T.C.
TRAKYA ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

HAFİF SIKLET İNVOLUTİF YER DEĞİŞTİRME KUTULARININ KRİPTOGRAFİK ÖZELLİKLERİNİN İNCELENMESİ

PINAR SAVAŞTÜRK

YÜKSEK LİSANS TEZİ

BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

Tez Danışmanı: Prof. Dr. Muharrem Tolga SAKALLI

EDİRNE-2024

PINAR SAVAŞTÜRK ’ın hazırladığı “**HAFİF SIKLET İNVOLUTİF YER DEĞİŞTİRME KUTULARININ KRİPTOGRAFİK ÖZELLİKLERİNİN İNCELENMESİ**” başlıklı bu tez, tarafımızca okunmuş, kapsam ve niteliği açısından Bilgisayar Mühendisliği Anabilim Dalında bir **Yüksek Lisans tezi** olarak kabul edilmiştir.

Jüri Üyeleri İmza

Prof. Dr. Muharrem Tolga SAKALLI

Dr. Öğr. Üyesi Emir ÖZTÜRK

Dr. Öğr. Üyesi Bora ASLAN

Tez Savunma Tarihi: 08.01.2024

Bu tezin Yüksek Lisans tezi olarak gerekli şartları sağladığını onaylarım.

İmza

Tez Danışmanı

Prof. Dr. Muharrem Tolga SAKALLI

Trakya Üniversitesi Fen Bilimleri Enstitüsü onayı

Prof. Dr. Özlem ÇETİN ERDOĞAN
Fen Bilimleri Enstitüsü Müdürü

T.Ü. FEN BİLİMLERİ ENSTİTÜSÜ
BİLGİSAYAR MÜHENDİSLİĞİ YÜKSEK LİSANS PROGRAMI
DOĞRULUK BEYANI

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

08.01.2024
Pınar SAVAŞTÜRK

İmza

Yüksek Lisans Tezi
Hafif Sıklet İnvolutif Yer Değiştirme Kutularının Kriptografik Özelliklerinin İncelenmesi
T.Ü. Fen Bilimleri Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalı

ÖZET

Hafif sıklet şifreleme yöntemleri, IoT cihazlarının çeşitlenmesi ve yayınlaşması ile daha geniş kullanım alanına ulaşmıştır. Hafif sıklet şifrelemede kullanılan, tek doğrusal olmayan katman olan yer değiştirme kutularının kriptoanaliz yöntemlerine karşı dayanıklılığı aynı zamanda şifrelemenin de saldırılara karşı dayanıklılığı anlamına gelmektedir. Bu sebeple, tez çalışması kapsamında; hafif sıklet şifrelemede kullanılan S-kutuları, çeşitli kriptografik özelliklere göre incelenerek, doğrusal/diferansiyel kriptoanaliz yöntemlerine en dayanıklı S-kutularının sunulması amaçlanmıştır. 4-bit girişten 4-bit çıkışa ve 3-bit girişten 3-bit çıkışa haritalanan, bijektif, involutif tüm S-kutusu permütasyonları 10 kriptografik özelliğe göre incelenerek, kriptoanaliz yöntemlerine en dayanıklı S-kutuları tespit edilmiştir. Tez çalışmasında 3×3 boyutunda involutif 'Optimal' S-kutuları, doğrusal yaklaşım tablosunda en büyük mutlak değer 2, fark dağılım tablosunda en büyük değer 2 ve cebirsel derece 2 olacak şekilde tanımlanmıştır. 4×4 boyutunda involutif 'Optimal' S-kutuları, doğrusal yaklaşım tablosunda en büyük mutlak değer 4, fark dağılım tablosunda en büyük değer 4 ve cebirsel derece 3 olacak şekilde tanımlanmıştır. Optimal olan S-kutuları, geri kalan 7 kriptografik özellik olan; BIBO Örüntüsü, Doğrusal Dal Sayısı, Diferansiyel Dal Sayısı, Doğrusallık Frekansı, Diferansiyel Tekdüzelik Frekansı, Boomerang Bağlantı Tablosu Tekdüzeliği ve Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği açısından incelenerek sonuçlar ortaya konulmuştur. 5×5 boyutunda; doğrusal yaklaşım tablosunda en büyük mutlak değer, fark dağılım tablosu en büyük değer ve cebirsel derecede iyi özelliklere sahip S-kutuları genetik algoritma ile bulunarak, kriptografik özellikleri analiz edilmiştir. İncelenen kriptografik özelliklere göre en iyi değerlere sahip olan S-kutularının vektörel çıkış Boole fonksiyonlarından oluşan cebirsel ifadeleri optimizasyon işleminden geçirilmeden, bitslice kapı karmaşıklıkları analiz edilmiştir. Tez çalışmasında, hafif sıklet şifrelemede kullanılacak olan S-kutuları seçilirken 10 kriptografik özellik dikkate alınmış ve bu özelliklere göre en iyi değerlere sahip olan S-kutuları sunulmuştur.

Yıl : 2024

Sayfa Sayısı : 116

Anahtar Kelimeler : Involutif Yer Değiştirme Kutuları, Hafif Sıklet Involutif Yer Değiştirme Kutuları, Yer Değiştirme Kutuları Kriptoanaliz

Master of Science Thesis
Examination of Cryptographic Properties of Lightweight Involutive Substitution Boxes
Trakya University Institute of Natural and Applied Sciences
Department of Computer Engineering

ABSTRACT

Lightweight encryption methods have reached wider use with the diversification and proliferation of IoT devices. The resistance of substitution boxes, the only non-linear layer used in lightweight encryption, to cryptanalysis methods, it also means that encryption is resistant to attacks. For this reason, within the scope of the thesis study; by examining S-boxes used in lightweight encryption according to various cryptographic properties, it was aimed to present S-boxes that are most resistant to linear/differential cryptanalysis methods. All bijective and involutive S-box permutations, mapped from 4-bit input to 4-bit output and from 3-bit input to 3-bit output, were examined according to 10 cryptographic features and the S-boxes most resistant to cryptanalysis methods were determined. In the thesis study, involutive S-boxes of 3×3 size defined as 'Optimal' like this; largest absolute value in the linear approximation table is 2, the largest value in the difference distribution table is 2 and the algebraic degree is 2. Involutive S-boxes of 4×4 size defined as 'Optimal' like this; largest absolute value in the approximation table is 4, the largest value in the difference distribution table is 4 and the algebraic degree is 3. The optimal S-boxes are the remaining 7 cryptographic features; BIBO Pattern, Linear Branch Number, Differential Branch Number, Frequency of Linearity, Frequency of Differential Uniformity, Boomerang Connectivity Table Uniformity and Differential Linear Connectivity Table Uniformity were examined and the results were presented. S-boxes of 5×5 size with the largest absolute value in the linear approximation table, the largest value in the difference distribution table and algebraic degree good properties were found with the genetic algorithm and their cryptographic properties were analyzed. Bitslice gate complexities were analyzed without optimizing the algebraic expressions consisting of vectorial output Boolean functions of S-boxes, which have the best values according to the cryptographic features examined. In the thesis study; while selecting the S-boxes to be used in lightweight encryption, 10 cryptographic features were taken into consideration and the S-boxes with the best values according to these features were presented.

Year : 2024

Number of Pages : 116

Keywords : Involutive Substitution Boxes, Lightweight Involutive Substitution Boxes, Substitution Boxes Cryptoanalysis

TEŞEKKÜR

Tez sürecimde kıymetli katkılarını, yardımlarını ve sabrını benden esirgemeyen danışmanım Sayın Prof. Dr. Muharrem Tolga SAKALLI'ya (Trakya Üniversitesi Bilgisayar Mühendisliği Bölüm Başkanı),

Tez çalışmasına yaptığı uygulama destekli katkıları ve yardımları için Sayın Dr. Öğr. Üyesi Emir ÖZTÜRK'e (Trakya Üniversitesi Bilgisayar Mühendisliği Öğretim Üyesi),

Varlıkları ile hayatıma anlam katan kıymetli babam Eşref SAVAŞTÜRK, sevgili annem Nazlı SAVAŞTÜRK, değerli abilerim İbrahim SAVAŞTÜRK ve Tolga SAVAŞTÜRK'e manevi desteklerinden dolayı,

Teşekkürlerimi sunmaktayım.

Pınar SAVAŞTÜRK

İÇİNDEKİLER

ÖZET iv

ABSTRACT vi

TEŞEKKÜR viii

SİMGELER DİZİNİ xiii

KISALTMALAR DİZİNİ xiv

ŞEKİLLER DİZİNİ xv

ÇİZELGELER DİZİNİ xvi

1 GİRİŞ 1

1.1 Kriptografi 1
1.2 Bilgi Güvenliği Açısından Kriptografi 2
1.3 NIST - Hafif Sıklet Kriptografi 2
1.4 Kriptografik Sitemin Bileşenleri 2
1.4.1 Anahtar (Key) 3
1.4.2 Açık Metin (Plaintext) 3
1.4.3 Şifreleme (Encryption) 3
1.4.4 Şifre Çözme (Decryption) 3
1.5 Kriptoanaliz 3
1.5.1 Doğrusal Kriptoanaliz 4
1.5.2 Diferansiyel Kriptoanaliz 5
1.6 Simetrik Şifreleme Algoritmaları 6
1.7 Blok Şifreleme Algoritmaları 6
1.8 Tezin Amacı, Önemi ve Ana Hatları 8

2 MATEMATİKSEL ALTYAPI **10**
2.1 Boole Fonkiyonları . . . 11
2.1.1 Cebirsel Gösterim Biçimi (Algebraic Normal Form - ANF) . . . 12
2.1.2 Doğrusal (Affine) Fonksiyon . . . 13
2.1.3 Hamming Ağırlık/Uzaklık . . . 14
2.1.4 Doğrusal Olmama (Non-Linearity) . . . 15
2.2 Yer Değiştirme Kutuları (S-Kutuları - Substitution Boxes - S-Boxes) . . . 16
2.2.1 Involutif Yer Değiştirme Kutuları . . . 17
2.2.2 Sabit Nokta (Fixed Point) Sayısı . . . 18
2.2.3 Doğrusal Yaklaşım Tablosu (Linear Approximation Table - LAT) . 19
2.2.4 Fark Dağılım Tablosu (Difference Distribution Table - DDT) . . . 23
2.2.5 Cebirsel Derece (Algebraic Degree - AD) . . . 26
2.2.6 Kötü Girdi Kötü Çıktı Örüntüsü (Bad Input Bad Output Pattern - BIBO Pattern - BIBO Örüntüsü) . . . 28
2.2.6.1 BIBO DDT Sayısının Elde Edilmesi . . . 28
2.2.6.2 BIBO LAT Sayısının Elde Edilmesi . . . 29
2.2.7 Dal Sayısı (Branch Number) . . . 31
2.2.7.1 Doğrusal Dal Sayısı (Linear Branch Number - LBN) . . 31
2.2.7.2 Diferansiyel Dal Sayısı (Differential Branch Number - DBN) . . . 33
2.2.8 Frekans İncelemesi . . . 35
2.2.8.1 Diferansiyel Tekdüzelik Frekansı (Frequency of Differential Uniformity) . . . 36
2.2.8.2 Doğrusallık Frekansı (Frequency of Linearity) . . . 37
2.2.9 Boomerang Bağlantı Tablosu (Boomerang Connectivity Table - BCT) . . . 39
2.2.9.1 Boomerang Bağlantı Tablosu Tekdüzeliği (Boomerang Connectivity Table Uniformity - BCTU) . . . 42
2.2.10 Diferansiyel Doğrusal Bağlantı Tablosu (Differential Linear Connectivity Table - DLCT) . . . 43
2.2.10.1 Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği (Differential Linear Connectivity Table Uniformity - DLCTU) . . . 44
2.2.11 Bitslice Kapı Karmaşıklığı (Bitslice Gate Complexity - BGC) . . . 44

3 3 × 3 BOYUTUNDA TÜM İNVOLUTİF S-KUTULARININ KRİPTOGRAFİK ÖZELLİKLERİNİN İNCELEME SONUÇLARI **47**

3.1 3 × 3 Boyutunda Optimal S-kutularının Sabit Nokta ve Doğrusal/Diferansiyel Dal Sayıları İnceleme Sonuçları 49
3.2 3 × 3 Boyutunda Optimal S-kutularının BIBO Örüntüsü İnceleme Sonuçları 49
3.3 3 × 3 Boyutunda Optimal S-kutularının Boomerang Bağlantı Tablosu Tekdüzeliği İnceleme Sonuçları 50
3.4 3 × 3 Boyutunda Optimal S-kutularının BCTU Değeri ve Diferansiyel Tekdüzelik/Doğrusallık Frekans İnceleme Sonuçları 50
3.5 3 × 3 Boyutunda Optimal S-kutularının DLCTU Değeri ve Diferansiyel Tekdüzelik/Doğrusallık Frekans İnceleme Sonuçları 51
3.6 3 × 3 Boyutunda Optimal S-kutularının Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği İnceleme Sonuçları 51
3.7 3 × 3 Boyutunda 10 Kriptografik Özelliğe Göre En İyi Değerlere Sahip S-kutusu Örneği İncelemesi 52
3.8 3 × 3 Boyutunda 10 Kriptografik Özelliğe Göre En İyi S-Kutularının Bitslice Kapı Karmaşıklığı İnceleme Sonuçları 53
3.9 3 × 3 Boyutunda Literatürde Bulunan 4 Tane S-Kutusunun 10 Kriptografik Özelliğinin İncelenme Sonuçları 54

