \alpha & \alpha \\ \alpha^{14} & \alpha^3 & \alpha^4 & \alpha \\ \alpha & \alpha & \alpha^4 & 1 \end{bmatrix} \text{ MDS matris, } \mathbb{F}_{2^4} / (0 \times 13) \text{ sonlu cismi üzerinde tanımlı}$$

$\alpha^4, \alpha, 1, \alpha^3, \alpha^{14}$ elemanlarının, \mathbb{F}_2 cismi üzerinde 4×4 ikili matris karşılıkları

$$\alpha^4 = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, \alpha = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, 1 = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \alpha^3 = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}, \alpha^{14} = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

olmak üzere, A matrisinin \mathbb{F}_2 sonlu cismi üzerinde karşılığı olan 16×16 ikili matris Eşitlik (9.6)'da verilmiştir.

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \\ y_4 \\ y_5 \\ y_6 \\ y_7 \\ y_8 \\ y_9 \\ y_{10} \\ y_{11} \\ y_{12} \\ y_{13} \\ y_{14} \\ y_{15} \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \\ x_8 \\ x_9 \\ x_{10} \\ x_{11} \\ x_{12} \\ x_{13} \\ x_{14} \\ x_{15} \end{bmatrix} \tag{9.6}$$

A matrisinin Eşitlik (9.6)'da verilen giriş $(x_0, x_1, \dots, x_{15})$ ve çıkış $(y_0, y_1, \dots, y_{15})$ haritalaması, cebirsel olarak Eşitlik (9.7)'deki gibi ifade edilebilir;

$$\begin{aligned}
 y_0 &= x_0 \oplus x_3 \oplus x_7 \oplus x_8 \oplus x_{12} \oplus x_{15} \\
 y_1 &= x_0 \oplus x_1 \oplus x_3 \oplus x_4 \oplus x_7 \oplus x_9 \oplus x_{12} \oplus x_{13} \oplus x_{15} \\
 y_2 &= x_1 \oplus x_2 \oplus x_5 \oplus x_{10} \oplus x_{13} \oplus x_{14} \\
 y_3 &= x_2 \oplus x_3 \oplus x_6 \oplus x_{11} \oplus x_{14} \oplus x_{15} \\
 y_4 &= x_1 \oplus x_4 \oplus x_5 \oplus x_{11} \oplus x_{15} \\
 y_5 &= x_1 \oplus x_2 \oplus x_6 \oplus x_8 \oplus x_{11} \oplus x_{12} \oplus x_{15} \\
 y_6 &= x_2 \oplus x_3 \oplus x_7 \oplus x_9 \oplus x_{13} \\
 y_7 &= x_0 \oplus x_3 \oplus x_4 \oplus x_{10} \oplus x_{14} \\
 y_8 &= x_0 \oplus x_1 \oplus x_5 \oplus x_8 \oplus x_{11} \oplus x_{15} \\
 y_9 &= x_2 \oplus x_5 \oplus x_6 \oplus x_8 \oplus x_9 \oplus x_{11} \oplus x_{12} \oplus x_{15} \\
 y_{10} &= x_3 \oplus x_6 \oplus x_7 \oplus x_9 \oplus x_{10} \oplus x_{13} \\
 y_{11} &= x_0 \oplus x_4 \oplus x_7 \oplus x_{10} \oplus x_{11} \oplus x_{14} \\
 y_{12} &= x_3 \oplus x_7 \oplus x_8 \oplus x_{11} \oplus x_{12} \\
 y_{13} &= x_0 \oplus x_3 \oplus x_4 \oplus x_7 \oplus x_8 \oplus x_9 \oplus x_{11} \oplus x_{13} \\
 y_{14} &= x_1 \oplus x_5 \oplus x_9 \oplus x_{10} \oplus x_{14} \\
 y_{15} &= x_2 \oplus x_6 \oplus x_{10} \oplus x_{11} \oplus x_{15}
 \end{aligned} \tag{9.7}$$

Tanım 9.12. (Derinlik): Devreyi oluşturan en uzun yoluun uzunluğu olarak tanımlanabilir.

Bir yayılım matrisinde, devre derinliğinin minimum derinlikte olması ve bu devrenin minimum XOR sayısıyla gerçekleşmesi amaçlanır [24]. Bir devre farklı derinliklerle tasarlanabilir, literatürde yayılım tabakalarının devre derinliği optimizasyonu çalışılan açık problemlerden biridir [3].

Örnek 9.13: $v_1 = x_1 \oplus x_2 \oplus x_3 \oplus x_4$, $v_2 = x_5$, $v_3 = x_6 \oplus x_7 \oplus x_8 \oplus x_9$ olmak üzere $v_1 \oplus v_2 \oplus v_3$ toplam devresi farklı derinliklerde tasarlanabilir. Şekil 9.1 ve Şekil 9.2'de $v_1 \oplus v_2 \oplus v_3$ toplam devresinin farklı tasarımları verilmiştir. Şekiller üzerinde verilen kesik çizgiler "1 devre derinliğini" temsil etmektedir. Şekil 9.1 ve Şekil 9.2'de verilen toplam devreleri ve bu devreleri oluşturan alt devreler (ara değerler) ele alındığında v_1 alt devresinin derinliği; her iki tasarım için de 2'dir. v_2 alt devresinin derinliği her iki devre tasarımda da aynı olmak üzere 0'dır. Çünkü v_2 çıkış değeri x_5 giriş değerine eşit olup, v_2

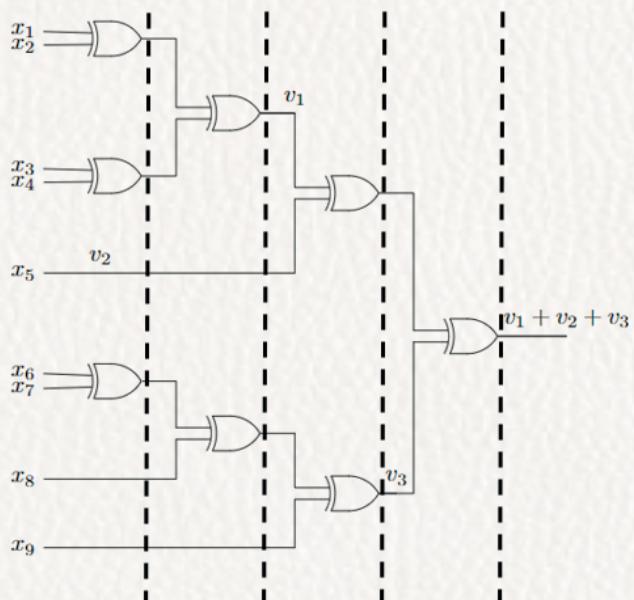
alt devresini oluşturmak için herhangi bir XOR kapısı kullanılmamıştır. v_3 alt devresinin derinliği her iki devre tasarımında da 3'tür. Ancak $v_1 \oplus v_2 \oplus v_3$ toplam devresinin derinlik değerleri ele alındığında;

$$v_1 \oplus v_2 \oplus v_3 = \left(\underbrace{(x_1 \oplus x_2) \oplus (x_3 \oplus x_4)}_{v_1} \right) \oplus \underbrace{x_5}_{v_2} \oplus \left(\underbrace{(x_6 \oplus x_7) \oplus x_8}_{v_3} \right) \oplus x_9 \quad \text{olarak}$$

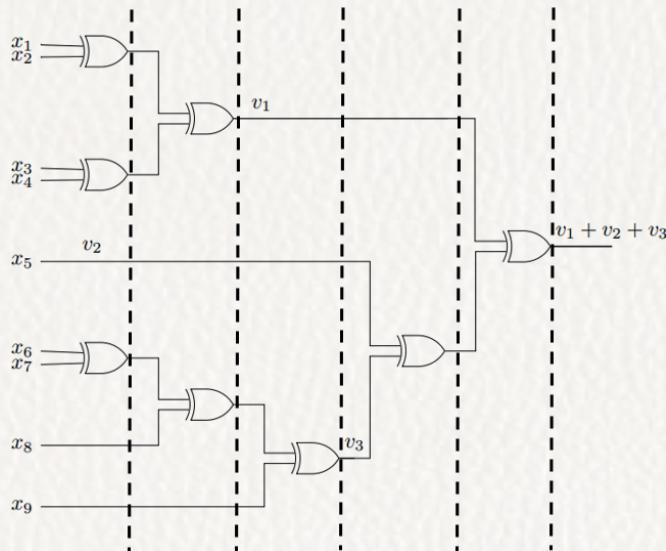
tasarlanan ve Şekil 9.1'de verilen $v_1 \oplus v_2 \oplus v_3$ toplam devresinin derinliği 4'tür.

$$v_1 \oplus v_2 \oplus v_3 = \left(\underbrace{(x_1 \oplus x_2) \oplus (x_3 \oplus x_4)}_{v_1} \right) \oplus \underbrace{x_5}_{v_2} \oplus \left(\underbrace{\left(\underbrace{(x_6 \oplus x_7) \oplus x_8}_{v_3} \right) \oplus x_9}_{v_4} \right) \quad \text{olarak}$$

tasarlanan ve Şekil 9.2'de verilen $v_1 \oplus v_2 \oplus v_3$ toplam devresinin derinliği ise 5'tir.