4 4 × 4 BOYUTUNDA İNVOLUTİF S-KUTULARININ KRİPTOGRAFİK ÖZELLİKLERİNİN İNCELEME SONUÇLARI 55

4.1 4 × 4 Boyutunda Optimal S-kutularının Sabit Nokta ve Doğrusal/Diferansiyel Dal Sayıları İnceleme Sonuçları 56
4.2 4 × 4 Boyutunda Optimal S-kutularının BIBO Örüntüsü İnceleme Sonuçları 57
4.3 4 × 4 Boyutunda Optimal S-kutularının Boomerang Bağlantı Tablosu Tekdüzeliği İnceleme Sonuçları 59
4.4 4 × 4 Boyutunda Optimal S-kutularının Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği İnceleme Sonuçları 61
4.5 4 × 4 Boyutunda Optimal S-kutularının DLCTU ve Diferansiyel Tekdüzelik/Doğrusallık Frekans İnceleme Sonuçları 62
4.6 4 × 4 Boyutunda Optimal S-kutularının BCTU Değeri ve Diferansiyel Tekdüzelik/Doğrusallık Frekans İnceleme Sonuçları 64
4.7 4 × 4 Boyutunda 10 Kriptografik Özelliğe Göre En İyi Değerlere Sahip S-kutusu Örneği İncelemesi 66
4.8 4 × 4 Boyutunda 10 Kriptografik Özelliğe Göre En İyi S-Kutularının Bitslice Kapı Karmaşıklığı İnceleme Sonuçları 66
4.9 4 × 4 Boyutunda Literatürde Bulunan 17 İnvolutif S-Kutusunun 10 Kriptografik Özelliğe Göre İncelenme Sonuçları 67

5 GENETİK ALGORİTMA İLE 5 × 5 BOYUTUNDA ELDE EDİLEN S-KUTULARININ KRİPTOGRAFİK ÖZELLİKLERİNİN İNCELENMESİ 71
5.1 5 × 5 Boyutunda Literatürde Bulunan 10 İnvolutif Olmayan S-Kutusunun Kriptografik Özelliklerinin İncelenme Sonuçları 75

6 SONUÇ VE GELECEK ÇALIŞMALAR 76
6.1 3 × 3 Boyutunda S-Kutularının Kriptografik Özelliklere Göre Karşılaştırmaları 77
6.2 4 × 4 Boyutunda S-Kutularının Kriptografik Özelliklere Göre Karşılaştırmaları 77
6.2.1 4 × 4 Boyutunda Sabit Nokta Sayısı 0 Olan Alt Grubun S-Kutularının Karşılaştırması 78
6.2.2 4 × 4 Boyutunda Sabit Nokta Sayısı 2 Olan Alt Grubun S-Kutularının Karşılaştırması 78
6.2.3 4 × 4 Boyutunda Sabit Nokta Sayısı 4 Olan Alt Grubun S-Kutularının Karşılaştırması 79
6.2.4 4 × 4 Boyutunda Sabit Nokta Sayısı 6 Olan Alt Grubun S-Kutularının Karşılaştırması 79
6.3 Bitslice Kapı Karmaşıklığı (Bitslice Gate Complexity) Karşılaştırma . . . 80

KAYNAKLAR 81

EKLER 86

A 3 × 3 BOYUTUNDA 10 KRİPTOGRAFİK ÖZELLİĞE GÖRE EN İYİ DEĞERLERE SAHİP 32 TANE S-KUTUSU 86

B 4 × 4 BOYUTUNDA 10 KRİPTOGRAFİK ÖZELLİĞE GÖRE EN İYİ DEĞERLERE SAHİP 384 TANE S-KUTUSU 88

ÖZGEÇMİŞ 97

SİMGELER DİZİNİ

α	Alfa
BGC	Bitslice Kapı Karmaşıklığı (Bitslice Gate Complexity)
β	Boomerang Bağlantı Tablosu (Boomerang Connectivity Table - BCT)
$BCTU$	Boomerang Bağlantı Tablosu Tekdüzeliği (Boomerang Connectivity Table Uniformity)
$\#\mathcal{U}$	Diferansiyel Tekdüzelik Frekansı (Frequency of Differential Uniformity)
$DLCTU$	Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği (Differential Linear Connectivity Table Uniformity)
$\#\mathcal{L}$	Doğrusallık Frekansı (Frequency of Linearity)
$\oplus$	eXclusive OR (XOR)
wt	Hamming Ağırlık (Hamming Weight)
$\bullet$	Nokta Ürünü (Dot Product)
$S(x)$	S-Kutusu (Substitution Box/S-box)
$S^{-1}(x)$	S-Kutusunun Tersi (Inverse of S-box)
$\#$	Toplam Sayısı (Number of)

KISALTMALAR DİZİNİ

AD	Algebraic Degree (Cebirsel Derece)
AES	Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
ANF	Algebraic Normal Form (Cebirsel Gösterim Biçimi)
BCT	Boomerang Connectivity Table (Boomerang Bağlantı Tablosu)
DBN	Differential Branch Number (Diferansiyel Dal Sayısı)
DDT	Difference Distribution Table (Fark Dağılım Tablosu)
DES	Data Encryption Standard (Veri Şifreleme Standardı)
DLCT	Differential Linear Connectivity Table (Diferansiyel Doğrusal Bağlantı Tablosu)
FP	Fixed Point (Sabit Nokta)
IoT	Internet of Things (Nesnelerin İnterneti)
LAT	Linear Approximation Table (Doğrusal Yaklaşım Tablosu)
LBN	Linear Branch Number (Doğrusal Dal Sayısı)
LFSR	Linear Feedback Shift Register (Doğrusal Geri Beslemeli Saklayıcı)
NIST	National Institute of Standars and Technology (Ulusal Standartlar ve Teknoloji Enstitüsü)
S-BOX	Substitution Box (Yer Değiştirme Kutusu)

ŞEKİLLER DİZİNİ

Şekil 2.1. Geri Beslemeli Saklayıcı Örneği 11
Şekil 2.2. Bijektif İnvolutif S-Kutusu Permütasyon Sayısı Hesabı 18
Şekil 4.1. 4 × 4 Boyutunda Optimal S-Kutuları Sabit Nokta ve Dal Sayılarının İncelenmesi 57

ÇİZELGELER DİZİNİ

Çizelge 2.1. $F_2^3 \rightarrow F_2$'ye Tanımlı Boole Fonksiyonu Cebirsel İfadesi 13
Çizelge 2.2. $F_2^4 \rightarrow F_2$'ye Tanımlı Boole Fonksiyonu Cebirsel İfadesi 13
Çizelge 2.3. $F_2^4 \rightarrow F_2$'ye Tanımlı İki Boole Fonksiyonunun Hamming Ağırlığının Hesaplanması 15
Çizelge 2.4. $F_2^4 \rightarrow F_2$'ye Tanımlı $f_4(x)$ Boole Fonksiyonunun Doğrusal Olmama Değer Hesabı Hazırlığı 16
Çizelge 2.5. $f_4(x)$ Boole Fonksiyonunun $F_2^4 \rightarrow F_2$'ye Tanımlı Bütün Doğrusal Fonksiyonlarına Olan Hamming Uzaklıkları 16
Çizelge 2.6. 4 × 4 Boyutunda Yer Değiştirme Kutusu (S-Kutusu) 17
Çizelge 2.7. 4 × 4 Boyutunda Involutif Yer Değiştirme Kutusu (S-Kutusu) 17
Çizelge 2.8. 4 × 4 Boyutlu 4 Sabit Noktalı S-Kutusu 19
Çizelge 2.9. 4 × 4 Boyutlu Sabit Noktasız S-Kutusu 19
Çizelge 2.10. 3 × 3 S-Kutusu 20
Çizelge 2.11. 3 × 3 S-Kutusunun LAT (2, 5) Değeri Hesaplaması 20
Çizelge 2.12. 3 × 3 S-Kutusu Doğrusal Yaklaşım Tablosu 21
Çizelge 2.13. Doğrusal Yaklaşım Tablosu Hesaplaması İçin 4-Bit Giriş 4-Bit Çıkış S-Kutusu 22
Çizelge 2.14. 4 × 4 Boyutlu S-Kutusunun LAT (7, 5) Değeri Hesaplaması 22
Çizelge 2.15. 4 × 4 Boyutlu S-Kutusunun Doğrusal Yaklaşım Tablosu (LAT) 23
Çizelge 2.16. 3 × 3 S-Kutusunun DDT (3, 5) Değeri Hesaplaması 24
Çizelge 2.17. 3 × 3 S-Kutusunun Fark Dağılım Tablosu 24
Çizelge 2.18. Fark Dağılım Tablosu Hesaplaması İçin 4 × 4 Boyutunda S-Kutusu . 25
Çizelge 2.19. 4 × 4 Boyutlu S-Kutusunun DDT (A, E) Değeri Hesaplaması 25
Çizelge 2.20. 4 × 4 Boyutlu S-Kutusunun Fark Dağılım Tablosu (DDT) 26
Çizelge 2.21. Piccolo Hafif Sıklet Blok Şifreleme S-Kutusu 27
Çizelge 2.22. Piccolo S-Kutusu Vektörel Çıkış Boole Fonksiyonları Cebirsel İfadesi 27
Çizelge 2.23. $F_2^4 \rightarrow F_2^4$'e Tanımlanan S-Kutusunun 1-1 Aktif Bit Tablosu 29

Çizelge 2.24. GIFT'in S-Kutusu 29
Çizelge 2.25. GIFT S-Kutusu BIBO DDT sayısı İncelemesi 30
Çizelge 2.26. GIFT S-Kutusu BIBO LAT Sayısı İncelemesi 30
Çizelge 2.27. 3 × 3 S-Kutusu Doğrusal Dal Sayısı İncelemesi 32
Çizelge 2.28. 3 × 3 S-Kutusunun Diferansiyel Dal Sayısı İncelemesi ($a = [0-3]$) 33
Çizelge 2.29. 3 × 3 S-Kutusunun Diferansiyel Dal Sayısı İncelemesi ($a = [4-7]$) 34
Çizelge 2.30. GIFT S-Kutusunun Diferansiyel Tekdüzelik Frekans İncelemesi . . . 37
Çizelge 2.31. GIFT S-Kutusu Doğrusallık Frekans Değer İncelemesi 39
Çizelge 2.32. Serpent_S0 S-Kutusu ve S-Kutusunun Tersi 40
Çizelge 2.33. Panda S-Kutusu 41
Çizelge 2.34. Panda S-Kutusu Fark Dağılım Tablosu 41
Çizelge 2.35. Panda S-Kutusu Boomerang Bağlantı Tablosu 42
Çizelge 2.36. KLEIN S-Kutusu 44
Çizelge 2.37. KLEIN S-Kutusunun Diferansiyel Doğrusal Bağlantı Tablosu 45
Çizelge 2.38. Bitslice Kapı Karmaşıklığı Hesaplamak İçin S-Kutusu 45
Çizelge 2.39. Bitslice Kapı Karmaşıklığı Hesaplamak İçin S-Kutusu Doğruluk Tablosu 46
Çizelge 3.1. 3 × 3 Boyutunda İnvolutif S-Kutularının En Büyük Fark Dağılım Tablosu ve En Büyük Mutlak Doğrusal Yaklaşım Tablosu Değerleri Karşılaştırılması 47
Çizelge 3.2. Fark Dağılım Tablosu, Doğrusal Yaklaşım Tablosu, Cebirsel Derece Açısından 3 × 3 Boyutunda İnvolutif S-Kutularının İncelenmesi . . . 48
Çizelge 3.3. 3 × 3 Boyutunda Optimal ve 2 Sabit Noktalı S-kutularının BIBO Örüntüsü İnceleme Sonuçları 49
Çizelge 3.4. 3 × 3 Boyutunda Optimal 2 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri İnceleme Sonuçları 50
Çizelge 3.5. 3 × 3 Boyutunda 2 Sabit Noktalı Optimal S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri ve Diferansiyel Tekdüzelik/Doğrusallık Frekanslarının İnceleme Sonuçları 50
Çizelge 3.6. 3 × 3 Boyutunda Optimal 2 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre DLCTU Değeri ve Diferansiyel Tekdüzelik/Doğrusallık Frekanslarının İnceleme Sonuçları 51
Çizelge 3.7. 3 × 3 Boyutunda 2 Sabit Noktalı Optimal S-kutularının BIBO Örüntü Gruplarına Göre DLCTU Değeri İnceleme Sonuçları 52
Çizelge 3.8. 3 × 3 Optimal S-Kutusu Örneği 53
Çizelge 3.9. 3 × 3 Boyutunda 10 Kriptografik Özelliğe Göre En İyi S-Kutularının Bitslice Kapı Karmaşıklığı Sonuçları 53