Şekil 9.1. $(v_1 + v_2 + v_3)$ Devresinin 4 Derinlikli Tasarlanması



Şekil 9.2. $(v_1 + v_2 + v_3)$ Devresinin 5 Derinlikli Tasarlanması

Blok şifrelerde kullanılan yayılım matrisleri farklı devre tasarımları ile tasarlanabilir. En iyi devre tasarıının bulunması; devre derinliğinin azaltılmasıının yanı sıra, matris devresinin giriş ve çıkış haritalamasının cebirsel ifadesini de değiştirir. Böylece cebirsel ifadenin daha az sayıda XOR sayısıyla ifade edilmesine imkân sağlar. Literatürde (tersi kendisine eşit) MDS matrislerin minimum derinlikte ve minimum XOR sayısıyla gerçekleşen devrelerle tasarlanması için, faklı optimizasyon yöntemleri önerilmiştir. Bölüm 9.4’te bu optimizasyon yöntemleri detaylarıyla verilmiştir.

Minimum XOR sayısı ve derinlik parametreleri ile düşük maliyetli (tersi kendisine eşit) MDS matrislerin tasarlanması hafif sıklet kriptosistemlerin yayılım tabakaları için son derece önemlidir. Bu nedenle Bölüm 9.3’te MDS matrisler için farklı tasarım yöntemleri ayrıntılı olarak ele alınmıştır.

9.3. (TERSİ KENDİSİNÉ EŞİT) MDS MATRİS TASARIM YÖNTEMLERİ

MDS matrisler diğer yayılım tabakalarına oranla maliyetlidir ancak en iyi yayılımı sağlarlar. Bu nedenle düşük maliyet ve düşük gecikmeli (tersi kendisine eşit) MDS matrislerin tasarıımı önemli bir çalışma problemidir [29].

(Tersi kendisine eşit) MDS matrislerin tasarımları için iki temel tasarım yöntemi vardır; özyinelemeli (recursive) ve özyinelemeli–olmayan (non– recursive). Özyinelemeli tasarım yöntemleri seri–tabanlı (serial-based) uygulamalar olarak adlandırılırken, özyinelemeli–olmayan tasarım yöntemleri ise döngü–tabanlı (round–based) uygulamalar olarak adlandırılır. Özyinelemeli yapılarda matrisin k . kuvveti MDS matrisken, özyinelemeli–olmayan yapılarda ise matrisin kendisi MDS matristir [26].

Bunun yanında bir diğer (tersi kendisine eşit) MDS tasarım sınıflandırması ise; doğrudan tasarım (direct construction), arama (searching) ve hibrit (hybrid) yöntemlerle tasarım şeklinde yapılabilir. Bu sınıflandırma temelde bir matris formunun doğrudan MDS matris üretip üretmediği üzerine kurulmuştur [25], [26].

Tasarım yöntemleri aşağıda verilen alt başlıklarda kapsamlı olarak detaylandırmıştır.

9.3.1. (Tersi Kendisine Eşit) MDS Matrisler için Özyinelemeli ve Özyinelemeli – Olmayan Tasarım Yöntemleri

Özyinelemeli yapılarda (tersi kendisine eşit) MDS matris, A seri matrisinin (genellikle Companion matrisle [26] başlar) k . kuvveti A^k olarak hesaplanır. A^k MDS matrisinin kendisinin devre uygulaması yerine, A matrisinin devresi k kez uygulanır. Yayılma özelliği MDS matris koşulundan dolayı maksimum kalırken, donanım maliyeti düşük kalır çünkü A matrisinin devresinin k kez uygulanması devre maliyetini çok artırmaz [30].

Tanım 9.14. (Seri Matris): $z_0, \dots, z_{d-1} \in \mathbb{F}_{2^m}$ olmak üzere $d \times d$ boyutlu $Seri(z_0, \dots, z_{d-1})$ gösterimiyle seri matrisi Eşitlik (9.8)'deki gibidir;

$$Seri(z_0, \dots, z_{d-1}) = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ z_0 & z_1 & \dots & \dots & \dots & z_{d-1} \end{bmatrix} \quad (9.8)$$

Böylece $Seri(z_0, \dots, z_{d-1})^k$ matris formundan MDS matrisler üretilir.

Tanım 9.15. (Companion Matris):

$g(x) = a_0 + a_1x + a_2x^2 + \dots + a_{d-1}x^{k-1} + x^k \in \mathbb{F}_q[x]$ $k.$ dereceden monik polinom (en yüksek dereceli terimin (x^k) katsayısı 1 olan polinom) olmak üzere, Companion matris C_g Eşitlik (9.9)'daki gibidir;

$$C_g = \begin{bmatrix} 0 & 1 & 0 & 0 & \dots & 0 \\ 0 & 0 & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \\ -a_0 & -a_1 & \dots & \dots & \dots & -a_{k-1} \end{bmatrix} \quad (9.9)$$

ve $\text{Companion}(-a_0, -a_1, \dots, -a_{k-1})$ gösterimi ile ifade edilir.

Eşitlik (9.8)'de verilen $Seri(z_0, \dots, z_{d-1})$ matrisi aynı zamanda $z_0 + z_1x + z_2x^2 + \dots + z_{d-1}x^{d-1} + x^d$ polinomuna göre Companion matristir.

Özyinelemeli MDS matris tasarım yöntemlerinde seri matrislerin önemi açık-tır. Bu nedenle literatürde daha düşük maliyetli seri matrislerin tasarımını için farklı formlar önerilmiştir. LFS (Linear Feedback Serial – Doğrusal Geribes-lemeli Seri) matris formu [32] ve DSI (Diagonal – Serial Invertible – Diago-nal Seri Tersi Alınabilir) matris formu [31] bu formlardan ikisidir. Bu matris formlarına ait tanımlar aşağıda verilmiştir.

Tanım 9.16. (LFS Matris): $L = LFS(z_0, z_1, \dots, z_{k-1})$ matrisinin elemanları aña-ğidakı gibi ifade edilir;

$$L_{ij} = \begin{cases} z_j, & i=k-1 \\ 1, & i+1=j \\ 0, & \text{diğer durumlarda} \end{cases} \quad (9.10)$$

L matrisinin tersi L^{-1} matrisi aşağıdaki gibi ifade edilir;

$$L_{ij}^{-1} = \begin{cases} \frac{z_j + 1}{z_0}, & i=0, z_k=1 \\ 1, & i=j+1 \\ 0, & \text{diğer durumlarda} \end{cases} \quad (9.11)$$

Eşitlik (9.11)'deki ifade için eğer $z_0 = 1$ ise, LFS matrisin kendisi ve tersi aynı $z_1, z_2 \dots, z_{k-1}$ sonlu cisim elemanlarına sahip olur. Diğer bir ifadeyle; her iki matris için gerekli donanım kaynağı birbirine eşittir [32]. Bunun yanında [31]'de verilen çalışmada $z_0 \neq 1$ olduğu durumlarda, kendisi ve tersi aynı donanım kaynaklarına sahip olan matrislerin varlığı ispatlanmıştır.

Tanım 9.17. (DSI Matris): $k \times k$ boyutlu $D = DSI(D_{ij})_{1 \leq i,j \leq k} \in \mathbb{F}_{2^n}$ matrisi $a = (a_i)_{1 \leq i \leq k} \in \mathbb{F}_{2^n}, a_i \neq 0$ ve $b = (b_i)_{1 \leq i \leq k-1} \in \mathbb{F}_{2^n}$ vektörleri tarafından belirlenir ve aşağıdaki gibi ifade edilir;

$$D_{ij} = \begin{cases} a_1, & i=1, j=k \\ a_i, & i=j+1 \\ b_i, & i=j \leq k-1 \\ 0, & \text{diğer durumlarda} \end{cases} \quad (9.12)$$

Örnek 9.18: 6×6 boyutlu $D_1 = DSI(a, b)$ matrisi aşağıdaki gibi ifade edilir;

$$D_1 = \begin{bmatrix} b_1 & 0 & 0 & 0 & 0 & a_1 \\ a_2 & b_2 & 0 & 0 & 0 & 0 \\ 0 & a_3 & b_3 & 0 & 0 & 0 \\ 0 & 0 & a_4 & b_4 & 0 & 0 \\ 0 & 0 & 0 & a_5 & b_5 & 0 \\ 0 & 0 & 0 & 0 & a_6 & 0 \end{bmatrix} \quad (9.13)$$

DSI matris formu $LFS(z_0, z_1, \dots, z_{k-1})$ matris yapısından esinlenerek tasarlanmıştır. Tasarımdaki amaç; permütasyon matrisinin yapısı korunarak, satırların ikili doğrusal kombinasyonları ile daha yüksek yayılım sağlamaktır. DSI matrislerin cebirsel özellikleriyle ilgili kapsamlı bilgiye [31]'den erişilebilir.

Özyinelemeli yapılarda, DSI matrislerin kullanımı daha yüksek boyutlu matrisler için iyi sonuçlar elde edilmesini sağlasa da, DSI matrisler yerine Companion matrislerin kullanılması Companion matrislerin güçlü matematiksel teorisi nedeniyle kaçınılmazdır. Ancak arama yöntemiyle bulunabilecek küçük boyutlu matrisler için donanım maliyeti açısından kıyaslandığında; DSI matrisler Companion matrlislere göre daha düşük maliyetli devreye sahip matrislerin üretilmesine imkân sağlar [26].

Özyinelemeli – olmayan yapılarda matrisin kendisi MDS matristir, seri matrislerdeki gibi matrisin k . kuvveti uygulanmaz. Cauchy ve Vandermonde matris formları bu yapıların üretilemesini sağlar, çünkü bu matris formları kanıtlanabilir MDS olma avantajına sahiptirler [33]. Bu matris formları Eşitlik (9.14) ve Eşitlik (9.15)'te verilmiştir.