Çizelge 3.10. 3 × 3 Boyutunda 10 Kriptografik Özelliğe Göre En İyi ve Bitslice Kapı Karmaşıklığı En Az Olan S-Kutuları 53
Çizelge 3.11. 3 × 3 Boyutunda Literatürde Bulunan İnvolutif Olmayan 4 S-Kutusunun Kriptografik Özellikleri 54
Çizelge 4.1. 4 × 4 Boyutunda İnvolutif S-Kutularının En Büyük Fark Dağılım Tablosu ve En Büyük Mutlak Doğrusal Yaklaşım Tablosu Değerleri Karşılaştırılması 55
Çizelge 4.2. Fark Dağılım Tablosu, Doğrusal Yaklaşım Tablosu, Cebirsel Derece Açısından 4 × 4 Boyutunda S-Kutularının İncelenmesi 56
Çizelge 4.3. 4 × 4 Boyutunda Optimal ve 0 Sabit Noktalı S-kutularının BIBO Örüntü İnceleme Sonuçları 57
Çizelge 4.4. 4 × 4 Boyutunda Optimal ve 2 Sabit Noktalı S-kutularının BIBO Örüntü İnceleme Sonuçları 58
Çizelge 4.5. 4 × 4 Boyutunda Optimal ve 4 Sabit Noktalı S-kutularının BIBO Örüntü İnceleme Sonuçları 58
Çizelge 4.6. 4 × 4 Boyutunda Optimal ve 6 Sabit Noktalı S-kutularının BIBO Örüntüsü İnceleme Sonuçları 58
Çizelge 4.7. 4 × 4 Boyutunda Optimal 0 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri İnceleme Sonuçları 59
Çizelge 4.8. 4 × 4 Boyutunda Optimal 2 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri İnceleme Sonuçları 60
Çizelge 4.9. 4 × 4 Boyutunda Optimal 4 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri İnceleme Sonuçları 61
Çizelge 4.10. 4 × 4 Boyutunda Optimal 6 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri İnceleme Sonuçları 62
Çizelge 4.11. 4 × 4 Boyutunda Optimal 2 Sabit Noktalı S-kutularının DLCTU değerinin 8 Olduğu BIBO Örüntü Gruplarına Göre Diferansiyel Tekdüzelik/Doğrusallık Frekanslarının İnceleme Sonuçları 63
Çizelge 4.12. 4 × 4 Boyutunda Optimal 4 Sabit Noktalı S-kutularının DLCTU Değerinin 8 Olduğu BIBO Örüntü Gruplarına Göre Diferansiyel Tekdüzelik/Doğrusallık Frekanslarının İnceleme Sonuçları 64
Çizelge 4.13. 4 × 4 Boyutunda Optimal 2 Sabit Noktalı BCTU Değerinin 10 Olduğu S-Kutularının BIBO Örüntülerine Göre Diferansiyel Tekdüzelik/Doğrusallık Frekanslarının İnceleme Sonuçları 65
Çizelge 4.14. 4 × 4 Boyutunda Kriptografik Özelliklere Göre En İyi S-Kutularının Bitslice Kapı Karmaşıklığı Sonuçları 67

Çizelge 4.15. 4 × 4 Boyutunda 10 Kriptografik Özelliğe Göre En İyi ve Bitslice Kapı Karmaşıklığı En Az Olan S-Kutuları (İlk 20) 68
Çizelge 4.16. 4 × 4 Boyutunda 10 Kriptografik Özelliğe Göre En İyi ve Bitslice Kapı Karmaşıklığı En Az Olan S-Kutuları (Son 28) 69
Çizelge 4.17. 4 × 4 Boyutunda Literatürde Bulunan İnvolutif 17 S-Kutusunu Kriptografik Özellikleri 70
Çizelge 5.1. 5 × 5 Boyutunda S-Kutusu-1 73
Çizelge 5.2. 5 × 5 Boyutunda S-Kutusu-2 74
Çizelge 5.3. 5 × 5 Boyutunda Literatürde Bulunan 10 İnvolutif Olmayan S-Kutusunun Kriptografik Özelliklerinin İncelenmesi 75

BÖLÜM 1

GİRİŞ

1.1 Kriptografi

Resim, sayısal metin, akan görüntü, dosya ve farklı formattaki verilerin orjinal hallerine çeşitli işlemler uygulayarak anlaşılmaz hale getirilmesine *Kriptografi* denilmektedir (Buchmann, 2004). Orjinal halinde bulunması istenmeyen, diğer bir deyişle olası saldırılara karşı korunması istenen veriler, kriptografik yöntemler ile şifreleme işlemlerinden geçirilmektedir. Kriptografide amaç, verinin güvenliğini sağlamaktır (Menezes, Van Oorschot & Vanstone, 2018). Güvenilirliği sağlayan ölçütler; verinin gizli kalması, bütünlüğünün zarar görmemesi ve kullanılabilirliğini sürdürmesidir (Sklavos & Zaharakis, 2016). Kriptografik yapılar ile veriler şifrelenmektedir. Saldırgan, şifrelenmiş olan verinin iletildiği ağı izleyebilmekte veya analiz edebilmektedir (Shree, Ahlawat vd., 2017). Bu durumlarda şifrelenmiş olan veri, gizliliğini korumalıdır. Kriptografik yapılar ile anlaşılamaz/okunamaz hale getirilen verilerin, her koşulda tutarlı halde olması gerekmektedir. Saldırgan, veri üzerinde değişiklik yapmaya çalışabilir, ağ trafiğinde sahte işlemler yaparak veri bütünlüğünü hedef alan saldırılarda bulunabilmektedir (Dutta, Ghosh & Bayoumi, 2019). Bu durumlarda güvenliğin hedeflerinden olan, veri bütünlüğü zarar görebilmektedir. Ayrıca saldırganlar; veriye, veri trafiğine veya sistemlere; servislerin durması, yavaşlaması veya ele geçirilmesi yönünde ataklar/saldırılar yaparak kullanılabilirliğe zarar verebilmektedirler (Shree, Ahlawat vd., 2017). Kriptografi ile gizlilik, bütünlük ve kullanılabilirlik gibi güvenlik hedeflerinin sağlanması amaçlanmaktadır.

1.2 Bilgi Güvenliği Açısından Kriptografi

Bankacılık numaralarının korunması, mesajların korunması, doğru şekilde ileti gönderimi gibi konular bilginin gizliliği ve güvenliği kavramlarıyla ilişkilidir (Sharma vd., 2017). Verinin gizliliği sağlandığı sürece, veri/bilgi güvenliği de sağlanmaktadır.

Bilgisayarların gelişmesi ve İnternet'in oluşması ile bilgi güvenliği önem arz etmektedir. İnternet, yapısı itibari ile güvenliği sağlamak için tasarlanan bir yapı olmadığı için kriptografi son derece önemli hale gelmiştir (Smith, 1997).

Kriptografiye hedefleri kapsamında; gizlilik, bütünlük, reddedilemezlik, kimlik denetimi özelliklerince ihtiyaç duyulmaktadır. Bilgi güvenliğinin sağlanması için kriptografi kullanılmaktadır (Sharma vd., 2017). Kriptografi, ispatlanabilir bilgi güvenliği sağlaması açısından, temel yapı taşı konumundadır. Bilgi güvenliğinin tamamını oluşturmasa da, kriptografi matematiksel olarak ispatlanabilecek güvenliği sağlamaktadır.

1.3 NIST - Hafif Sıklet Kriptografi

NIST (National Institute of Standards and Technology) belirli zamanlarda, ihtiyaç durumlarında kriptosistemler üzerine yarışmalar açmaktadır (Nist, 2023). Boyut ve enerji bakımından sınırlı kapasitesi olan sensör cihazlar, akıllı kartlar, RFID etiketler yaygın olarak kullanılmaktadır. Bu cihazlara üçlü DES (Data Encryption Standard (Veri Şifreleme Standardı)) veya AES (Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)) gibi büyük yer kaplayan (alan karmaşıklığı açısından büyük) algoritmaların çalıştırılması fiziki yetersizlik sebeplerinden dolayı mümkün olmamaktadır (Bhanot & Hans, 2015). İhtiyaç duyulan durum; sınırlı kaynak kullanımı ve hızı yüksek kriptografik yapı kurulmasıdır. NIST'in temel amacı, bu ihtiyaçlara uygun şekilde hız ve güvenliği temellendirerek **standartlaştırma** ortaya konulmasını sağlamaktır. NIST'in yaptığı yarışmanın sonucunda (Center, 2023), ASCON standartlaşma için yarışmayı kazanan algoritma olmuştur (Turan vd., 2023).

1.4 Kriptografik Sitemin Bileşenleri

Kriptografik sistemleri ifade ederken, bazı bileşenler kullanılmaktadır. Bunlar: Anahtar, Açık Metin, Şifreleme ve Şifre Çözme şeklindedir. Tez kapsamında, sıklıkla kullanılan bu kavramların açıklamaları; bu bölümün devamında, alt bölümler şeklinde sunulmaktadır.

1.4.1 Anahtar (Key)

Kriptografik bir sistemin en önemli parçalarından biridir (Hellman, 2002). Simetrik şifrelemede tek bir anahtar ile şifreleme ve şifre çözme yapılırken, asimetrik şifrelemede her iki işlem için ayrı anahtarlar kullanılır (Al-Shabi, 2019). Asimetrik veya simetrik şifrelemede, gizlilik anahtarın gizliliği ile ilintilidir. Anahtarlar, güvenliğin en önemli kısmı olduğundan dolayı yeteri uzunlukta ve karmaşıklıkta olması gerekmektedir.

1.4.2 Açık Metin (Plaintext)

Şifrelemenin yapılacağı metin veya yapıdır. Kullanılacak anahtar ile gerekli işlemlerden geçirilerek, şifreli metin elde edilmiş olur. Genellikle okunabilirliği olduğu için açık metinler, bilinmezliği ve entropisi daha düşük hallerdedirler (Canard, Pointcheval, Santos & Traoré, 2018). Açık metinlere göre, entropisi yüksek ve rastgeleliği olan şifreli metinler, sıkıştırma yapmaya daha uygundurlar.

1.4.3 Şifreleme (Encryption)

Açık metnin anahtar ile işlemlerden geçirilip şifreli metin hale dönüştürülmesinin bütününe şifreleme (encryption) denilmektedir (Mushtaq vd., 2017). İşlemlerin sonucunda okunabilirliği ve anlaşılabilirliği çok daha düşük olan çıktılar elde edilmiş olmaktadır.

1.4.4 Şifre Çözme (Decryption)

Şifreli metnin anahtar ile işleme sokulup açık metnin elde edilmesinin bütünüdür. Şifreleme sistemlerine göre anahtarın yapısı değişiklik göstersede her halükarda, şifre çözme işleminde anahtar kullanılmaktadır (Mushtaq vd., 2017).

1.5 Kriptoanaliz

Bilgilerin güvenilirliği; transferinde, depolanmasında, işlenmesinde ve çeşitli işlemler için gereklidir (Sharma vd., 2017). Güvenilirliği sağlamak için matematiksel yöntemler ve işlemler ile verilerin şifrelenmesi, kriptografinin alanına girerken; kriptografik yapıların saldırılara karşı direncinin incelenmesi *Kriptoanaliz* bilimine girmektedir (Tiwari, Nandi & Mishra, 2013). Kriptoanaliz incelemeler ile şifrelenmiş olan verinin, saldırılara karşı dayanıklılığı saptanmaktadır. Bu nedenle, kullanılan şifreleme algoritması veya yapısının güçlü ve zayıf yönleri belirlenebilmektedir. Kriptoanaliz incelenmeleri sonucunda şifrelemenin, saldırılara karşı açık/zayıf yönleri ortaya koymak için önemlidir (Blondeau & Nyberg, 2013).

Kriptoanaliz incelemeler, saldırı modellerini temel almaktadırlar. Bu modeller:

yalnızca şifreli metin saldırısı, bilinen açık metin saldırısı, seçilmiş açık metin saldırısı, seçilmiş şifreli metin saldırısı ve seçilmiş başlatma vektörü saldırısı şeklinde olmaktadır (Stinson, 2005). Saldırı modelleri aşağıdaki şekilde listelenmiştir (Tuncay, 2021).

- **Yalnızca Şifreli Metin Saldırısı**: Saldırganın, sadece metinlerin şifreli hallerine ulaşabildiği saldırı modelidir.
- **Bilinen Açık Metin Saldırısı**: Saldırganın, aynı anahtar ile şifrelenen açık - şifreli metin 2'li gruplarına erişmektedir.
- **Seçilmiş Açık Metin Saldırısı**: Saldırgan, seçtiği açık metinlerin şifreli hallerine ulaşabilmektedir. Saldırganın şifreli hallerine ulaşabilmesinin sebebi, şifreleme cihazına erişiminin olmasından kaynaklanmaktadır.
- **Seçilmiş Şifreli Metin Saldırısı**: Saldırganın; seçmiş olduğu şifreli metinlerin, şifrelerinin çözülmüş haline ulaşabildiği saldırı modelidir. Diğer bir deyişle, saldırgan şifre çözme cihazına ulaşabilmektedir.
- **Seçilmiş Başlatma Vektörü Saldırısı**: Şifreleme yapısına uygun olarak belirlenmiş olan başlangıç vektörü (Initialization Vector) ve şifresi çözülmüş metinlere ulaşabilen saldırgan tarafından, şifreli metinlere ulaşılabilecek olan saldırı modelidir.

Tespit edilen açık noktalardan, saldırı modelleri uygulanarak, verinin orjinal haline erişimini sağlamak için denemelerde bulunulmaktadır. Diğer bir deyişle kriptoanaliz sayesinde, kriptografik yapıların güvenilirliği test edilip incelenmiş olmaktadır. Şifrelemede algoritmanın bilindiği, kullanılan anahtarın gizli olduğu kabul edilmektedir (Petitcolas, 2023). Çünkü anahtar bilinirse, algoritma zaten bilinmekte olduğu için veriye ulaşılabilmektedir. Kriptoanaliz ile kriptografik yapının incelenmesi amaçlanmaktadır (Jiao, Lei, Gao, Xie & Yuan, 2019).

1.5.1 Doğrusal Kriptoanaliz

Kriptografik yapılar kullanılarak şifrelenmiş olan metin/veri/görüntülerin, istatiksel olarak yapılan saldırılarla incelenmesine *Doğrusal Kriptoanaliz* denilmektedir (Bao, Guo, Ling & Sasaki, 2019). Açık metnin, şifreli metne çevrilmesindeki doğrusal olma değeri arttıkça, doğrusal kriptoanaliz ile şifrenin kırılması kolaylaşmaktadır (S. Kim, Hong, Sung & Hong, 2020). Bu sebeple şifrelemede doğrusal olmama değeri yüksek olan yer değiştirme kutuları kullanılarak, doğrusal kriptoanalize dayanıklı şifrelenmiş yapılar oluşturulmaya çalışılmaktadır (M. Liu, Lu & Lin, 2021). S-kutularına ($m \times m$

boyutunda bijektif) doğrusal kriptoanaliz yapılırken **bias (sapma) değeri** ϵ hesaplaması, $(2^m - 1)(2^m - 1)$ tane doğrusal durum değerlendirilerek, yüksek$(+/-(1/2))$ olanlar belirlenerek (Sağıroğlu vd., 2019) doğrusal kriptoanaliz saldırısı yapılma durumu analiz edilmektedir (M. Liu vd., 2021). S-kutusunun, belirlenen ifadeye göre gerçekleşme olasılığı p olmaktadır. Olasılık değeri, yer değiştirme kutusunun bütün giriş ve çıkş bitlerine göre ortaya konulan doğruluk tablosuna göre hesaplanmaktadır. Bu durumda sapma değeri: $\epsilon = p - (1/2)$ olmaktadır (Sağıroğlu vd., 2019). Bu değerin incelenmesi ile saldırı yapılabilecek noktalar tespit edilerek, şifreleme yapısı incelenmektedir (Y. Liu, Sun & Li, 2021).

Doğrusal kriptoanaliz ile birlikte, Doğrusal Yaklaşım Tablosu'ndan (Linear Approximation Table) elde edilen değer (0, 0 konumu dışındaki en büyük mutlak değer) kullanılarak şifrelemenin doğrusal kriptoanalize dayanıklı olacağı döngü sayısı belirlenmektedir (Chen, Gong, Tang & Dong, 2022). Bunun için öncelikle en büyük Doğrusal Olasılık (Linear Probability - LP) Eşitlik 1.1 şeklinde hesaplanmaktadır:

$$LP_{Algoritma-max} = (((2^{m-1} + (MaxLAT))/2^{m-1}) - 1)^2 \quad (1.1)$$

Hesaplanan Eşitlik 1.1 de aktif S-kutuları hesaplamaya katıldığında Eşitlik 1.2 haline dönüşmektedir (Li, Liu, Guo & Liu, 2022):

$$LP_{Algoritma-max}^{AktifS-Kutusu} < 2^{-(m-1)} \quad (1.2)$$

Anlaşılacağı üzere, Eşitlik 1.2 de eşitliğini sağlayan ilk döngü durumunda, doğrusal kriptoanalize dayanıklı minimum döngü sayısı tespit edilmiş olmaktadır (Sağıroğlu vd., 2019).

1.5.2 Diferansiyel Kriptoanaliz

Doğrusal yapıda olmayan yer değiştirme kutularının **diferansiyel farklarının** incelenmesi ile analiz edilmesidir (M. Liu vd., 2021). S-kutusundan oluşturulan DDT (Difference Distribution Table - Fark Dağılım Tablosu) diferansiyel kriptoanaliz de aktif olarak kullanılmaktadır (Bao vd., 2019). Ayrıca diferansiyel kriptoanaliz için seçilen açık metin ve şifreli metinlere ihtiyaç duyulmaktadır. Gerekli olan metin çiftlerinin sayısını belirlemek için öncelikle diferansiyel incelemenin olasılık (p) değeri gerekmektedir. S-kutusunun doğruluk tablosundaki elemanlardan, a giriş, b çıkış farkı olduğu durumda, $S(x) \oplus S(x \oplus a) = b$ şeklinde eşitliği sağlayan durumlara göre p olasılık değeri hesaplanmaktadır (S. Kim vd., 2020). Sabit olarak c alındığında gerekli metin çifti sayısı

Eşitlik 1.3 şeklinde ifade edilmektedir (Sağıroğlu vd., 2019):

$$c/p \tag{1.3}$$

S-kutularında, diferansiyel kriptoanalize karşı güçlü olması için aktif yer değiştirme kutusunun sayısı önemli faktördür. Sayı arttıkça, şifrenin diferansiyel kriptoanalize karşı dayanıklılığı artmaktadır (Sağıroğlu vd., 2019). Aktif yer değiştirme kutusunun en küçük değeri bilindiği durumda, $m \times m$ boyutunda S-kutusunun Diferansiyel Olasılık (Differential Probability - DP_S) karşı dayanıklılığı Eşitlik 1.4 şekilde hesaplanmaktadır:

$$DP_S(a, b) = \#\{S(x) \oplus S(x \oplus a) = b\}/2^m \tag{1.4}$$

Eşitlik 1.4'te; $S(x) \oplus S(x \oplus a) = b$ eşitliğini sağlayan toplam elemanların sayısının (#) 2^m'e bölümünün sonucunun diferansiyel olasılık değerine eşit olduğu ifade edilmiştir.

1.6 Simetrik Şifreleme Algoritmaları

Şifreleme algoritmalarında amaç; açık metni, anahtar ile bir dizi matematiksel işlemlerden geçirerek, şifreli hale getirmektir. *Kreckhoff Prensibi'nde* belirtildiği gibi, şifrelemede kullanılan algoritma gizli olmamalı, sadece kullanılan anahtarın gizli olması gerekmektedir (Petitcolas, 2023). Simetrik şifrelemede, açık metnin (plaintext) şifrelendiği anahtar ile şifreli metnin (ciphertext) şifresinin çözüldüğü anahtar aynıdır. Diğer bir deyişle gizli olan tek anahtarın, şifreleme işlemi yapan ve şifreyi çözen taraflarca gizli tutulması gerekmektedir. Şifrelenecek olan veri x olarak tanımlanırsa, şifreleme algoritması E_k, şifre çözme algotiması da D_k şeklinde belirtildiğinde, aynı gizli anahtar ile şifreleme ve şifre çözme yapısı Eşitlik 1.5 şeklinde formülüze edilmektedir:

$$D_k(E_k(x)) = x \tag{1.5}$$

Şifrelemede gönderici, göndermek istediği veriyi belirlenen algoritma ve gizli anahtarı ile şifreleyerek alıcıya iletmektedir. Alıcı da kendisinde var olan gizli anahtar ile bilinen algoritmayı kullanarak şifreyi çözmektedir. Simetrik şifrelemede, anahtarın gizli kalması ve saldırılara karşı dayanıklı olması gerekmektedir. Gönderici ve alıcı tarafından, şifreleme anahtarının paylaşılması gerekmektedir (Sağıroğlu vd., 2019).

1.7 Blok Şifreleme Algoritmaları

Akan şifrelerdeki gibi blok şifreler de simetrik anahtarlı kripto sistemlerdir. Şifreleme ve şifre çözme işlemileri aynı anahtar ile yapılmaktadır (Sağıroğlu vd., 2019). Blok şifrelerde; açık metni, n tane döngüde karmaşıklaştırmak için S-kutuları

ve doğrusal dönüşümler kullanılmaktadır. Döngüler işletilerek açık metin, şifreli metin haline getirilmektedir (Jangra & Singh, 2022).

Simetrik şifreleme algoritması uygulanırken, açık metindeki verilerin, **bloklar** halinde şifrelenmesi durumunda *Blok Şifreleme Algoritması* kullanılmaktadır (Sağıroğlu vd., 2019). Gönderici ve alıcıda aynı olarak bulunan gizli diğer bir deyişle simetrik anahtar ile açık metin, n bit uzunluğunda bloklar ile şifrelenmektedir. Şifre çözme işlemi yapılırken de aynı şekilde, şifrelendiği blok uzunluğu ile (n) şifre çözme işlemi yapılmaktadır. Eğer ki şifrelenecek olan veri n bit uzunluğundan küçük kalırsa, n bit uzunluğuna ulaştırmak için bloğa bit eklemeleri yapılmaktadır. Kullanılan n değeri algoritmaya, yaklaşıma, ihtiyaca göre değişkenlik gösterebilirken; genellikle **64, 128, 256, 512** bit uzunluklu bloklar seçilmektedir (Sağıroğlu vd., 2019). Şifrelenecek olan veri bloklara bölündükten sonra, bloklardaki bit değerlerine permütasyon, yer değiştirme işlemleri uygulanmaktadır. Blok şifrelemelerde temel olarak, yayılma ve karıştırma yaklaşımları uygulanmaktadır (Bahceci & Özkaynak, 2020). Karıştırmada; haritalama işlemi, yer değiştirme kutuları kullanarak uygulanmaktadır. S-kutularında, verinin farklı değerlere yönlendirilmesi/haritalanması yapılırken, aynı girdi değerlerinin aynı çıktı değerlerine haritalanması durumları oluşabileceği için karıştırmanın yanında yayılmanın da kullanılması gerekmektedir.

Modern blok şifrelemelerde kullanılan Permütasyon Kutuları (P-Kutuları) ile bitler farklı konumlara haritalanarak, yerleri değiştirilmektedir (Mousavi & Sadeghiyan, 2021). Olası permütasyon durumlarına göre giriş bitlerini, çıkış bitlerine yönlediren P-kutuları; doğrudan, genişleme ve sıkıştırma olarak 3 gruba ayrılmaktadır. Doğrudan P-kutuları giriş biti kadar çıkış bitine haritalamanın yapıldığı durumlardır. Genişletmede; çıkış bitleri, giriş bitlerinden fazla, sıkıştırmada; giriş bitleri çıkış bitlerinden daha fazla olacak şekilde tasarlanmıştır. Genişletme ve sıkıştırma permütasyon kutularının tersleri olmamaktadır. Diğer bir deyişle permütasyon kutusundan geçirilen bitler ters işlem ile orjinal haline gelememektedir. Doğrudan P-kutularının tersi vardır.

Blok şifrelemenin önemli bir bileşeni olan diğer elemanı da *Yer Değiştirme Kutularıdır (S-Kutuları)*. Blok şifrelemede kullanılmasının önemi, **doğrusal olmamalarındandır** (S. Kim vd., 2020). Genellikle şifrelemelerde doğrusal olmayan tek yapı olarak S-kutuları kullanılmaktadır (Li vd., 2022). Bu özelliği ile şifrelemenin güvenliğinde, yer değiştirme kutuları önemli rol oynamaktadır. Yer değiştirme kutusunun $n \times n$ boyutunda olması ve aynı zamanda birebir, örten özellikleri barındırması halinde bijektif olduğu anlamına gelmektedir (Jangra & Singh, 2022). S-kutuları oluşturulurken; rastgele, sezgisel veya cebirsel şeklilde oluşturulabilmektedirler. Aktif olarak tasarlanılan ve kullanılan S-kutuları sonlu cisimlerde, üssel haritalama ile *cebirsel* olarak oluşturulmaktadır

(Sağıroğlu vd., 2019). Sonlu cisimlerde üssel işlemler için tersi alma şeklinde kullanılmaktadır. Yer değiştirme kutuları sonlu cisim üzerinde tanımlanırsa, indirgenemez polinomlar kullanılmaktadır. Ters alma işlemi; sonlu cisimlerde kullanıldığı durumlarda, S-kutusunun kullanıldığı blok şifrelemenin doğrusal ve diferansiyel kriptoanalize karşı dayanıklılığını arttırmaktadır (Saarinen, 2012). AES şifreleme döngülerinin ilk aşaması olan **SubBytes** dönüşümünde; $x^8 + x^4 + x^3 + x + 1$ indirgenemez polinomu ve $x \rightarrow x^{-1}$ haritalaması ile oluşturulan yer değiştime kutusu kullanılmıştır (Jangra & Singh, 2022).

Blok şifrelemede doğrusal yapıda olmayan S-kutuları, genellikle doğrusal dönüşümler ile bir arada kullanılarak, şifrelemenin yayılımı sağlanmaktadır. XOR ($\oplus$) işlemi, şifrelemede aktif kullanılmaktadır. XOR ($\oplus$) işlemi; doğruluk tablosuna göre, 2 durumun farklı olmasında 1 aynı olmasında 0 sonucunu veren işlemdir. Diğer bir deyişle $1 \oplus 1 = 0, 0 \oplus 0 = 0, 1 \oplus 0 = 1$ ve $0 \oplus 1 = 1$ şeklindedir. Ayrıca parçalı olarak yer değiştirme, öteleme gibi işlemlerde blok şifrelemede kullanılan tekniklerdendir.

Döngüsel olarak blok şifreleme yapıldığında, ürün şifresi haline gelmektedir (Jangra & Singh, 2022). Şifreleme standartlarından olan AES, şifrelemesini bloklar ile gerçekleştirmektedir (Nechvatal vd., 2001). Her blok 16 byte içermektedir. AES, şifrelemesini yaparken 128 bit uzunluğunda bloklara ayırarak işlemlerini gerçekleştirmektedir (Bao vd., 2019). Tekrar sayısı olan 10 olduğu için, 10 döngüde şifrelemeyi tamamlamaktadır. Anahtar uzunluğuna göre dögü sayısı değişiklik göstermektedir. Her döngü (son döngü hariç) 4 aşamadan oluşmaktadır. Bunlar: SubBytes, ShifRows, MixCloumn, AddRoundKey şeklindedir (Jangra & Singh, 2022). *SubBytes* içerinde AES'e ait olan S-kutusuna göre dönüşüm gerçekleştirilmektedir. *ShiftRows* aşamasında, 4 byte uzunluğunda olan kelimelere (word) gerekli dairesel öteleme işlemi yaptırılmaktadır. *MixCloumn* aşamasında, bit bazında, MDS (Maximum Distance Separable - Maksimum Uzaklıkta Ayrılabilen) matris ile kelime çarpımı yapılmaktadır. *AddRoundKey*'de şifreleme anahtarı, planlamaya uygun olarak gerekli matematiksel işlemlerden geçirilmektedir (Sağıroğlu vd., 2019). Bu işlem döngü sayısı kadar tekrar ettikçe blok şifreleme uygulanmış olmaktadır.