Tanım 9.19. (Cauchy Matris): $k \times k$ boyutlu, $\{\alpha_0, \alpha_1, \dots, \alpha_{k-1}\} \in \mathbb{F}_{2^n}$ ve $\{\beta_0, \beta_1, \dots, \beta_{k-1}\} \in \mathbb{F}_{2^n}$ iki ayrık set, tüm $0 \leq i, j \leq n-1$ için $\alpha_i + \beta_j \neq 0$ olmak üzere, $C[i, j] = \frac{1}{\alpha_i + \beta_j}$ Cauchy matrisi aşağıdaki gibi ifade edilir;

$$C = \begin{bmatrix} \frac{1}{\alpha_0 + \beta_0} & \frac{1}{\alpha_0 + \beta_1} & \dots & \frac{1}{\alpha_0 + \beta_{k-1}} \\ \frac{1}{\alpha_1 + \beta_0} & \frac{1}{\alpha_1 + \beta_1} & \dots & \frac{1}{\alpha_1 + \beta_{k-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{1}{\alpha_{k-1} + \beta_0} & \frac{1}{\alpha_{k-1} + \beta_1} & \dots & \frac{1}{\alpha_{k-1} + \beta_{k-1}} \end{bmatrix} \quad (9.14)$$

Cauchy matrisler ile elde edilen katsayılar çok karmaşıktır, bu da donanım – verimli MDS matrislerin tasarılanmasına engeldir [34].

Tanım 9.20. (Vandermonde Matris): $n \times n$ boyutlu, $A = vand(a_0, a_1, \dots, a_{n-1})$ Vandermonde matrisi aşağıdaki gibi ifade edilir;

$$A = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_0^2 & a_1^2 & a_2^2 & \dots & a_{n-1}^2 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ a_0^{n-1} & a_1^{n-1} & a_2^{n-1} & \dots & a_{n-1}^{n-1} \end{bmatrix} \quad (9.15)$$

Özyinelemeli ve özyinelemeli – olmayan yöntemler karşılaştırıldığında; özyinelemeli yapılar daha az donanım alanı gereksinimi için daha fazla saat vuruşuna (clock cycle) ihtiyaç duyar. Özyinelemeli – olmayan uygulamalarda

bir saat vuruşunda, $k \times k$ boyutu için yayılım matrisinin tümü hesaplanır ve uygulanır. Bu nedenle matrisin k^2 elemanın da olabildiğince düşük maliyetli (XOR sayılı) olması istenir. Özyinelemeli uygulamalarda seri matrisin önemsiz olmayan ($\neq 0$) satırı hesaplanır ve bu işlem k defa özyinelemeli olarak tekrarlanır. Bu nedenle hesaplama zamanı bir dizi k saat vuruşu alır.

9.3.2. (Tersi Kendisine Eşit) MDS Matrisler İçin Doğrudan Tasarım, Arama ve Hibrit Tasarım Yöntemleri

Doğrudan tasarım yöntemi, özel kodlar ve özel matris formları kullanılarak, üretilen matrisin doğrudan MDS matris olduğu yapılardır. Gabidulin [35] ve BCH [36] kodları cebirsel özelliklerini sayesinde direkt olarak MDS matrislerin üretilmesini sağlar. Cauchy, Vandermonde ve Companion özel matris formlarının kullanılması ile de doğrudan MDS matrisler tasarlabilir. Cauchy ve Vandermonde matris formları kullanılarak üretilen MDS matrisler donanım – verimli değildir, bu nedenle arama yöntemiyle üretilen MDS matrisler daha verimli uygulamalara sahiptir [26].

Arama yönteminde, rastgele üretim ve bazı özel matris formları kullanılarak bir matrisin MDS olup olmadığı kontrol edilir. Rastgele üretimde matrisin elemanları sonlu cisim üzerinden seçilerek, bu matrisin tüm alt kare matrislerinin tekil olmayan matris olup olmadığını kontrol edilmesi ve doğrulanması gereklidir, böylece (tersi kendisine eşit) MDS matrislerin elde edilmesi sağlanır. Ancak aranacak uzay çok büyük olduğu için rastgele üretim yöntemi verimli bir yöntem değildir. Bu nedenle (tersi kendisine eşit) MDS matrislerin bulunması için; arama uzayı bazı özel matris formlarının kullanılmasıyla kücültülür. Cebirsel özellikleri sayesinde (tersi kendisine eşit) MDS matrislerin üretilmesini sağlayan bu özel matris formları aşağıdaki tanımlarda verilmiştir.

Tanım 9.21. (Dairesel Matris): $n \times n$ boyutlu, $A = Circ(a_0, a_1, \dots, a_{n-1})$ Dairesel (Circulant) matrisi aşağıdaki gibi ifade edilir;

$$A = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \dots & a_{n-3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix} \quad (9.16)$$

Dairesel matrislerin yayılım tabakalarında kullanılmasının önemli avantajları vardır [26];

- Dairesel matris formuyla MDS matrislerin bulunma olasılığı, rastgele üretim yöntemiyle kıyaslandığında yüksektir,
- $n \times n$ boyutlu Cauchy ve Hadamard matris formundaki matrislerin MDS matris olabilmeleri için; en az n farklı elemana sahip olmaları gereklidir, Dairesel matris formunda ise en çok n farklı eleman kullanılır. Bu da daha düşük donanım maliyetli MDS matrislerin üretilmesini sağlar,
- Dairesel matris formu özyinelemeli ve özyinelemeli – olmayan MDS matris tasarımlarının ikisinde de kullanılır.
- Dairesel matrisler avantajlarının yanı sıra bazı dezavantajlara da sahiptir [37];
- Dairesel MDS matrisler ile tersi kendisine eşit MDS matrisler üretilemez,
- $2^n \times 2^n$ Dairesel MDS matrisler ortogonal değildir.

Bu nedenle tersi kendisine eşit MDS matrislerin bulunması için sol – Dairesel matris formu önerilmiştir. Bu formda, her satır vektörü bir önceki satır vektörünün bir eleman dairesel sola kaydırılmasıyla elde edilir.

Tanım 9.22. (sol – Dairesel Matris): $n \times n$ boyutlu, $B = l - Circ(a_0, a_1, \dots, a_{n-1})$ sol – Dairesel (left–Circulant) matrisi aşağıdaki gibi ifade edilir;

$$B = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_1 & a_2 & a_3 & \dots & a_0 \\ a_2 & a_3 & a_4 & \dots & a_1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \end{bmatrix} \quad (9.17)$$

Daha verimli MDS matrislerin tasarımları için Dairesel – benzeri (Circulant-like) matris formu [38] önerilmiştir. [37]'de verilen çalışmada Dairesel–benzeri matris formu ele alınarak, Tip-I Dairesel–benzeri (Type-I Circulant-like) ve Tip-II Dairesel – benzeri (Type-II Circulant-like) matris formları önerilmiştir.

Tanım 9.23. (Tip – I Dairesel – benzeri Matris): $A = \text{Circ}(1, a_1, \dots, a_{n-2})$, $\mathbf{1} = \underbrace{(1, 1, \dots, 1)}_{n-1 \text{ tan e}}$ ve $\mathbf{1}$ birim eleman, $a \neq 0, a_i \neq 0, i = \{1, 2, \dots, (n-2)\}$ olmak üzere, $n \times n$ boyutlu, Tip – I Dairesel – benzeri matris $T_1 = \text{TypeI}(a, \text{Circ}(1, a_1, \dots, a_{n-2}))$ aşağıdaki gibi ifade edilir;

$$T_1 = \begin{bmatrix} a & \mathbf{1} \\ \mathbf{1}^T & A \end{bmatrix} \quad (9.18)$$

Tip-I Dairesel-benzeri matris formunun tersi neredeyse kendisine eşittir, bu form Neredeyse Tip–I Dairesel–benzeri (Almost Type–I Circulant–like) olarak adlandırılmış olup matris formu Eşitlik (9.19)'da verilmiştir.

Tanım 9.24. (Neredeyse Tip – I Dairesel – benzeri Matris): $A = \text{Circ}(a_0, \dots, a_{n-2})$, $\mathbf{b} = \underbrace{(b, b, \dots, b)}_{n-1 \text{ tan e}}$, $a, b \neq 0, a_i \neq 0, i = \{0, 1, \dots, (n-2)\}$ olmak üzere, $n \times n$ boyutlu, Neredeyse Tip–I Dairesel–benzeri matris $T_2 = \text{AlmostTypeI}(a, b, \text{Circ}(a_0, \dots, a_{n-2}))$ aşağıdaki gibi ifade edilir;

$$T_2 = \begin{bmatrix} a & \mathbf{b} \\ \mathbf{b}^T & A \end{bmatrix} \quad (9.19)$$

Tip–I Dairesel–benzeri matris formu çift boyutlarda tersi kendisine eşit MDS veya ortogonal MDS matrisler üretmez, bu nedenle Tip–II Dairesel–benzeri matris formu önerilmiştir.

Tanım 9.25. (Tip–II Dairesel–benzeri Matris): $A = \text{Circ}(a_0, \dots, a_{n-1})$ olmak üzere, $2n \times 2n$ boyutlu Tip–II Dairesel–benzeri matris $T_3 = \text{TypeII}(\text{Circ}(a_0, \dots, a_{n-1}))$ aşağıdaki gibi ifade edilir;

$$T_3 = \begin{bmatrix} A & A^{-1} \\ A^3 + A & A \end{bmatrix} \quad (9.20)$$

n tek sayı olmak üzere $2n \times 2n$ boyutlu Tip–II Dairesel–benzeri matris formu tersi kendisine eşit MDS matrislerin üretilmesini sağlar [37].