1.8 Tezin Amacı, Önemi ve Ana Hatları

Hafif sıklet şifrelemenin yaygın olarak kullanıldığı IoT cihazları, modern teknoloji dünyamızın ayrılmaz bir parçası haline gelmiştir. IoT cihazlarının İnternet bağlantısı sağlaması, kendi aralarında veri aktarması ve istenilen komutların çalıştırılması durumunda şifreleme ile gizlilik sağlanmaktadır. Bu nedenle hafıza kapasitesi/güç kaynağı kısıtlı olan cihazlarda kullanılabilecek, hafif sıklet şifreleme yapılarına ihtiyaç duyulmaktadır. Sınırlı kaynaklar kullanan hafif sıklet şifrelemelerde, şifrelemenin

doğrusal olmamasını sağlayan tek katman S-kutularıdır (Jangra & Singh, 2022). S-kutuları için doğrusal olmama durumu kritik olmasına rağmen, diğer iyi kriptografik özelliklere sahip olan S-kutuları kriptanaliz yöntemlerine karşı daha dayanıklı hale gelmektedir. İyi kriptografik özelliklere sahip S-kutuları seçilirse, hafif sıklet blok şifreler de saldırılara karşı daha dayanıklı hale gelmektedir.

Belirtilen durumlar dikkate alındığında bu çalışmanın temel amacı; hafif sıklet blok şifrelemede kullanılacak 3×3 ve 4×4 boyutunda, involutif S-kutularını seçerken, 10 kriptografik özelliği inceleyerek mümkün olan en iyi değerlere sahip olan S-kutuları seçimlerini ortaya koymaktır. İncelenen kriptografik özellikler şunlardır: En yüksek Fark Dağılım Tablosu değeri (Tablodaki (0, 0) konumu hariç), En yüksek mutlak Doğrusal Yaklaşım Tablosu değeri (Tablodaki (0, 0) konumu hariç), Cebirsel Derece, BIBO Örüntüsü, Doğrusal Dal Sayısı, Diferansiyel Dal Sayısı, Doğrusallık Frekansı, Diferansiyel Tekdüzelik/Uniformity Frekansı, Boomerang Bağlantı Tablosu Tekdüzeliği/Uniformity, Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği'dir (Bao vd., 2019). S-kutuları incelenmiş ve *Sabit Nokta* sayıları da hesaplanmıştır. Ancak sabit nokta sayısı kriptografik özelliklere dahil edilmemiştir.

Tez kapsamında yapılan incelemelerin önemi; 3×3 ve 4×4 boyutunda tüm involutif, S-kutusu permütasyonlarının kriptografik özelliklerini analiz etmek, aynı zamanda 5×5 boyutunda genetik algoritma ile bulunan involutif, en büyük Fark Dağılım Tablosu, en büyük mutlak Doğrusal Yaklaşım Tablosu ve cebirsel derece açısından iyi değerlere sahip olan S-kutularını sunmak ve kriptografik özelliklerini analiz etmektir. 10 kriptografik özelliğe göre iyi değerlere sahip olan S-kutularının, vektörel çıkış Boole fonksiyonları optimizasyon işleminden geçirilmeden bitslice kapı karmaşıklığı hesaplanmıştır.

Tez çalışması altı bölümden oluşmaktadır. Bölüm 1'de kriptografi ile ilgili genel terimler, doğrusal/diferansiyel kriptoanaliz yöntemleri ve şifreleme algoritmaları açıklanmıştır. Bölüm 2'de tez için gerekli matematiksel altyapı verilmiştir. Bölüm 2'de verilen matematiksel altyapı; kriptografik özellikler, Boole fonskiyonları ve bitslice kapı karmaşıklarını açıklamaktadır. Bölüm 3 ve 4'te sırasıyla; 3×3 ve 4×4 boyutunda incelenen S-kutularının kriptografik özelliklerinin analizleri ve karşılaştırmaları sunulmuştur. Bölüm 5'te genetik algoritma ile elde edilen 5×5 boyutunda; en büyük Fark Dağılım Tablosu değeri, en büyük mutlak Doğrusal Yaklaşım Tablosu ve cebirsel derece açısından iyi özelliklere sahip olan S-kutuları sunulmuş ve bunların diğer kriptografik özelliklerinin inceleme sonuçları tespit edilmiştir. Tez çalışmasının son ve altıncı bölümünde, incelenen S-kutularının kriptografik özelliklerinin karşılaştırılması sunulmuştur.

BÖLÜM 2

MATEMATİKSEL ALTYAPI

Tezin bu bölümünde, tez çalışması için gerekli matematiksel altyapı ve tez kapsamında incelenen S-kutuları için kriptografik özelliklerin bir incelemesine yer verilmiştir. Bu bölüm içerisinde verilen kriptografik özelliklere, açıklamalara ve ifadelerin ispatlarına; Sağıroğlu vd. (2019), Bao vd. (2019), Bar-On, Dunkelman, Keller Weizman (2019), Cid, Huang, Peyrin, Sasaki Song (2018), M. Liu vd. (2021) ve Lu, Mesnager, Cui, Fan Wang (2022) kaynaklarından ulaşılabilmektedir.

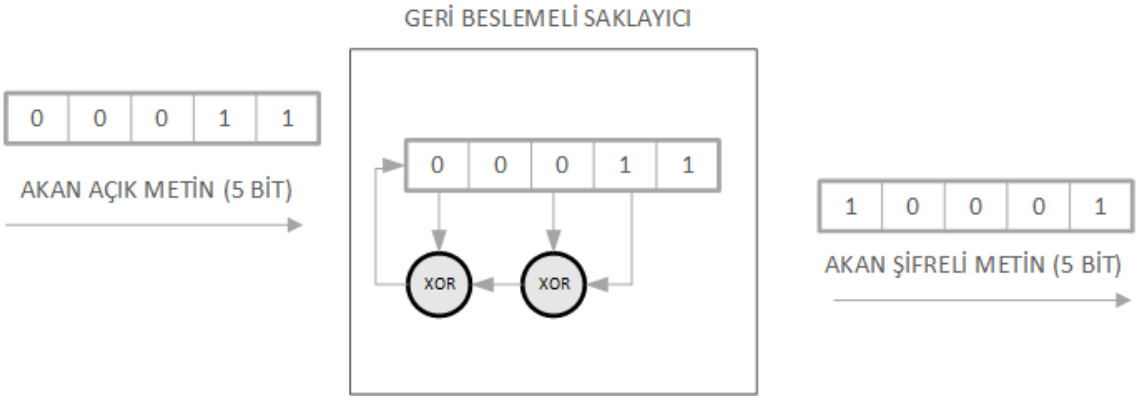
Kriptografide kullanılan toplama (+) ve çarpma ($\cdot$) ikili işlemlerinin, F kümesinde sağlayabileceği aksiyomlar takip edildiği şekilde özetlenebilir (Tuncay, 2021):

1. *Kapalılık*: $a, b \in F$ ise $a + b \in F$ ve $a \cdot b \in F$ olmaktadır.
2. *Değişme*: $a, b \in F$ ise $a + b = b + a$ ve $a \cdot b = b \cdot a$ olmaktadır.
3. *Birleşme*: $a, b, c \in F$ ise $(a + b) + c = a + (b + c)$ ve $(a \cdot b) \cdot c = a \cdot (b \cdot c)$'dir.
4. *Dağılma*: $a, b, c \in F$ ise $a + (b + c) = a + b + a + c$ ve $a \cdot (b \cdot c) = a \cdot b \cdot a \cdot c$'dir.
5. *Toplama (+) İşleminde Birim/Etkisiz Eleman*: Her $a \in F$ için $a + e = e + a = a$ olan bir $e \in F$ bulunmaktadır.
6. *Çarpma ($\cdot$) İşleminde Birim/Etkisiz Eleman*: Her $a \in F$ için $a \cdot e = e \cdot a = a$ olan bir $e \in F$ bulunmaktadır.
7. *Toplama (+) İşleminde Ters Eleman*: Her $a \in F$ için $a + a' = e$ ve $a' + a = e$ olan bir $a' \in F$ bulunmaktadır.
8. *Çarpma ($\cdot$) İşleminde Ters Eleman*: Her $a \in F$ için $a \cdot a' = e$ ve $a' \cdot a = e$ olan bir $a' \in F$ bulunmaktadır.

Bir F kümesinde; $1-4$ aralığındaki aksiyomların, sadece toplama (+) işlemi üzerinde gerçekleştiği cebirsel yapılara, **grup** adı verilmektedir (Forouzan, 2008). Hem $1-4$ aralığındaki aksiyomları, toplama (+) ve çarpma ($\cdot$) ikili işlemlerinde sağlayan hem de $5-7$ aralığındaki 3 aksiyomu sağlayan (çarpma işleminde ters eleman hariç) F kümesine **halka** denir (Galbraith, 2012). Tüm aksiyomları sağlayan cebirsel yapı, **cisim** olarak ifade edilir (Sağıroğlu vd., 2019). Cismin, sonlu sayıda eleman bulundurması haline **sonlu cisim** denilmektedir (Tuncay, 2021).

2.1 Boole Fonkiyonları

Kriptografik işlemlerde *Boole Fonksiyonları*, çok sayıda simetrik şifreleme yapılarının tasarımında kullanılmaktadır (Sağıroğlu vd., 2019). Akan şifrelemelerde kullanılan LFRS'larda (Linear Feedback Shift Register - Doğrusal Geri Beslemeli Saklayıcı) doğrusal olmayan Boole fonksiyonları işlev görmektedir. Blok şifrelerde kullanılan yer değiştirme kutularının oluşturulmasında, Boole fonksiyonları yer almaktadır. (Braeken, 2006).



Şekil 2.1. Geri Beslemeli Saklayıcı Örneği

Modellenmiş olan Şekil 2.1'de, 5 bit uzunluğunda akan açık metin üzerinde, bir Boole fonksiyonu ile şematize edilmiş işlemler yapıldıktan sonra, işlem sonucu olan bit değeri 5 bit uzunluğundaki akan açık metin yapısının başına eklenmiş ve sağ yönüne doğru kaydırma işlemi yapılmıştır. Böylelikle akan şifreli metin oluşturulmuş olmaktadır. Şekil 2.1'de bir Boole fonkisyonu ile akış şifrelerinde kullanılan bir geri beslemeli saklayıcının, soyutlanmış modellemesi verilmiştir.

F_2: 1 ve 0 elemanlarından oluşan sonlu cisim, F_2^m: F_2 üzerinde, m boyutlu vektör uzayına karşılık geldiğinde ve bir Boole fonksiyonu f sembolü ile ifade edildiğinde; $f(x)$: $F_2^m \rightarrow F_2$ şeklinde haritalama olarak Boole fonksiyonu tanımlanmaktadır (Sağıroğlu vd., 2019). $F_2^m \rightarrow F_2$ haritalanması yapılan bir Boole fonksiyonu, doğruluk tablosu (truth

table) ile gösterilebilmektedir.

Bir Boole fonksiyonun doğruluk tablosu; m basamak sayısında ikilik (binary) diğer bir deyişle **0** ve **1**'lerden oluşan tüm fonksiyon değerlerini içerisinde barındıran vektördür (Sağıroğlu vd., 2019). Bir f Boole fonksiyonun doğruluk tablosu; $f(x) = (f(00\cdots0), \cdots, f(11\cdots1))$ şeklinde f'nin 2^m tane fonksiyon değerinden oluşmaktadır.

2.1.1 Cebirsel Gösterim Biçimi (Algebraic Normal Form - ANF)

Bir $f(x)$ Boole fonksiyonunu ifade etmenin farklı bir yöntemide *Cebirsel Gösterim Biçimi'dir (Algebraic Normal Form - ANF)*. Bir Boole fonksiyonun, cebirsel ifadesinin yapılması için; **XOR** ve **AND** işlemleri kullanılmaktadır (Bao vd., 2019). Boole fonksiyonun cebirsel ifadesinde; AND işlemlerine, çarpımlar karşılık gelmektedir (Sağıroğlu vd., 2019).

Algorithm 1: Bir Boole Fonksiyonunun Cebirsel İfade Algoritması

$g(x_m, \cdots, x_1) \leftarrow f(0, \cdots, 0);$
$k \leftarrow 1;$
while $k \neq 2^m$ **do**
  $k \leftarrow ikililer\ ;$ $\quad /* \quad b_m \cdot 2^{m-1} + \cdots + b_3 \cdot 2^2 + b_2 \cdot 2 + b_1 \quad */$
  if $g(b_m, b_{m-1}, \cdots, b_2, b_1) \neq f(b_m, b_{m-1}, \cdots, b_2, b_1)$ **then**
    $carpim \leftarrow 1;$
    $i \leftarrow 1;$
    while $i \neq m$ **do**
      $carpim \leftarrow carpim \cdot x_i^{b_i};$
      $i \leftarrow i + 1;$
    $g(x_m, x_{m-1}, \cdots, x_1) \leftarrow g(x_m, x_{m-1}, \cdots, x_1) \bigoplus carpim;$
$CebirselForm(f) \leftarrow g(x_m, x_{m-1}, \cdots, x_1)$

Algoritma 1'de verilen sözde kod ile; $F_2^m \rightarrow F_2$ şeklinde haritalaması yapılan bir f Boole fonksiyonunun cebirsel ifadesi elde edilmesi için tüm fonksiyon değerlerinden faydalanılır. Bütün doğruluk tablosu fonksiyon değerleri hesaplamaya katılarak, bir Boole fonksiyonunun cebirsel ifadesi ortaya konulmaktadır (Sağıroğlu vd., 2019).