Tanım 9.26. (Toeplitz Matris): $n \times n$ boyutlu Toeplitz matris $T_4 = \text{Toep}(a_0, a_1, \dots, a_{n-1}; a_{-1}, a_{-2}, \dots, a_{-(n-1)})$ aşağıdaki gibi ifade edilir;

$$T_4 = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-2} & a_{n-1} \\ a_{-1} & a_0 & a_1 & \dots & a_{n-3} & a_{n-2} \\ a_{-2} & a_{-1} & a_0 & \dots & a_{n-4} & a_{n-3} \\ a_{-3} & a_{-2} & a_{-1} & \dots & a_{n-5} & a_{n-4} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{-(n-1)} & a_{-(n-2)} & a_{-(n-3)} & \dots & a_{-1} & a_0 \end{bmatrix} \quad (9.21)$$

Dairesel matrisler Toeplitz matrislerin özel bir formudur. Toeplitz matris formunda; soldan sağa azalan köşegen üzerindeki elemanlar sabittir. Toeplitz matris formunun gösterimi; matrisin birinci satır ve birinci sütün elemanları yan yana yazılarak ifade edilir;

$$\text{Toep}(\underbrace{a_0, a_1, \dots, a_{n-1}}_{\text{birinci satır elemanları}}; \underbrace{a_{-1}, a_{-2}, \dots, a_{-(n-1)}}_{\text{birinci sütun elemanları}}).$$

Elemanları \mathbb{F}_{2^n} üzerinde tanımlı, $k \geq 3$ olmak üzere $k \times k$ boyutlu bir Toeplitz MDS matrisin tersi kendisine eşit olamaz. Ayrıca $k \geq 2$ olmak üzere $2^k \times 2^k$ boyutlu Toeplitz matris ortogonal ise, bu matris MDS matris olamaz [26].

Tanım 9.27. (Hankel Matris): $n \times n$ boyutlu Hankel matris $H = \text{Hank}(a_0, a_1, \dots, a_{n-1}; a_n, a_{n+1}, \dots, a_{2n-2})$ aşağıdaki gibi ifade edilir;

$$H = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-2} & a_{n-1} \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n \\ a_2 & a_3 & a_4 & \dots & a_n & a_{n+1} \\ a_3 & a_4 & a_5 & \dots & a_{n+1} & a_{n+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{n-1} & a_n & a_{n+1} & \dots & a_{2n-3} & a_{2n-2} \end{bmatrix} \quad (9.22)$$

Hankel matris, Toeplitz matris formunun satır permütasyonu uygulanmış hâlidir. Aynı zamanda sol – Dairesel matris formunun özel bir durumudur. Hankel matris cebirsel olarak Toeplitz matrisin özelliklerini gösterir. Şöyledi ki; elemanları \mathbb{F}_{2^n} üzerinde tanımlı, $k \geq 3$ olmak üzere $k \times k$ boyutlu bir Hankel MDS matrisin tersi kendisine eşit olamaz. Ayrıca, $k \geq 2$ olmak üzere $2^k \times 2^k$ boyutlu Hankel matris ortogonal ise, bu matris MDS matris olamaz [26].

Tanım 9.28. (Hadamard Matris): Elemanları \mathbb{F}_{2^n} üzerinde tanımlı, $2^k \times 2^k$ boyutlu sonlu cisim Hadamard (finite field Hadamard – kısaca Hadamard) matris H aşağıdaki gibi ifade edilir;

$$H = \begin{bmatrix} U & V \\ V & U \end{bmatrix} \quad (9.23)$$

U ve V alt matrisleri de Hadamard matristir. 4×4 boyutlu $H_1 = \text{Had}(a_0, a_1, a_2, a_3)$ Hadamard matrisi Eşitlik (9.24)'te verilmiştir.

$$H_1 = \begin{bmatrix} a_0 & a_1 & a_2 & a_3 \\ a_1 & a_0 & a_3 & a_2 \\ a_2 & a_3 & a_0 & a_1 \\ a_3 & a_2 & a_1 & a_0 \end{bmatrix} \quad (9.24)$$

Bir Hadamard matrisin eğer ilk satırındaki elemanların toplamı 1'e eşitse bu matrisin tersi kendisine eşittir [39]. Elemanları \mathbb{F}_{2^m} üzerinde tanımlı $k \times k$ boyutlu Hadamard matrlslere ait önemli özellikler aşağıda verilmiştir [40];

- $k \times k$ boyutlu H Hadamard matrisinin, a_i ilk satır elemanlarını temsil etmek üzere, $H_{i,j} = a_{i \oplus j}$ 'dir.
- $k \times k$ boyutlu H Hadamard matrisi bi-simetrik matristir. Şöyled ki; $H = H^T$ ve $HJ = JH$ (J matrisi $k \times k$ boyutlu dönüşüm (exchange) matrisi olmak üzere, yani $J_{i,k-i+1} = 1$, diğer elemanları ise 0'dır).
- $c = \bigoplus_{i=0}^{k-1} a_i$ ve I $k \times k$ boyutlu birim matris olmak üzere, $H^2 = c^2 I$ koşulunu sağlar.

Hadamard matrisler, iki Vandermonde matris kullanılarak üretilenbildiği gibi [41], Cauchy matrisler kullanılarak da üretilebilir ve bu matris formu Hadamard-Cauchy olarak adlandırılır [23].

MDS matrislerin üretilmesi için birçok farklı özel matris formundan yararlanılırken, tersi kendisine eşit MDS matrislerin üretilmesi için bilinen yöntemler; rastgele üretim yöntemi, Hadamard matris formu, Tip-II Dairesel-benzeri matris formudur. Bu nedenle özellikle tersi kendisine eşit MDS matrislerin üretilmesi için hibrit üretim yöntemi önerilmiştir.

Hibrit üretim yöntemi GHadamard (Generalized Hadamard – Genelleştirilmiş Hadamard) [40] matris formunun önerilmesiyle ortaya çıkmıştır. Hibrit yönteme, (tersi kendisine eşit) MDS matrislerin arama maliyetini düşürmek için doğrudan üretim ve arama yöntemleri birleştirilmiştir. Hibrit yapı, temeline özel matris formlarını alır ve bu özel matris formları kullanılarak yeni (tersi kendisine eşit) MDS matrisler arama maliyeti olmadan doğrudan üretilir. Arama yöntemi doğrudan üretilen (tersi kendisine eşit) MDS matrisler içinden minimum XOR sayılı matrislerin bulunması için kullanılır. GHadamard matris formu, tersi kendisine eşit MDS matrislerin üretilmesini sağlayan kısıtlı üretim yöntemlerinden biridir.

Tanım 9.29. (GHadamard Matris): Elemanları \mathbb{F}_{2^m} üzerinde tanımlı, 2×2 boyutlu $H = Had(a_0, a_1)$ Hadamard matrisi, $b_1 \neq 0, b_1 \in \mathbb{F}_{2^n}$ olmak üzere, 2×2 boyutlu $GH = Ghad(a_0, a_1; b_1)$ GHadamard matrisi aşağıdaki gibi ifade edilir;

$$GH = \begin{bmatrix} a_0 & a_1 b_1 \\ a_1 b_1^{-1} & a_0 \end{bmatrix} \quad (9.25)$$

4×4 boyutlu $GH_1 = Ghad(a_0, a_1; b_1, a_2; b_2, a_3; b_3)$ GHadamard matrisi Eşitlik (9.26)'da verilmiştir.

$$GH_1 = \begin{bmatrix} a_0 & a_1 b_1 & a_2 b_2 & a_3 b_3 \\ a_1 b_1^{-1} & a_0 & a_3 b_1^{-1} b_2 & a_2 b_1^{-1} b_3 \\ a_2 b_2^{-1} & a_3 b_2^{-1} b_1 & a_0 & a_1 b_2^{-1} b_3 \\ a_3 b_3^{-1} & a_2 b_3^{-1} b_1 & a_1 b_3^{-1} b_2 & a_0 \end{bmatrix} \quad (9.26)$$

GHadamard matris formu; verilen Hadamard tersi kendisine eşit MDS matrisinden yeni tersi kendisine eşit MDS matrislerin doğrudan üretilmesini sağlarken, Hadamard MDS matrislerden de yeni Hadamard MDS matrisler üretir. GHadamard matris formu tek veya çift herhangi bir boyuta uygulanabilir, bu da Tip – II Dairesel – benzeri matris formundaki gibi kısıtlamaya sebep olmaz.

Tanım 9.30. Elemanları \mathbb{F}_{2^m} üzerinde tanımlı $A = \begin{bmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{bmatrix}$ mat-

risi eğer tersi kendisine eşitse, A matrisi a_{11}, a_{22} elemanları ile ifa-

de edilebilir, şöyle ki $a_{11} \neq a_{22} \neq a_{33}$ ve $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$ olmak üzere $a_{12} = (a_{11} + 1)b_0$, $a_{13} = (a_{11} + 1)b_1$, $a_{21} = (a_{22} + 1)b_0^{-1}$, $a_{23} = (a_{22} + 1)b_0^{-1}b_1$, $a_{31} = (a_{11} + a_{22})b_1^{-1}$, $a_{32} = (a_{11} + a_{22})b_1^{-1}b_0$, $a_{33} = a_{11} + a_{22} + 1$ olur. Buradan 3×3 boyutlu tersi kendisine eşit matris formu $(IM)_{3 \times 3}$ aşağıdaki gibi ifade edilir;

$$(IM)_{3 \times 3} = \begin{bmatrix} a_{11} & (a_{11} + 1)b_0 & (a_{11} + 1)b_1 \\ (a_{22} + 1)b_0^{-1} & a_{22} & (a_{22} + 1)b_0^{-1}b_1 \\ (a_{11} + a_{22})b_1^{-1} & (a_{11} + a_{22})b_1^{-1}b_0 & a_{11} + a_{22} + 1 \end{bmatrix} \quad (9.27)$$

Eşitlik (9.27)'de verilen $(IM)_{3 \times 3}$ matris formu üzerinde $a_{11} \neq a_{22}$, $a_{11}, a_{22} \neq 0$, $a_{11}, a_{22} \neq 1$, $a_{11} + a_{22} \neq 1$ ve $b_0, b_1 \in \mathbb{F}_{2^m} - \{0\}$ kısıtları altında, bu matris formu ile \mathbb{F}_{2^m} üzerinde 3×3 boyutlu tersi kendisine eşit MDS matrislerin tamamı üretilebilir [54].

(Tersi kendisine eşit) MDS matrisler farklı üretim yöntemleriyle tasarlanırken bir taraftan da minimum XOR sayılı ve minimum derinlikli matrislerin bulunması için optimizasyon yöntemleri önerilmiştir. Bölüm 9.4'te bu yöntemler verilmiştir.

9.4. (TERSİ KENDİSİNÉ EŞİT) MDS MATRİSLER İÇİN YEREL VE GENEL OPTİMİZASYON YÖNTEMLERİ

Bir blok şifrenin yayılım tabakasında kullanılmak üzere (tersi kendisine eşit) MDS matrisler tasarlanırken bu matrisin özellikle donanım maliyetinin minimum olması beklenir ve bunun için farklı optimizasyon yöntemleri önerilmiştir. Bu yöntemler temelde; yerel optimizasyon (local optimization) ve genel

optimizasyon (global optimization) olarak ikiye ayrılır. Şekil 9.3'te yerel (a) ve genel (b) optimizasyon yöntemleri arasındaki fark bir yayılım matrisi üzerinde gösterilmiştir. Yerel optimizasyon yöntemlerinde; matrisin elemanlarına ayrı ayrı odaklanılarak bu elemanların minimum XOR sayılı elemanlardan seçilmesi hedeflenir. Genel optimizasyon (global optimization) yöntemlerinde ise matrisin tamamına odaklanılarak tüm yayılım matrisinin XOR sayısı optimize edilir.

$$\text{a)} \quad \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{bmatrix} \quad \text{b)} \quad \begin{bmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{bmatrix}$$

Şekil 9.3. a) Yerel Optimizasyon b) Genel Optimizasyon

Literatürde yer alan yerel ve genel optimizasyon yöntemleri aşağıdaki alt başlıklarda kapsamlı olarak verilmiştir.

9.4.1. (Tersi Kendisine Eşit) MDS Matrisler için Yerel Optimizasyon Yöntemleri

Özyinelemeli yapılarla üretilen MDS matrislerin yerel optimizasyonu ele alındığında, bu yöntemler en genel ifadeyle özyinelemeli seri matristen üretilen MDS matrislerin elemanlarına odaklanarak verimli matrislerin üretilmesini hedefler. “Yayılım matrislerinin donanım uygulamalarında devre alanının azaltılması” fikri, 2007 yılında PRESENT şifreleme algoritmasının yayılım tabakasında özyinelemeli matrislerin kullanımıyla ortaya atılmıştır. Şifreleme algoritmalarının yayılım tabakalarında özyinelemeli seri matrislerin uygulanması fikri yeni bir araştırma alanını açmıştır. 2011 yılında LED blok şifreleme algoritması ve PHOTON hash fonksiyonunun [42] yayılım tabakalarında da seri matrislerle oluşturulan MDS matrisler kullanılmıştır. Sonraki yıllarda yapılan çalışmalarda “verimli MDS matrislerin oluşturulabilmesi için, seri mat-

risin elemanları nasıl seçilmelidir” sorusu üzerine yoğunlaşılmıştır. 2012 yılında yapılan çalışmada [41], farklı matris boyutları için farklı formlara sahip yayılım matrisleriyle en iyi yayılmanın sağlanabilmesi için, daha az sayıda doğrusal fonksiyonun kullanılması fikri önerilmiştir. 2013 yılında yapılan çalışmada [43], en iyi yayılım tabakalarının üretilmesi için iterasyon sayısı artırılarak bit-seviyeli LFSR’lerin (Linear Feedback Serial Register–Doğrusal Geri-beslemeli Seri Yazmaç) kullanılması fikri ortaya atılmıştır. 2015 yılında yapılan çalışmada [44], düşük maliyetli tersi kendisine eşit MDS matrislerin üretilmesi için LFSR’lerden üretilen yayılım tabakalarına odaklanılmıştır. Aynı yıl yapılan bir diğer çalışmada ise [36], özyinelemeli MDS matrislerin doğrudan üretimi için BCH kodlar kullanılmıştır. 2017 yılında yapılan çalışmada [45], özyinelemeli MDS matrislerin üretilmesi için kullanılabilecek farklı BCH kod sınıfı adayları verilmiştir. Bu sınıflar sayesinde; arama uzayı küçültüerek arama karmaşıklığı düşürülmüştür. Ayrıca, özyinelemeli yapılarla MDS matris üretimi için Companion matrislerin kullanılması verimli uygulamaların elde edilmesini sağlamıştır. Özyinelemeli yapılarla üretilen (tersi kendisine eşit) MDS matrisler için önerilen yerel optimizasyon yöntemleri ele alındığında, bu alanın iyi çalışıldığı ve çalışmaların doyum noktasına ulaştığı görülebilir [36].

Özyinelemeli – olmayan döngü – tabanlı MDS matrislerin donanım uygulamaları, özyinelemeli seri matrislere oranla daha verimlidir [39]. Bu nedenle özellikle XOR sayısı metriği tanıtıldıktan sonra çalışmalar, “döngü – tabanlı MDS matrislerin minimum XOR sayılı yerel optimizasyon uygulamalarının bulunması” üzerine odaklanmıştır. Başlangıçta bir yayılım matrisinin ikili matris gösterimindeki 1’lerin sayısı, bu matrisin donanım uygulaması için gereken XOR sayısı değeri için sınır değer olarak kullanılmıştır ancak bu sınır değeri ilgili yayılım matrisi için gereken maksimum XOR sayısının sınır değeridir. Bu nedenle sonraki çalışmalarda maksimum sınır değerinin “yayılım matrisinin elemanlarına odaklanılarak (diğer bir ifadeyle minimum XOR sayılı elemanları seçerek)” düşürüleceği gösterilmiştir [24]. 2015 yılında yapılan çalışmada [39], donanım – verimli MDS matrislerin tasarıımı için indirgenemez polinom seçiminin önemli olduğu kanıtlanmıştır. Çünkü bir eleman, farklı indirgenemez polinomlarla üretilen sonlu cisimler üzerinde, farklı XOR

sayılarına sahiptir. Aynı çalışmada minimum XOR sayılı tersi kendisine eşit MDS matrislerin bulunması için, Hadamard – Cauchy formunda matrisler önerilmiştir. 2016 yılında yapılan çalışmada [30], farklı sonlu cisimler üzerinde her bir eleman için gereken XOR sayıları verilerek, optimum XOR sayısına sahip elemanlarla oluşturulan tersi kendisine eşit MDS matrisler verilmiştir. 2017 yılında yapılan çalışmada [46], Toeplitz matrisler kullanılarak minimum XOR sayılı MDS matrisler üretilmiştir. Elemanları F_{2^n} sonlu cismi üzerinde tanımlı (tersi kendisine eşit) MDS matrisin, F_2 sonlu cismi üzerinde $n \times n$ blok matrisle ifade edilebileceği Örnek 9.11'de verilmiştir. 2018 yılında yapılan çalışmada [47], bu gösterim (blok matrisle ifade etme) kullanılarak yapılan arama veya üretim yöntemlerinde bazı (tersi kendisine eşit) MDS matrislerin bulunamayacağı problemi ele alınmıştır. Çünkü F_2 sonlu cismi üzerinde her matris F_{2^n} sonlu cismi üzerinde temsil edilmeyebilir, bu durum minimal polinomun indirgenemez olup olmadığına bağlıdır. Çalışmada ayrıca blok Vandermonde ve blok Cauchy – benzeri matrisler kullanarak (tersi kendisine eşit) MDS matrisler doğrudan üretilmiştir. 2018 yılında yapılan çalışmada [40], GHadamard matris formıyla farklı boyutlarda ve farklı indirgenemez polinom altında minimum XOR sayılı (tersi kendisine eşit) MDS matrisler verilmiştir. 2019 yılında yapılan çalışmada [54], F_{2^n} sonlu cismi üzerinde 3×3 boyutlu tersi kendisine eşit MDS matrislerin tamamının üretildiği yeni bir matris formu önerilmiştir. 2020 yılında yapılan çalışmada [55] ise, MDS matrislerin otomorfizma ve izomorfizmaları tanımlanarak, bu matrislerin verimli uygulamaları elde edilmiştir.

Özyinelemeli – olmayan yapılarla üretilen (tersi kendisine eşit) MDS matrisler için önerilen yerel optimizasyon yöntemleri ele alındığında, bu yöntemlerle sadece matrisin elemanlarına odaklanıldığı açıkça görülebilir. Ancak 2017 yılında Kranz ve arkadaşlarının, verilen bir yayılım matrisinin elemanlarının yerel optimizasyonu yerine, matrisin tamamına odaklanıp genel optimizasyon yöntemleriyle daha düşük XOR sayılı matrisler elde edilebileceğini göstermeleriyle, çalışmaların neredeyse tamamı genel optimizasyon yöntemleriyle (tersi kendisine eşit) MDS matrislerin bulunması üzerine kaymıştır [33].