$F_2^m \rightarrow F_2$'e tanımlı bir $f(x)$ Boole fonksiyonun cebirsel ifadesi $\alpha_{m,m-1,m-2,\cdots,2,1} \in F_2$ olmak üzere Eşitlik 2.1'deki gibi genelleştirilebilir (Sağıroğlu vd., 2019).

$$f(x) = f(x_m, x_{m-1}, \cdots, x_2, x_1) = \alpha_0 \oplus (\sum_{i=1}^{m} \alpha_i x_i) \oplus (\sum_{1 \leqslant i < j \leqslant m} \alpha_{ij} x_i x_j) \oplus \cdots \oplus \alpha_{m,m-1,m-2,\cdots,2,1} x_m x_{m-1} x_{m-2}, \cdots, x_1 \tag{2.1}$$

Örnek 2.1. $F_2^3 \rightarrow F_2$*'ye* $f(x_3, x_2, x_1) = \{0,1,0,0,1,1,1,1\}$ *Boole fonksiyonunun cebirsel ifadesi, Algoritma 1'e göre Çizelge 2.1'deki adımlar takip edilerek elde edilebilir (Sağıroğlu vd., 2019).*

Çizelge 2.1. $F_2^3 \rightarrow F_2$'ye Tanımlı Boole Fonksiyonu Cebirsel İfadesi

k	b_3	b_2	b_1	$f(b_3, b_2, b_1)$	$g(b_3, b_2, b_1)$
	0	0	0	0	0
1	0	0	1	1	x_1
2	0	1	0	0	x_1
3	0	1	1	0	$x_1 \oplus x_1x_2$
4	1	0	0	1	$x_1 \oplus x_3 \oplus x_1x_2$
5	1	0	1	1	$x_1 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3$
6	1	1	0	1	$x_1 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3$
7	1	1	1	1	$x_1 \oplus x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_2x_3$

Örnek 2.2. $F_2^4 \rightarrow F_2$*'ye* $f(x_4, x_3, x_2, x_1) = \{0,1,1,1,0,1,0,1,0,0,1,0,0,0,1,1\}$ *Boole fonksiyonun cebirsel ifadesi, Algoritma 1'e göre Çizelge 2.2'deki adımlar takip edilerek elde edilebilir.*

Çizelge 2.2. $F_2^4 \rightarrow F_2$'ye Tanımlı Boole Fonksiyonu Cebirsel İfadesi

k	b_4	b_3	b_2	b_1	$f(b_4, b_3, b_2, b_1)$	$g(b_4, b_3, b_2, b_1)$
	0	0	0	0	0	0
1	0	0	0	1	1	x_1
2	0	0	1	0	1	$x_1 \oplus x_2$
3	0	0	1	1	1	$x_1 \oplus x_2 \oplus x_1x_2$
4	0	1	0	0	0	$x_1 \oplus x_2 \oplus x_1x_2$
5	0	1	0	1	1	$x_1 \oplus x_2 \oplus x_1x_2$
6	0	1	1	0	0	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3$
7	0	1	1	1	1	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_2x_3$
8	1	0	0	0	0	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_2x_3$
9	1	0	0	1	0	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2x_3$
10	1	0	1	0	1	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2x_3$
11	1	0	1	1	0	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2x_3$
12	1	1	0	0	0	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2x_3$
13	1	1	0	1	0	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2x_3$
14	1	1	1	0	1	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2x_3 \oplus x_2x_3x_4$
15	1	1	1	1	1	$x_1 \oplus x_2 \oplus x_1x_2 \oplus x_2x_3 \oplus x_1x_4 \oplus x_1x_2x_3 \oplus x_2x_3x_4$

2.1.2 Doğrusal (Affine) Fonksiyon

$f(x)$: $F_2^m \rightarrow F_2$'e tanımlı olan bir Boole fonksiyonu; Eşitlik 2.2 şeklinde gösterilebiliyorsa, bu Boole fonksiyonu *Doğrusal (Affine) Fonksiyon* veya *1. Dereceden*

Fonksiyon olarak tanımlanmaktadır (Sağıroğlu vd., 2019).

$$f(x) = x \bullet w \oplus c \tag{2.2}$$

Eşitlik 2.2'de belirtilen $\oplus$ işlemi XOR'u, $\bullet$ işlemi *Nokta Ürünü*'nü temsil etmektedir (Saarinen, 2012). Aynı eşitlikte bulunan c değeri F_2 sonlu cismindeki sabit değere karşılık gelmektedir. F_2^m'in elemanları olan x ve w vektörlerinin, nokta ürünü ile genelleştirilmesi Eşitlik 2.3'te ifade edilmiştir.

$$x \bullet w = x_1 \cdot w_1 \oplus x_2 \cdot w_2 \oplus x_3 \cdot w_3 \oplus \cdots \oplus x_m \cdot w_m \tag{2.3}$$

Örnek 2.3. *$F_2^3 \rightarrow F_2$'ye tanımlı, $f_1(x_3, x_2, x_1) = x_2 \oplus x_3$ olan bir Boole fonksiyonu; doğrusal bir fonksiyondur.*

Örnek 2.4. *$F_2^3 \rightarrow F_2$'ye tanımlı, $f_2(x_3, x_2, x_1) = x_2x_3 \oplus x_1 \oplus x_3$ olan bir Boole fonksiyonu, x_2x_3 teriminde çarpım durumunda 2 değişken olduğundan dolayı doğrusal olmayan fonksiyondur.*

2.1.3 Hamming Ağırlık/Uzaklık

Bir $f(x)$ Boole fonksiyonunun, doğruluk tablosunda bulunan **1** değerlerinin toplam sayısı, *Hamming Ağırlığını veya Uzaklığını* ifade etmektedir (Chen vd., 2022). Bir $f(x)$ Boole fonksiyonun Hamming ağırlığı, $wt(f(x))$ şeklinde ifade edilebilmektedir (Sağıroğlu vd., 2019).

$f(x)$: $F_2^m \rightarrow F_2$'ye tanımlı olan Boole fonksiyonunun, doğruluk tablosunda bulunan 0 ve 1'lerin sayılarının eşit olması durumunda, dengeli Boole fonksiyonu olmaktadır. Dolayısıyla bir Boole fonksiyonunun dengeli olabilmesi için Hamming ağırlığının, 2^{m-1} olması gerekmektedir (Sağıroğlu vd., 2019).

İki Boole fonksiyonu $f(x), g(x)$: $F_2^m \rightarrow F_2$'ye tanımlı olmak üzere; Boole fonksiyonlarının doğruluk tablolarındaki, birbirlerinden farklı oldukları konum sayılarının toplamı, iki Boole fonksiyonun Hamming uzaklığını vermektedir. İki Boole fonksiyonunun Hamming uzaklığını elde etmek için, Boole fonksiyonlarının XOR toplamının elde edilmesi ve elde edilen Boole fonksiyonunun Hamming ağırlığının (diğer deyişle 1'lerin sayısı) hesaplanması yeterli olur. Bu hesaplama; $d_H(f, g) = wt(f(x) \oplus g(x))$ olarak ifade edilmektedir.

Örnek 2.5. *Çizelge 2.3'te, iki Boole fonksiyonu $f_1(x), g_1(x)$: $F_2^4 \rightarrow F_2$'ye cebirsel ifadeleri, takip edildiği şekilde tanımlansın:*
$f_1(x_4, x_3, x_2, x_1) = x_2 \oplus x_3$
$g_1(x_4, x_3, x_2, x_1) = x_1 \oplus x_4$

Çizelge 2.3. $F_2^4 \rightarrow F_2$'ye Tanımlı İki Boole Fonksiyonunun Hamming Ağırlığının Hesaplanması

x_4	x_3	x_2	x_1	$f_1(x)$	$g_1(x)$	$f_1(x) \oplus g_1(x)$
0	0	0	0	0	0	0
0	0	0	1	0	1	**1**
0	0	1	0	1	0	**1**
0	0	1	1	1	1	0
0	1	0	0	1	0	**1**
0	1	0	1	1	1	0
0	1	1	0	0	0	0
0	1	1	1	0	1	**1**
1	0	0	0	0	1	**1**
1	0	0	1	0	0	0
1	0	1	0	1	1	0
1	0	1	1	1	0	**1**
1	1	0	0	1	1	0
1	1	0	1	1	0	**1**
1	1	1	0	0	1	**1**
1	1	1	1	0	0	0

Her Boole fonksiyonu için tanımlanan işlemler yapıldıktan sonra; Boole fonksiyonları takip edildiği gibi elde edilebilir:

$f_1(x_4, x_3, x_2, x_1) = \{0,0,1,1,1,1,0,0,0,0,1,1,1,1,0,0\}$

$g_1(x_4, x_3, x_2, x_1) = \{0,1,0,1,0,1,0,1,1,0,1,0,1,0,1,0\}$

$f_1(x)$ ve $g_1(x)$ Boole fonksiyonlarının Hamming uzaklığı aşağıdaki gibi tespit edilmektedir (Sağıroğlu vd., 2019):

$d_H(f_1, g_1) = wt(f_1 \oplus g_1) = 8.$

2.1.4 Doğrusal Olmama (Non-Linearity)

Bir Boole fonksiyon olan $f(x)$'in *Doğrusal Olmama (Non-Linearity) Değeri*; $f(x)$'in bütün doğrusal fonksiyonlarına olan en küçük Hamming uzaklığı olarak ifade edilmektedir ve N_f şeklinde gösterilmektedir (Sağıroğlu vd., 2019).

Örnek 2.6. *Çizelge 2.4'te verilen $F_2^4 \rightarrow F_2$'ye tanımlı, $f_4(x_4, x_3, x_2, x_1) = x_1x_3x_4 \oplus x_1 \oplus x_2x_4 \oplus x_3x_4 \oplus x_3 \oplus x_4 \oplus 1$ Boole fonksiyonun doğrusal olmama değeri takip edildiği şekilde hesaplanmaktadır:*

$f_4(x)$ Boole fonksiyonun doğrusal olmama değeri; tanımlı olan bütün doğrusal fonksiyonlara olan Hamming uzaklıkların en küçüğü olacağı için, $F_2^4 \rightarrow F_2$'ye tanımlı olan bütün doğrusal fonksiyonlar; Çizelge 2.4'te $a_1(x)$'ten $a_{32}(x)$'e olacak şekilde ifade edilmektedir. Örnek olarak Çizelge 2.4'te gösterildiği gibi, $f_4(x)$ Boole fonksiyonunun $a_6(x) = x_1 \oplus x_3$ doğrusal fonksiyonuna olan Hamming ağırlığı, $d_H(f_4, a_6) = 12$ olmaktadır.

Çizelge 2.4. $F_2^4 \rightarrow F_2$'ye Tanımlı $f_4(x)$ Boole Fonksiyonunun Doğrusal Olmama Değer Hesabı Hazırlığı

x_4	x_3	x_2	x_1	$f_4(x)$	$a(x)(O)$	$a(x)(1)$	$a_6(x) = x_1 \oplus x_3$	$f_1(x) \oplus a_6(x)$
0	0	0	0	1	$a_1(x) = 0$	$a_{17}(x) = 1$	0	**1***
0	0	0	1	0	$a_2(x) = x_1$	$a_{18}(x) = 1 \oplus x_1$	1	**1***
0	0	1	0	1	$a_3(x) = x_2$	$a_{19}(x) = 1 \oplus x_2$	0	**1***
0	0	1	1	0	$a_4(x) = x_1 \oplus x_2$	$a_{20}(x) = 1 \oplus x_1 \oplus x_2$	1	**1***
0	1	0	0	0	$a_5(x) = x_3$	$a_{21}(x) = 1 \oplus x_3$	1	**1***
0	1	0	1	1	$a_6(x) = x_1 \oplus x_3$	$a_{22}(x) = 1 \oplus x_1 \oplus x_3$	0	**1***
0	1	1	0	0	$a_7(x) = x_2 \oplus x_3$	$a_{23}(x) = 1 \oplus x_2 \oplus x_3$	1	**1***
0	1	1	1	1	$a_8(x) = x_1 \oplus x_2 \oplus x_3$	$a_{24}(x) = 1 \oplus x_1 \oplus x_2 \oplus x_3$	0	**1***
1	0	0	0	0	$a_9(x) = x_4$	$a_{25}(x) = 1 \oplus x_4$	0	0
1	0	0	1	1	$a_{10}(x) = x_1 \oplus x_4$	$a_{26}(x) = 1 \oplus x_1 \oplus x_4$	1	0
1	0	1	0	1	$a_{11}(x) = x_2 \oplus x_4$	$a_{27}(x) = 1 \oplus x_2 \oplus x_4$	0	**1***
1	0	1	1	0	$a_{12}(x) = x_1 \oplus x_2 \oplus x_4$	$a_{28}(x) = 1 \oplus x_1 \oplus x_2 \oplus x_4$	1	**1***
1	1	0	0	0	$a_{13}(x) = x_3 \oplus x_4$	$a_{29}(x) = 1 \oplus x_3 \oplus x_4$	1	**1***
1	1	0	1	0	$a_{14}(x) = x_1 \oplus x_3 \oplus x_4$	$a_{30}(x) = 1 \oplus x_1 \oplus x_3 \oplus x_4$	0	0
1	1	1	0	1	$a_{15}(x) = x_2 \oplus x_3 \oplus x_4$	$a_{31}(x) = 1 \oplus x_2 \oplus x_3 \oplus x_4$	1	0
1	1	1	1	1	$a_{16}(x) = x_1 \oplus x_2 \oplus x_3 \oplus x_4$	$a_{32}(x) = 1 \oplus x_1 \oplus x_2 \oplus x_3 \oplus x_4$	0	**1***

Dolayısıyla, $f_4(x)$ Boole fonksiyonunun doğrusal olmama değeri Çizelge 2.5'teki en küçük değere göre $N_{f_4} = 4$ olarak tespit edilir.