9.4.2. (Tersi Kendisine Eşit) MDS Matrisler için Genel Optimizasyon Yöntemleri

Temelde, genel optimizasyon yöntemlerinde yayılım matrisini oluşturan doğrusal fonksiyonların devresi, Doğrusal Düz Sıralı Program (Linear Straight - Line Programs) olarak ifade edilir. Bu sıralı programlar $X_i = X_j \oplus X_k$ formundaki talimatlarla gerçekleştirilir, burada X_i programda daha önce görülmeyen bir toplam ifadesiyken, X_j ve X_k programda daha önce görülen girdileri ifade eder [48]. Genel optimizasyon yöntemlerinde amaç, bir yayılım matrisinin devresini uygulayabilecek en kısa doğrusal programı (Shortest Linear Program - SLP) bulmaktır. En kısa SLP programı minimum derinlik ve minimum XOR sayısıyla devrenin tasarımini verir. Burada matrisin elemanlarına değil, matrisi oluşturan devrenin tamamı göz önünde bulundurulur.

İki farklı genel optimizasyon tekniği vardır; iptalsiz (cancellation – free) programlar ve sezgisel (heuristic) yöntemler. İptalsız programlarda, $u = v \oplus w$ programının her satırı için, v değişkenlerinin hiçbirini w ifadesinde mevcut değildir, yani hesaplamada değişkenlerin iptali yoktur ve program iptale izin vermeyecek şekilde tasarlanır. Şöyle ki; $v = x_1 + x_2, w = x_1 + x_3$ ise program $v \oplus w$ işlemine izin vermeyecektir çünkü her iki değişken de x_1 girdisini içerdikinden x_1 girdileri birbirini iptal edecektir. Bu nedenle iptalsız programlarda bu duruma yol açacak değişkenlerin toplamlarına izin verilmez. Sezgisel optimizasyon yöntemleri ise iptallere izin vererek genel (common) optimum devre yolunun bulunması için önerilen programlardır.

Paar 1997 yılındaki çalışmasında [49], \mathbb{F}_{2^n} sonlu cismi üzerinde sabit bir elemanla çarpma işlemi için gereken XOR sayısının Red – Solomon kodlayıcıları kullanarak azaltılabilceğini göstermiştir. Aynı çalışmada PAAR1 ve PAAR2 genel optimizasyon algoritmalarını önermiştir. Bu algoritmalar iptale izin vermezler bu nedenle iptalsız programlardır. Her iki algoritma temelde en çok geçen alt ifadelerin bulunmasına ve bu ifadelerin toplanmasına dayanır. PAAR2 algoritmasının PAAR1'den farkı, işlemleri iteratif olarak yapmasıdır. Çalışmada \mathbb{F}_{2^4} sonlu cismi üzerinde %17.5, \mathbb{F}_{2^8} sonlu cismi üzerinde %40 XOR sayılarında azalma sağlanmıştır.

Örnek 9.31 : $\begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}$ yayılım matrisinin PAAR1 algoritması kullanılarak genel optimizasyonu yapıldığında;

$$\begin{bmatrix} y_0 \\ y_1 \\ y_2 \\ y_3 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \end{bmatrix} \rightarrow \begin{array}{l} x_0 \oplus x_2 \oplus x_3 \\ x_0 \oplus x_1 \oplus x_2 \\ x_0 \oplus x_1 \oplus x_2 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{array} \quad (9.28)$$

Başlangıçta en çok geçen alt ifadeler belirlenir; $(x_0 \oplus x_2)$, daha sonra t_0 ara değişkenine $t_0 = x_0 \oplus x_2$ değeri verilir ve cebirsel ifade aşağıdaki gibi ifade edilir;

$$\begin{array}{l} t_0 \oplus x_3 \\ \rightarrow t_0 \oplus x_1 \\ t_0 \oplus x_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{array} \quad (9.29)$$

Sonrasında yine en çok geçen alt ifadeler belirlenir; $(t_0 \oplus x_1)$, daha sonra t_1 ara değişkenine $t_1 = t_0 \oplus x_1$ değeri verilir ve cebirsel ifade aşağıdaki gibi ifade edilir;

$$\begin{array}{l} t_0 \oplus x_3 \\ \rightarrow t_1 \\ t_1 \oplus x_3 \\ x_1 \oplus x_2 \oplus x_3 \end{array} \quad (9.30)$$

Genel optimizasyon yapılmadan önce Eşitlik (9.28)'de verilen yayılım matrisi 9 XOR sayısıyla uygulanabilirken, PAAR1 genel optimizasyon algoritmasının uygulanmasıyla Eşitlik (9.30)'dan da görüleceği gibi 4 XOR sayısıyla uygulanabilir.

Boyar ve Peralta 2010 yılındaki çalışmasında [50], yeni bir sezgisel optimizasyon yöntemi önermiştir. Hangi alt ifadelerin birbiriyle toplanacağına karar verilirken yeni mesafelerin toplamını minimum yapan çiftler seçilir, seçim sonucunda eğer kuyruk oluşursa (mesafe değerleri birbirine eşitse) öklid normu (normu maksimum yapan çiftler seçilir) kullanılır. Önerilen yöntem PAAR1 algoritmasından yavaştır ancak XOR sayılarında iyileşmeler sağlamıştır. Boyar ve arkadaşları 2013 yılındaki çalışmalarında [51] ise SLP programları geliştirerek, [50]'deki çalışmada verilen sonuçları daha da optimize etmişlerdir. Boyar ve arkadaşlarının 2017 yılındaki çalışmasında [52], gerekli maksimum derinlik değeri korunarak, PAAR1 ve PAAR2 algoritmaları ön işleme adımları eklenerek ve iptallere izin verilerek iyileştirilmiştir. Önerilen yöntemde devre üzerinde şu adımlar uygulanır; doğrusal olmayan bileşenlerin daha düşük derinlikli yapılara yeniden sentezlenmesi, önerdikleri See-Saw Yöntemi ile doğrusal bileşenleri yeniden sentezleyen rastgele açgözlü (greedy) bir sezgisel yöntem uygulanması. Bu yöntem sayesinde global optimizasyon için verimli sonuçlar elde edilmiştir. Boyar ve arkadaşlarının 2019 yılındaki çalışmasında [53] ise, verilen derinlik sınırı değerine göre küçük devrelerin oluşturulması için yeni bir sezgisel DCLO (Depth - Constrained Linear Optimization – Derinlik Sınırlı Doğrusal Optimizasyon) yöntemi önerilmiştir. Yöntem [52]'de verilen See-Saw algoritmasını iteratif olarak tekrarlayarak kullanır.

Tan ve Peyrin 2019 yılındaki çalışmasında [3], [50]'de verilen optimizasyon yöntemine rastgelelik ekleyerek RNBP (Random Normal Boyar Peralta) algoritmasını önermişlerdir. Çalışmada ayrıca deterministik olmayan A1 ve A2 optimizasyon algoritmaları da önerilmiştir. Bu algoritmalar da RNBP gibi [50]'de verilen algoritma tabanlıdır. Ancak bu algoritmaların temel farkı, olabildiğince çok sayıda yakın hedefin mesafesini azaltabilecek elemanın aranması yerine, en yakın hedeflerden biri seçilerek bu hedefi minimum yapacak kapı (girdi çiftleri) seçilir. Bu adım filtreleme (filtering) adımı olarak adlandırılmıştır. Filtreleme adımı daha uzaktaki hedefleri en aza indirgeyen kapılarıfiltrelemek için kullanılır, böylece bu kapılarla işlem yapılmaz. Filtreleme işleminden sonra toplam mesafeyi minimum yapan kapılardan birinin seçildiği seçme (selection) adımı uygulanır. Sonrasında kuyruğun kırılması işlemi [50]'deki gibi öklid normunu maksimum yapan çiftlerin seçileceği kuyruk-kırma (tie-breaking) adımı uygulanır. Son adım olan rastgeleleştirme (randomisation) adımında ise, eğer kuyruk – kırma adımı kuyruğu kırmak için çözüm sağlanamazsa aday kapılar arasından rastgele biri seçilir. A2 algoritma-

sında A1 algoritmasından farklı olarak, kuyruk – kırma adımı atlanır böylece daha fazla rastgelelik sağlanmış olur.

Tablo 9.1'de yukarı verilen genel optimizasyon yöntemlerinin özet bir karşılaştırılması verilmiştir.

Tablo 9.1. Genel Optimizasyon Yöntemlerinin Karşılaştırılması

Algoritma	Yıl	Yöntem	Dezavantajları
PAAR1 (iptalsız) [49]	1997	İteratif olarak alt ifadeleri eler.	En sık geçen çiftler önceden hesaplanabilir bu da sadece yerel optimum çözüm sağlar, genel optimum çözüm garanti etmez.
PAAR2 (iptalsız) [49]	1997	İteratif olarak alt ifadeleri eler. En yüksek frekans değerine sahip tüm olası çiftleri kontrol eder.	En sık geçen çiftler önceden hesaplanabilir bu da sadece yerel optimum çözüm sağlar, genel optimum çözüm garanti etmez.
BP10 (sezgisel) [50]	2010	İptallere izin verir. İki adımdan oluşur; ilk adımda doğrusal olmayan bileşenler (AND kapısı) optimize edilirken, ikinci adımda doğrusal bileşenler (XOR kapısı) optimize edilir.	Devre derinliğini önemsemeyez.
BP13 (sezgisel) [51]	2013	BP10 ile çok benzerdir. Yöntem iptallere izin verir. İki adımdan oluşur; ilk adımda doğrusal olmayan bileşenler (AND kapısı) ad – hoc sezgisel yöntemiyle optimize edilirken, ikinci adımda doğrusal bileşenler (XOR kapısı) optimize edilir. Eğer kuyruk olsursa öklid norm değerini maksimum yapan çiftler seçilir.	Devre derinliğini önemsemeyez.
BP17 (sezgisel) [52]	2017	BP10 ve BP13 ile çok benzerdir. Daha düşük derinlikli devreler bulmak için See-Saw metodu uygulanır.	Devre derinliği önemsenir ancak verilen devre derinliği sınır değerine göre kısıtlama yapılamaz.
BP19 (sezgisel) [53]	2019	Verilen devre derinliğine göre küçük doğrusal devrelerin bulunması için DCLÖ yöntemini kullanır. Doğrusal bileşenlerin alt ve üst sınırlarını değiştirmek için See-Saw metodu uygulanır. AND, XOR ve XNOR kapısı sayılarını azaltmayı amaçlar.	Devre derinliği önemsenir ancak doğrusal bileşenlerin yanı sıra, doğrusal olmayan bileşenler de dikkate alınır ve optimize edilir. Sadece doğrusal bileşenlerin optimize edileceği durumlarda yöntemin See-Saw kısmı kullanılmalıdır.
TP19 (sezgisel) [3]	2019	RNPB algoritmasıyla BP10 algoritmasına rastgelelik eklenmiştir. A1 ve A2 optimizasyon algoritmalarında, kuyruk kırmada kullanılan öklid normunu ile çözüm sağlanamazsa, rastgelelik adımı sayesinde kuyruk problemi çözülmüş olur.	Devre derinliğini önemsemeyez.

Literatürde önerilen genel optimizasyon algoritmalarının yanı sıra, yayılım matrislerinin genel devre optimizasyonunu yapan SAT-based [56] ve LIGHTER [57] gibi biçimlendirici (former) araçlar ile Yosys [58] ve ABC [59] gibi hazır devre sentezleyicileri mevcuttur.

Genel optimizasyon yöntemleri, biçimlendirici araçlar ve hazır devre sentezleyicileri sayesinde blok şifrelerin yayılım tabakalarında kullanılan (tersi kendisine eşit) MDS matrislerin donanım üzerinde optimize edilmiş verimli uygulamaları mümkündür.

9.5. SONUÇ VE DEĞERLENDİRMELER

Bu bölümde, blok şifrelerin yayılım tabakaları genel bir bakış açısıyla ele alınmıştır. Bu kapsamında, blok şifrelerdeki yayılma tekniğinin önemi ve yayılmanın hangi bileşenlerle sağlandığı açıklanmıştır. En iyi ve verimli yayılım tabakalarının tasarımlı için, (tersi kendisine eşit) MDS matrislerin önemi vurgulanmış, bu matrislerin cebirsel özellikleri detaylarıyla verilmiştir. Bunun yanı sıra (tersi kendisine eşit) MDS matrislerin tasarımlı için kullanılan yöntemler, bu yöntemlerin avantajları ve dezavantajları karşılaştırmalı olarak sunulmuştur. Donanım-verimli (tersi kendisine eşit) MDS matrislerin üretilmesi için özellikle XOR sayısı ve devre derinliği parametrelerinin önemi vurgulanmış, bu matrisler için yerel ve genel optimizasyon yöntemleri kıyaslamalı olarak verilmiştir. Genel optimizasyon yöntemlerinde yayılım matrisini oluşturan devrenin tamamı göz önünde bulundurulduğundan, yerel optimizasyon yöntemleri yerine genel optimizasyon yöntemlerinin kullanılması, bir yayılım matrisinin daha düşük XOR sayılı ve minimum devre derinlikli tasarımının gerçeklenmesine olanak sağlar. Genel optimizasyon teknikleri ile bulunması hedeflenen en kısa SLP programı, biçimlendirici araçlar ve hazır devre sentezleyicileri kullanılarak daha da optimize edilir. Bu nedenle farklı yerel optimizasyon yöntemlerinin geliştirilmesinin yanı sıra genel optimizasyon yöntemlerinin de tasarımlı önemli birer açık problemdir.

Düşük maliyetli (tersi kendisine eşit) MDS matrislerin üretilmesi için yeni yerel ve genel optimizasyon yöntemlerinin geliştirilmesi açık problem-

leri için olası ileriki çalışmalar ele alındığında, kriptografik açıdan güçlü ve verimli ikili yayılım tabakalarının tasarımları için literatürde yer alan bazı yöntemler [60], [61] yeni ve minimum maliyetli tersi kendisine eşit MDS matrislerin tasarımları için kullanılabilir. Bazı özel matris formlarının kullanımı kaynaklı sonlu cisim üzerinde çalışılan alan, aslında aranılan minimum XOR sayılı ve minimum derinlikli (tersi kendisine eşit) MDS matrisleri içermiyor olabilir. Bu nedenle seçilecek özel boyutlar (4×4 , 8×8 , 16×16) için \mathbb{F}_{2^m} sonlu cismi üzerinde özellikle tersi kendisine eşit MDS matrislerin tamamını üretebilen yeni formların tasarlanması önemli çalışmalarlardır. Genel optimizasyon yöntemleri için; özellikle kuyruk kırma adımı sonunda seçilen aday çiftler arasından seçimler yapılırken adayların farklı istatistiksel dağılımlar göz önünde bulundurularak seçilmesi devreyi oluşturacak derinlik ve XOR sayısının azaltılmasında etkili olacaktır. Bunun yanı sıra yeni SLP programlarının geliştirilmesi olası çözüm önerilerindendir.

Düşük XOR maliyetli ve minimum derinlikli (tersi kendisine eşit) MDS matrislerin üretilmesi literatürde çalışılan önemli açık problemlerden biri olduğu için bu bölüm kapsamında verilen bilgiler diğer çalışmalar için bir rehber niteliği taşıyacaktır.

Teşekkür

Çalışmada, Meltem Kurt Pehlivanoğlu TÜBİTAK 2219-Yurt Dışı Doktora Sonrası Araştırma Burs Programı kapsamında kısmi olarak desteklenmiştir.

KAYNAKLAR

- [1] A. Kerckhoffs, La Cryptographie Militaire I-III, Journal des Sciences Militaires, pp. 5–38, 1883.
- [2] R. Avanzi, A Salad of Block Ciphers, IACR Cryptology ePrint Archive, Report 2016/1171, 2016.

- [3] Q. Q. Tan, T. Peyrin, Improved Heuristics for Short Linear Programs, Cryptology ePrint Archive, Report 2019/847, 2019.
- [4] G. Bertoni, J. Daemen, M. Peeters, G. Van Assche, The Making of KECCAK, Cryptologia, Vol. 38, No. 1, pp. 26–60, 2014.
- [5] J. Daemen, Cipher ve Hash Function Design Strategies Based On Linear and Differential Cryptanalysis, Katholieke Universiteit Leuven, PhD Thesis, Belgium, 1995.
- [6] L.E. Bassham, A. Rukhin, J. Soto, J. Nechvatal, M. Smid, E. Barker, S. Leigh, M. Levenson, M. Vangel, D. Banks, A. Heckert, J. Dray ve S. Vo, A Statistical Test Suite for Random and Pseudorandom Number Generators for Cryptographic Applications, Technical Report, United States, 2010.
- [7] M.T. Sakallı, Kriptografik Test Yöntemleri Ve Kriptoanaliz, Siber Güvenlik ve Savunma: Problemler ve Çözümler, pp. 87-134, 2019.
- [8] S. Sarkar, H. Syed, R. Sadhukhan, D. Mukhopadhyay, Lightweight Design choices for LED-like block ciphers, INDOCRYPT 2017, LNCS, Vol. 10698, pp. 267–281, 2017.
- [9] A. Bogdanov vd., PRESENT: An Ultra-Lightweight Block Cipher, CHES 2007, LNCS, Vol. 4727, pp. 450–466, 2007.
- [10] L. Knudsen, G. Leander, A. Poschmann, M.J.B. Robshaw, PRINTcipher: A Block Cipher for IC-Printing, CHES 2010, LNCS, Vol. 6225, pp. 16–32, 2010.
- [11] P. Barreto, V. Rijmen, The Khazad Legacy Level Block Cipher, First Open NESSIE Workshop, KULeuven, 2000.
- [12] P. Barreto, V. Rijmen, The Anubis Block Cipher, available at: <http://www.larc.usp.br/pbarreto/anubis-tweak.zip>
- [13] FX. Standaert, G. Piret, G. Rovroy, J.-J. Quisquater, JD. Legat, ICEBERG: An Involutional Cipher Efficient for Block Encryption in Reconfigurable Hardware, FSE 2004. LNCS, Vol. 3017, pp. 279–298, 2004.
- [14] NIST, Data Encryption Standard, Federal Information Processing Standard (FIPS), Publication 46, U.S. Department of Commerce, Washington D.C., 1977.
- [15] J.L. Massey, SAFER K-64: A Byte-oriented Block-ciphering Algorithm, FSE 1993, LNCS, Vol. 809, pp. 1–17, 1994.
- [16] J.L. Massey, SAFER K-64: One Year Later, FSE 1994, LNCS, Vol. 1008, pp. 212–241, 1995.
- [17] D. Wagner, N. Ferguson, B. Schneier, Cryptanalysis of FROG, Proc. 2nd AES Candidate Conference, National Institute of Standards and Technologies, pp. 175–181, 1999.