Çizelge 2.5. $f_4(x)$ Boole Fonksiyonunun $F_2^4 \rightarrow F_2$'ye Tanımlı Bütün Doğrusal Fonksiyonlarına Olan Hamming Uzaklıkları

$d_H(f_4, a_1) = 8$	$d_H(f_4, a_9) = 8$	$d_H(f_4, a_{17}) = 8$	$d_H(f_4, a_{25}) = 8$
$d_H(f_4, a_2) = 8$	$d_H(f_4, a_{10}) = 8$	$d_H(f_4, a_{18}) = 8$	$d_H(f_4, a_{26}) = 8$
$d_H(f_4, a_3) = 6$	$d_H(f_4, a_{11}) = 10$	$d_H(f_4, a_{19}) = 10$	$d_H(f_4, a_{27}) = 6$
$d_H(f_4, a_4) = 6$	$d_H(f_4, a_{12}) = 10$	$d_H(f_4, a_{20}) = 10$	$d_H(f_4, a_{28}) = 6$
$d_H(f_4, a_5) = 8$	$d_H(f_4, a_{13}) = 8$	$d_H(f_4, a_{21}) = 8$	$d_H(f_4, a_{29}) = 8$
$d_H(f_4, a_6) = 12$	$d_H(f_4, a_{14}) = 12$	$d_H(f_4, a_{22}) = 4$	$d_H(f_4, a_{30}) = 4$
$d_H(f_4, a_7) = 10$	$d_H(f_4, a_{15}) = 6$	$d_H(f_4, a_{23}) = 6$	$d_H(f_4, a_{31}) = 10$
$d_H(f_4, a_8) = 6$	$d_H(f_4, a_{16}) = 10$	$d_H(f_4, a_{24}) = 10$	$d_H(f_4, a_{32}) = 6$

2.2 Yer Değiştirme Kutuları (S-Kutuları - Substitution Boxes - S-Boxes)

Kriptografide kullanılan şifreleme tekniklerinde, doğrusal olmayan yapılara yer verilmektedir (Forouzan, 2008). Şifreleme yönteminin doğrusal yapıda olması, kriptoanaliz yöntemleriyle şifrelenmiş verinin kolaylıkla analiz edilmesine sebep olmaktadır. Şifreleme yapısının doğrusallığını ortadan kaldırmaya ihtiyaç duyulmaktadır. Bu amaçla blok şifrelemede, doğrusal olmayan tek yapı; yer değiştirme kutuları olmaktadır (Jangra & Singh, 2022). Yer değiştirme kutuları; örten ve birebir özelliğini sağlayan,diğer bir deyişle bijektif (bijective), blok şifrelemenin güvenli olabilmesini için gerekli şifreleme elemanıdır (Sağıroğlu vd., 2019).

Boyutu $n \times m$ olan, diğer bir deyişle n bitlik giriş ve m bitlik çıkış değerlerine sahip

olan S-kutusunun tanımlaması takip eden şekilde olmaktadır (Jangra & Singh, 2022):

$$S\colon F_2^n \rightarrow F_2^m.$$

S-kutusunun; vektörel giriş Boole fonksiyonları: $x_n, x_{n-1}, x_{n-2}, \cdots, x_1$ ve vektörel çıkış Boole fonksiyonları: $y_m, y_{m-1}, y_{m-2}, \cdots, y_1$ olarak ifade edilebilir (Sağıroğlu vd., 2019).

Veri Şifreleme Standardında (Data Encryption Standard - DES) farklı giriş ve çıkış değerlerine sahip olan S-kutusu kullanılmasına rağmen, blok şifrelemede genel olarak aynı giriş ve çıkış değerlerine sahip olan S-kutuları kullanılmaktadır. Bu sebeple S-kutularının gösterimi; $3 \times 3, 4 \times 4, 8 \times 8$ veya $m \times m$ şeklinde diğer bir deyişle $n = m$ olmaktadır. Tez çalışması kapsamında *m*-bit giriş ve *m*-bit çıkış değerlerinde olan S-kutuları üzerine çalışılmıştır.

Çizelge 2.6. 4 × 4 Boyutunda Yer Değiştirme Kutusu (S-Kutusu)

Giriş-Hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Giriş-Binary	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Çikış-Hex	0	1	5	7	A	D	2	F	6	B	4	9	3	C	8	E
Çıkış-Binary	0000	0001	0101	0111	1010	1101	0010	1111	0110	1011	0100	1001	0011	1100	1000	1110

Örnek 2.7. *4 bit giriş ve 4 bit çıkış şeklinde haritalaması yapılan bir S-kutusu Çizelge 2.6'da bulunmaktadır (Saarinen, 2012).*
7 hexedecimal giriş değerinin Çizelge 2.6'da bulunan S-kutusuna göre haritalanması takip edildiği gibi özetlenebilir:
İlgili yer değiştirme kutusu 7 hexedecimal giriş değerini, F hexedecimal çıkış değerine haritalamaktadır. Gösterimi takip edildiği şekilde olmaktadır:
S(7) = F.

2.2.1 Involutif Yer Değiştirme Kutuları

Yer değiştirme kutusunun involutif olması; tersinin kendisine eşit olmasıdır (Tuncay, 2015). İnvolutif bir S-kutusu, Çizelge 2.7'de verilmektedir. $F_2^m \rightarrow F_2^m$'ye tanımlı olan S-kutusu için; x değeri, F_2^m'in tüm olası girdi değerlerine; y değeride olası tüm çıktı değerlerine karşılık geldiğinde involutif S-kutusu $S(x) = y$ olarak ifade edilmektedir. İnvolutif S-kutularında her girdi değerinin $S(S(x)) = x$ durumunu sağlaması gerekmektedir (B. Liu, Gong, Qiu & Zheng, 2011).

Çizelge 2.7. 4 × 4 Boyutunda Involutif Yer Değiştirme Kutusu (S-Kutusu)

Giriş-Hex	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Giriş-Binary	0000	0001	0010	0011	0100	0101	0110	0111	1000	1001	1010	1011	1100	1101	1110	1111
Çıkış-Hex	0	1	7	C	8	D	E	2	4	B	F	9	3	5	6	A
Çıkış-Binary	0000	0001	0111	1100	1000	1101	1110	0010	0100	1011	1111	1001	0011	0101	0110	1010

Örnek 2.8. *Çizelge 2.7'de verilen,* $F_2^4 \rightarrow F_2^4$*'e tanımlı S-kutusuna göre;* $S(3) = C$ *ve* $S(S(3)) = 3$ *olmakta, benzer şekilde* $S(8) = 4$ *ve* $S(S(8)) = 8$ *olmaktadır. S-kutusunun,*

tüm girdi değerleri için $S(S(x)) = x$ durumu sağlandığından dolayı ilgili S-kutusu involutif olmaktadır.

$$n = i(n-1) + (n-1) * i(n-2) \tag{2.4}$$

Eşitlik 2.4; involutif permütasyonların sayısını vermektedir (Muir, 1960). Eşitlik 2.4 için, $i(0) = 1$ ve $i(1) = 1$ başlangıç değerleri kullanılarak Şekil 2.2'de belirtilen hesaplama yapılmaktadır. Eşitlik 2.4'teki hesaplamanın ispatlarına; Muir (1960, p. 6) ve Oeis (2023) kaynaklarından ulaşılabilmektedir.

```
i(2)    = i(1)  + 1  * i(0) =  2
i(3)    = i(2)  + 2  * i(1) =  4
i(4)    = i(3)  + 3  * i(2) =  10
i(5)    = i(4)  + 4  * i(3) =  26
i(6)    = i(5)  + 5  * i(4) =  76
i(7)    = i(6)  + 6  * i(5) =  232
i(8)    = i(7)  + 7  * i(6) =  764
i(9)    = i(8)  + 8  * i(7) =  2620
i(10)   = i(9)  + 9  * i(8) =  9496
i(11)   = i(10) + 10 * i(9) =  35696
i(12)   = i(11) + 11 * i(10) = 140152
i(13)   = i(12) + 12 * i(11) = 568504
i(14)   = i(13) + 13 * i(12) = 2390480
i(15)   = i(14) + 14 * i(13) = 10349536
i(16)   = i(15) + 15 * i(14) = 46206736
```

Şekil 2.2. Bijektif İnvolutif S-Kutusu Permütasyon Sayısı Hesabı

Boyutu $m \times m$ olan involutif tüm S-kutuları permütasyonlarının sayısını hesaplamak için; Şekil 2.2'deki gibi, $n = 2^m$ değerine ulaşıncaya kadar hesaplama yapılmaktadır.

Örnek 2.9. 3×3 *boyutunda S-kutusu permütasyonlarından, involutif yapıda olanlarının sayısı; Şekil 2.2'deki hesaplamaya göre* ***i(8) = 764*** *adet olmaktadır (Fu & Feng, 2019).*

Örnek 2.10. 4×4 *boyutunda S-kutusu permütasyonlarından, involutif yapıda olanlarının sayısı; Şekil 2.2'deki hesaplamaya göre* ***i(16) = 46,206,736*** *adet olmaktadır.*

2.2.2 Sabit Nokta (Fixed Point) Sayısı

S-kutularının; girdi değerinin, aynı çıktı değerine haritalandığı konumları, yer değiştirme kutusunun *sabit noktaları* olmaktadır (Ullrich vd., 2011). S-kutusunun

haritalamasındaki toplam sabit nokta sayısı, yer değiştirme kutusunun sabit nokta sayısını vermektedir.

Çizelge 2.8. 4 × 4 Boyutlu 4 Sabit Noktalı S-Kutusu

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(×)	3	4	D	0	1	E	6	7	8	F	B	A	C	2	5	9

Örnek 2.11. *Çizelge 2.8'de verilmiş olan* 4×4 *boyutlu S-kutusunda; 6, 7, 8 ve C konumlarındaki girdi-çıktı değerleri birbirlerine eşit olduğu için, verilen yer değiştirme kutusunun sabit nokta sayısı* ***4*** *olmaktadır.*

Çizelge 2.9. 4 × 4 Boyutlu Sabit Noktasız S-Kutusu

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(×)	8	2	1	E	C	7	9	5	0	6	F	D	4	B	3	A

Örnek 2.12. *Çizelge 2.9'da verilmiş olan* 4 × 4 *boyutlu S-kutusunda, hiç sabit nokta bulunmamaktadır. Başka bir ifadeyle; bu S-kutusu için bütün girdi değerleri farklı çıktı değerlerine haritalanmaktadır.*

Tez çalışması kapsamında, S-kutularının "sabit noktaları" incelenmiş ancak, analiz edilen *kriptografik özelliklere* dahil edilmemiştir.

2.2.3 Doğrusal Yaklaşım Tablosu (Linear Approximation Table - LAT)

Doğrusal kriptoanalize karşı, S-kutusunun güvenilirliğini saptamak için *Doğrusal Yaklaşım Tablosu* (Linear Approximation Table - LAT) kullanılmaktadır (Bao vd., 2019). Bir S-kutusunun doğrusal olmama değerini hesaplamak için Doğrusal Yaklaşım Tablosu kullanılabilir.

S: $F_2^m \rightarrow F_2^m$ 'e tanımlanan, m bit giriş ve m bit çıkış değerlerine sahip olan bir S-kutusunun doğrusal yaklaşım tablosu; 2^m tane satır ve 2^m tane sütun, diğer bir deyişle $2^m \times 2^m$ boyutunda olmaktadır (Ullrich vd., 2011). Doğrusal Yaklaşım Tablosu'ndaki her hücrenin satır ve sütun değerleri sırasıyla Γ_A, Γ_B şeklinde tanımlanırsa; Doğrusal Yaklaşım Tablosu'nun her bir hücresinin değeri Eşitlik 2.5 kullanılarak hesaplanmaktadır (Lu vd., 2022).

$$LAT(\Gamma_A, \Gamma_B) = \#\{x \in F_2^m | \Gamma_A \bullet x = \Gamma_B \bullet S(x)\} - 2^{m-1} \tag{2.5}$$

Eşitlik 2.5'e göre, Doğrusal Yaklaşım Tablosu'nun her hücresinin hesaplanmasında *Nokta Ürünü* kullanılmaktadır. Boyutu $m \times m$ olan S-kutusu

için; x değeri, F_2^m'in tüm olası girdi değerlerine; $S(x)$ değeri S-kutusunun olası tüm çıktı değerlerine karşılık gelmektedir. Eşitlik 2.5 ile Doğrusal Yaklaşım Tablosu'nun her bir hücresi hesaplanarak Doğrusal Yaklaşım Tablosu oluşturulmaktadır.

Yer değiştirme kutusunun *doğrusal olmama değeri* N_{L_s} ile ifade edilebilir (Sağıroğlu vd., 2019). $F_2^m \rightarrow F_2^m$ 'e tanımlanan bir S-kutusunun doğrusal olmama değeri, Eşitlik 2.6 kullanılarak hesaplanmaktadır.

$$N_{L_s} = 2^{m-1} - \max_{\Gamma_A, \Gamma_B \in F_2^m \setminus \{0\}} |(\Gamma_A, \Gamma_B)| \tag{2.6}$$

Eşitlik 2.6'ya göre, doğrusal yaklaşım tablosundan elde edilen en büyük mutlak değeri (Doğrusal Yaklaşım Tablosu'nun (0, 0) konumu hariç) küçüldükçe, S-kutusunun doğrusal olmama değeri artmaktadır. Bu sayede S-kutusu, doğrusal kriptoanaliz saldırılarına karşı dayanıklı olmaktadır.

Boyutu $m \times m$ olan bir S-kutusunun maksimum doğrusal olmama değeri takip edildiği şekilde hesaplanmaktadır (Sağıroğlu vd., 2019):

$$2^{m-1} - 2^{\frac{m}{2}-1}.$$

Bir S-kutusunun, Eşitlik 2.6 kullanılarak elde edilen doğrusal olmama değeri ile S-kutusunun maksimum doğrusal olmama değeri oranlanarak, yer değiştirme kutusunun yüzdelik olarak doğrusal olmama oranı hesaplanmaktadır (Jangra & Singh, 2022).