- [18] V. Rijmen, J. Daemen, B. Preneel, A. Bosselaers, E. De Win, The Cipher SHARK, FSE 1996, LNCS, Vol. 1039, pp. 99–111, 1996.
- [19] J. Daemen, L. Knudsen, V. Rijmen, The Block Cipher Square, FSE 1997, LNCS, Vol. 1267, pp. 149–165, 1997.
- [20] J. Daemen, V. Rijmen, The Design of Rijndael: AES - The Advanced Encryption Standard, Information Security and Cryptography, Springer, 2002.
- [21] B. Schneier, J. Kelsey, D. Whiting, D. Wagner, C. Hall, N. Ferguson, Twofish, A Block Encryption Algorithm, In First AES Candidate Conference, National Institute of Standard and Technology, 1998.
- [22] K. Aoki vd., Camellia: A 128-Bit Block Cipher Suitable for Multiple Platforms — Design and Analysis, SAC 2000, LNCS, Vol. 2012, pp. 39–56, 2001.
- [23] K.C. Gupta, I.G. Ray, On Constructions of Involutory MDS Matrices, AFRICACRYPT 2013, LNCS, Vol. 7918, pp. 43-60, 2013.
- [24] S. Duval, G. Leurent, MDS Matrices with Lightweight Circuits, IACR Trans. Symmetric Cryptol., Vol. 2018, No. 2, pp. 48–78, 2018.
- [25] M. Kurt Pehlivanoğlu, Maksimum Uzaklıkta Ayrılabilen Matrislerin Elde Edilebilmesi İçin Yeni Bir Matris Formu ve Bir Hafif Sıklet Blok Şifreye Uygulaması, Doktora Tezi, Kocaeli Üniversitesi, Kocaeli, Türkiye, 2018.
- [26] K.C. Gupta, S.K. Pandey, I.G. Ray, S. Samanta, Cryptographically Significant MDS Matrices Over Finite Fields: A Brief Survey And Some Generalized Results, Advances in Mathematics of Communications, Vol. 13, No. 4, 2019.
- [27] K. Khoo, T. Peyrin, A.Y. Poschmann, H. Yap, FOAM: Searching for Hardware-Optimal SPN Structures and Components with a Fair Comparison, CHES 2014, LNCS, Vol. 8731, pp. 433-450, 2014.
- [28] R. Zhao, B. Wu, R. Zhang, Q. Zhang, Designing Optimal Implementations of Linear Layers (Full Version), Cryptology ePrint Archive, Report 2016/1118, 2016.
- [29] S. Li, S. Sun, C. Li, Z. Wei ve L. Hu, Constructing Low- latency Involutory MDS matrices with Lightweight Circuits, IACR Transactions on Symmetric Cryptology, Vol. 1, pp. 84–117, 2019.
- [30] C. Beierle, T. Kranz, G. Leander, Lightweight Multiplication in $GF(2^n)$ with Applications to MDS Matrices, CRYPTO 2016, LNCS, Vol. 9814, pp. 625–653, 2016.
- [31] D. Toh, J. Teo, K. Khoo, S.M. Sim, Lightweight MDS Serial-Type Matrices with Minimal Fixed XOR Count, AFRICACRYPT 2018, LNCS, Vol. 10831, pp. 51–71, 2018.

- [32] K.C. Gupta, I.G. Ray, On Constructions of MDS Matrices from Companion Matrices for Lightweight Cryptography, CD-ARES 2013, LNCS, Vol. 8128, pp. 29–43, 2013.
- [33] T. Kranz, G. Leander, K. Stoffelen, F. Wiemer, Shorter Linear Straight-Line Programs for MDS Matrices, IACR Transactions on Symmetric Cryptology, Vol. 2017, No. 4, pp. 2017.
- [34] P.S.L.M. Barreto, M. J. Simplicio, CURUPIRA-1, A Block Cipher for Constrained Platforms, 25th Brazilian Symposium on Computer Networks and Distributed Systems, 2007.
- [35] T.P. Berger, Construction of Recursive MDS Diffusion Layers from Gabidulin Codes, INDOCRYPT 2013, LNCS, Vol. 8250, pp. 274-285 2013.
- [36] D. Augot, M. Finiasz, Direct Construction of Recursive MDS Diffusion Layers Using Shortened BCH Codes, FSE 2014, LNCS, Vol. 8540, pp. 3-17, 2015.
- [37] K.C. Gupta, I.G. Ray, Cryptographically Significant MDS Matrices Based on Circulant and Circulant-like Matrices for Lightweight Applications, Cryptogr. Commun., Vol. 7, pp. 257-287, 2015.
- [38] P. Junod, S. Vaudenay, Perfect Diffusion Primitives for Block Ciphers, SAC 2004, LNCS, Vol. 3357, pp. 84-99, 2004.
- [39] S.M. Sim, K. Khoo, F. Oggier, T. Peyrin, Lightweight MDS Involution Matrices, FSE 2015, LNCS, Vol. 9054, pp. 471-493, 2015.
- [40] M. K. Pehlivanoglu, M. T. Sakalli, S. Akleylik, N. Duru ve V. Rijmen, Generalisation of Hadamard Matrix to Generate Involutory MDS Matrices for Lightweight Cryptography, IET Information Security, Vol. 12, pp. 348–355, 2018.
- [41] M. Sajadieh, M. Dakhilalian, H. Mala, B. Omoomi, On Construction of Involutory MDS Matrices from Vandermonde Matrices in $GF(2^q)$, Des. Codes Cryptogr., Vol. 64, pp. 287–308, 2012.
- [42] J. Guo, T. Peyrin, A. Poschmann, The PHOTON Family of Lightweight Hash Functions, CRYPTO 2011, LNCS, Vol. 6841, pp. 222-239, 2011.
- [43] S. Wu, M. Wang, W. Wu, Recursive Diffusion Layers for (Lightweight) Block Ciphers and Hash Functions, SAC 2012, LNCS, Vol. 7707, pp. 355–371, 2013.
- [44] H. Xu, Y. Zheng, X. Lai, Construction of Perfect Diffusion Layers from Linear Feedback Shift Registers, IET Information Security, Vol. 9, No. 2, pp. 127–135, 2015.
- [45] K.C. Gupta, S.K. Pandey, A. Venkateswarlu, On the Direct Construction of Recursive MDS Matrices, Designs, Codes and Cryptography, Vol. 82, pp. 77-94, 2017.

- [46] S. Sarkar, H. Syed, Analysis of Toeplitz MDS Matrices, ACISP 2017, LNCS, Vol. 10343, pp. 3-18, 2017.
- [47] Q. Li, B. Wu, Z. Liu, Direct Constructions of (Involutory) MDS Matrices from Block Vandermonde and Cauchy-Like Matrices, WAIFI 2018, LNCS, Vol. 11321, pp. 275–290, 2018.
- [48] A. Visconti, C. V. Schiavo, R. Peralta, Improved upperbounds for the expected circuit complexity of dense systems of linear equations over GF(2), Inf. Process. Lett., Vol. 137, pp. 1–5, 2018.
- [49] C. Paar, Optimized Arithmetic for Reed-Solomon Encoders, 1997 IEEE International Symposium on Information Theory, pp. 250, 1997.
- [50] J. Boyar, R. Peralta, A New Combinational Logic Minimization Technique with Applications to Cryptology, SEA 2010, LNCS, Vol. 6049, pp. 178-189, 2010.
- [51] J. Boyar, P. Matthews, R. Peralta, Logic Minimization Techniques with Applications to Cryptology, Journal of Cryptology, Vol. 26, pp. 280–312, 2013.
- [52] J. Boyar, M. G. Find, R. Peralta, Low-Depth, Low-Size Circuits for Cryptographic Applications, BFA 2017. 2017.
- [53] J. Boyar, M. G. Find, R. Peralta, Small Low-depth Circuits for Cryptographic Applications, Cryptography and Communications, Vol. 11, No. 1, pp. 109–127, 2019.
- [54] G.G. Guzel, M.T. Sakalli, S. Akleylik, V. Rijmen, Y. Çengellenmiş, A New Matrix Form to Generate All 3×3 Involutory MDS Matrices over \mathbb{F}_{2^m} , Information Processing Letters, Vol.147, pp. 61-68, 2019
- [55] M.T. Sakalli, S. Akleylik, K. Akkanat, V. Rijmen, On the Automorphisms and Isomorphisms of MDS Matrices and their Efficient Implementations, Turkish Journal of Electrical Engineering and Computer Science, Vol. 28, No. 1, pp. 275-289, 2020.
- [56] K. Stoeffelen, Optimizing S-Box Implementations for Several Criteria Using SAT Solvers, FSE 2016, LNCS, Vol. 9783 pp. 140–160. Springer, 2016.
- [57] J. Jean, T. Peyrin, S.M. Sim, J. Tourteaux, Optimizing Implementations of Lightweight Building Blocks, IACR Trans. Symmetric Cryptol., Vol. 2017, No. 4, pp. 130–168, 2017.
- [58] C. Wolf, Yosys Open Synthesis Suite, available at: <http://www.clifford.at/yosys/>.
- [59] R.K. Brayton, A. Mishchenko, {ABC:} An Academic Industrial Strength Verification Tool, CAV 2010, Vol. 6174, LNCS, pp. 24–40, 2010.
- [60] S. Akleylik, V. Rijmen, M.T. Sakalli, E. Öztürk, Efficient Methods to Generate Cryptographically Significant Binary Diffusion Layers, IET Information Security, Vol. 11, No. 4, pp. 177-187,2017.

- [61] M.T. Sakallı, S. Akleylek, B. Aslan, E. Buluş, F. Büyüksaraçoğlu Sakallı, On the Construction of 20×20 and 24×24 Binary Matrices with Good Implementation Properties for Lightweight Block Ciphers and Hash Functions, Mathematical Problems in Engineering, Vol. 2014, pp. 1-13, 2014.