Çizelge 2.10. 3 × 3 S-Kutusu

Giriş-Hex	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Çıkış-Hex	7	4	5	1	0	2	6	3

Çizelge 2.11. 3 × 3 S-Kutusunun LAT (2, 5) Değeri Hesaplaması

$\Gamma_{A=2} \bullet x = \Gamma_{B=5} \bullet S(x)$	Giriş Kontrol	Çıkış Kontrol
010 000 101 111	0*	0*
010 001 101 100	0	1
010 010 101 101	1	0
010 011 101 001	1*	1*
010 100 101 000	0*	0*
010 101 101 010	0*	0*
010 110 101 110	1*	1*
010 111 101 011	1*	1*

Örnek 2.13. *Çizelge 2.10'da verilen 3-bit giriş ve 3-bit çıkış değerlerine sahip,* $F_2^3 \rightarrow F_2^3$*'e tanımlanan S-kutusunun Doğrusal Yaklaşım Tablosu'ndaki giriş maskesi hexadecimal 2,*

çıkış maskesi hexadecimal 5 olan hücrenin değerinin hesaplanmasının detaylı anlatımı Çizelge 2.11'de ortaya konulmaktadır. Hesaplama takip edildiği şekilde özetlenebilir:
LAT (2, 5) ifadesindeki $2 = \Gamma_A$ *ve* $5 = \Gamma_B$ *olarak temsil edilmektedir.* $\Gamma_{A=2}$ *olarak ifade edilen kolonda yalnızca 2 decimal (ondalık) değerinin 3 bit binary karşılığı bulunmaktadır. Çizelge 2.11'de belirtilen,* x *ile ifade edilen kolonda ilgili S-kutusunun tüm girdi değerleri bulunmaktadır.* $S(x)$ *olarak tanımlanan sütun;* x *değerlerinin Çizelge 2.10'da bulunan S-kutusuna göre haritalaması sonucu oluşan çıktı değerlerini ifade etmektedir.*
Giriş Kontrol kısmında, $\Gamma_{A=2}$ *ve* x *değerlerinin Nokta Ürünü hesaplamaları yapılmaktadır. Bu işlem yapılırken; her bit aynı konumdaki diğer bit ile çarpılır, sonra tüm çarpımlar XOR işleminden geçirilmektedir. Nokta ürünü hesaplaması* $\Gamma_{B=5}$ *ve* $S(x)$ *içinde yapılarak, Çıkış Kontrol değerleri oluşturulmaktadır.*
"Giriş Kontrol" ve "Çıkış Kontrol" değerlerinin birbirleri ile aynı olanları, "" ile işaretlenmiştir. Bu işaretlemeler aynı zamanda, "Giriş Kontrol" ve "Çıkış Kontrol" değerlerinin XOR işlem sonuçlarının* ***0*** *olanlara karşılık gelmektedir.*
İlgili S-kutusuna göre, Doğrusal Yaklaşım Tablosu içerisindeki ilgili hücrenin değerinin hesaplanması takip eden şekilde olmaktadır:
$LAT\ (2,\ 5) = 6 - 2^{3-1} = 6 - 2^2 = 2.$

Çizelge 2.12. 3 × 3 S-Kutusu Doğrusal Yaklaşım Tablosu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	4	0	0	0	0	0	0	0
1	0	0	0	0	-2	2	2	2
2	0	2	0	2	0	**2**	0	-2
3	0	-2	0	2	2	0	2	0
4	0	-2	2	0	-2	0	0	-2
5	0	-2	-2	0	0	2	-2	0
6	0	0	-2	2	-2	-2	0	0
7	0	0	-2	-2	0	0	2	-2

Örnek 2.14. *Çizelge 2.10'da verilmiş olan S-kutusunun, Doğrusal Yaklaşım Tablosu Çizelge 2.12'de bütün değerleri için gösterilmiştir.*
İlgili S-kutusuna göre ***LAT (2, 5)*** *konumundaki hesaplanan değerin gösterildiği, Çizelge 2.11'deki hesaplamalara benzer şekilde tüm tablo değerleri elde edilmektedir.*

Örnek 2.15. *Çizelge 2.10'da verilmiş olan S-kusunun Doğrusal Yaklaşım Tablosu'nun en büyük mutlak değeri ((0, 0) konumu hariç) takip edildiği şekilde olmaktadır:*
İlgili S-kutusunun Doğrusal Yaklaşım Tablosu Çizelge 2.12'de verilmiştir. Çizelge 2.12'ye göre ilgili S-kutusunun Doğrusal Yaklaşım Tablosu'ndaki en büyük mutlak ((0, 0) hariç) değeri ***2*** *olmaktadır.*

Çizelge 2.13. Doğrusal Yaklaşım Tablosu Hesaplaması İçin 4-Bit Giriş 4-Bit Çıkış S-Kutusu

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(×)	8	3	B	1	E	C	D	A	0	F	7	2	5	6	4	9

Örnek 2.16. *Çizelge 2.13'te verilen 4-bit giriş ve 4-bit çıkış değerlerine sahip olan S-kutusuna ait Doğrusal Yaklaşım Tablosu'ndaki giriş maskesi 7, çıkış maskesi 5 olan hücrenin değerinin hesaplanmasının takip edildiği şekilde özetlenebilir:*
Çizelge 2.14'te hesaplanmış olan giriş-çıkış kontrol bitlerinin birbirleri ile aynı olduğu (giriş kontol ⊕ çıkış kontrol = 0) satır sayısı toplanılarak 8 elde edilmektedir.
Eşitlik 2.5 kullanılarak, Çizelge 2.13'te verilen S-kutusuna ait Doğrusal Yaklaşım Tablosu'nun 7. satır, 5. sütun hücresinin değeri, Çizelge 2.13'e göre takip edildiği şekilde hesaplanmıştır:
$LAT\ (7,\ 5) = 8 - 2^{4-1} = 8 - 2^3 = \boldsymbol{0}$.

Çizelge 2.14. 4 × 4 Boyutlu S-Kutusunun LAT (7, 5) Değeri Hesaplaması

$\Gamma_{A=7} \bullet x$	$= \Gamma_{B=5} \bullet S(x)$			Giriş Kontrol	Çıkış Kontrol
0111	0000	0101	1000	0*	0*
0111	0001	0101	0011	1*	1*
0111	0010	0101	1011	1*	1*
0111	0011	0101	0001	0	1
0111	0100	0101	1110	1*	1*
0111	0101	0101	1100	0	1
0111	0110	0101	1101	0*	0*
0111	0111	0101	1010	1	0
0111	1000	0101	0000	0*	0*
0111	1001	0101	1111	1	0
0111	1010	0101	0111	1	0
0111	1011	0101	0010	0*	0*
0111	1100	0101	0101	1	0
0111	1101	0101	0110	0	1
0111	1110	0101	0100	0	1
0111	1111	0101	1001	1*	1*

Örnek 2.17. *Çizelge 2.13'te verilmiş olan, $F_2^4 \rightarrow F_2^4$'e tanımlanan S-kutusunun Doğrusal Yaklaşım Tablosu'nun en büyük mutlak değeri takip edildiği şekilde olmaktadır:*

Çizelge 2.15. 4 × 4 Boyutlu S-Kutusunun Doğrusal Yaklaşım Tablosu (LAT)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	2	2	-2	2	0	4	0	0	2	2	-2	2	0	-4
2	0	2	0	2	-2	0	2	4	0	-2	0	-2	2	0	-2	4
3	0	2	2	-4	4	2	2	0	0	-2	2	0	0	2	-2	0
4	0	-2	-2	4	4	2	2	0	2	0	0	-2	2	0	0	-2
5	0	2	0	2	2	0	2	0	-2	0	-2	0	-4	2	4	2
6	0	0	2	2	2	2	0	0	-2	2	0	4	0	-4	-2	2
7	0	4	4	0	0	**0**	0	0	2	2	-2	-2	2	-2	2	-2
8	0	0	0	0	2	-2	-2	2	-4	-4	0	0	2	-2	2	-2
9	0	0	-2	-2	0	0	2	2	-4	4	-2	-2	0	0	-2	-2
A	0	2	0	2	0	-2	0	-2	0	-2	-4	2	0	2	-4	-2
B	0	2	-2	0	-2	0	4	-2	0	-2	2	0	-2	-4	0	-2
C	0	-2	2	0	2	-4	0	2	2	0	0	-2	-4	-2	-2	0
D	0	2	0	2	0	2	-4	-2	-2	0	2	-4	-2	0	-2	0
E	0	0	-2	-2	0	4	-2	2	2	-2	-4	0	-2	-2	0	0
F	0	-4	4	0	-2	2	2	-2	-2	-2	-2	-2	0	0	0	0

*İlgili S-kutusunun Doğrusal Yaklaşım Tablosu Çizelge 2.15'te verilmiştir. Çizelge 2.15'e göre ilgili S-kutusunun en büyük mutlak Doğrusal Yaklaşım Tablosu değeri **4** olmaktadır.*

Literatürde bulunan Bao vd. (2019) çalışmasında verildiği üzere; bir S-kutusunun küp (cube) veya küp benzeri (cube-like) ataklara dayanıklı olabilmesi, en büyük mutlak Doğrusal Yaklaşım Tablosu değeri ile doğrudan ilişkişi olan S-kutusunun doğrusallık (linearity) değerinin düşük olması gerekmektedir. S-kutusunun doğrusallık değeri büyüdükçe, çıktı bitlerinin, girdi bitlerine olan bağımlılığı artmaktadır (Dinur & Shamir, 2009). Diğer bir deyişle, S-kutusunun olabildiğince doğrusallıktan uzaklaşması gerekmektedir (Fuhr, 2010).

2.2.4 Fark Dağılım Tablosu (Difference Distribution Table - DDT)

Bir yer değiştirme kutusunun, diferansiyel kriptoanaliz saldırılarına karşı dayanıklılığını ölçümlemek için kriptografik özellik olarak, *Fark Dağılım Tablosu (Difference Distribution Table - DDT)* kullanılmaktadır (Y. Liu vd., 2021). *XOR Dağılım Tablosu* olarak da ifade edilen Fark Dağılım Tablosu'nun hücreleri doldurulurken; $m \times m$ boyutunda S-kutusu, $F_2^m \rightarrow F_2^m$'e tanımlandığında a giriş farkı satır değerini, b çıkış farkı sütun değerini temsil etmektedir (Cid vd., 2018). Fark Dağılım Tablosu'nun hücrelerinin hesaplanması için Eşitlik 2.7 kullanılmaktadır (Bao vd., 2019).

$$DDT(a,b) = \#\{x \in F_2^m | S(x) \oplus S(x \oplus a) = b\} \tag{2.7}$$

Eşitlik 2.7'ye göre; boyutu $m \times m$ olan, bir S-kutusu için; x değeri, F_2^m'in tüm olası girdi değerlerine; $S(x)$ değeri de F_2^m'in olası tüm çıktı değerlerine karşılık gelmektedir. $S(x \oplus a)$, $x \oplus a$ işlem sonucunun, S-kutusundaki çıktı değerinin karşılığı olmaktadır. Eşitlik 2.7'de verilene göre, b değerine eşitlik olduğu durumların sayısının toplamı, direkt olarak fark dağılım tablosundaki ilgili hücrenin değerini vermektedir. Böylelikle Fark Dağılım Tablosu değerleri elde edilmiş olmaktadır (Cid vd., 2018).

Çizelge 2.16. 3 × 3 S-Kutusunun DDT (3, 5) Değeri Hesaplaması

$S(0) \oplus S(0 \oplus 3) = S(0) \oplus s(3) = 7 \oplus 1 = 6$
$S(1) \oplus S(1 \oplus 3) = S(1) \oplus s(2) = 4 \oplus 5 = 1$
$S(2) \oplus S(2 \oplus 3) = S(2) \oplus s(1) = 5 \oplus 4 = 1$
$S(3) \oplus S(3 \oplus 3) = S(3) \oplus s(0) = 1 \oplus 7 = 6$
$S(4) \oplus S(4 \oplus 3) = S(4) \oplus s(7) = 0 \oplus 3 = 3$
$S(5) \oplus S(5 \oplus 3) = S(5) \oplus s(6) = 2 \oplus 6 = 4$
$S(6) \oplus S(6 \oplus 3) = S(6) \oplus s(5) = 6 \oplus 2 = 4$
$S(7) \oplus S(7 \oplus 3) = S(7) \oplus s(4) = 3 \oplus 0 = 3$

Örnek 2.18. *Çizelge 2.10'da verilen* 3 × 3 *boyutunda S-kutusuna göre Fark Dağılım Tablosu'ndaki (3, 5) konumdaki değeri aşağıda belirtildiği gibi hesaplanmaktadır:*
Çizelge 2.16'daki işlemler sonucunda elde edilen değerler arasında, 5 değerinin toplam sayısı 0 olduğu için, Çizelge 2.10'da verilen S-kutusun DDT (3, 5) konumdaki değeri ***0*** *olmaktadır. Çizelge 2.16'dan elde edilen* ***0*** *değeri, ilgili konumda Çizelge 2.17'de koyu renk ile ifade edilmiştir.*

Çizelge 2.17. 3 × 3 S-Kutusunun Fark Dağılım Tablosu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	8	0	0	0	0	0	0	0
1	0	0	2	2	2	2	0	0
2	0	2	2	0	0	2	2	0
3	0	2	0	2	2	**0**	2	0
4	0	0	2	2	0	0	2	2
5	0	0	0	0	2	2	2	2
6	0	2	0	2	0	2	0	2
7	0	2	2	0	2	0	0	2

Örnek 2.19. *Çizelge 2.10'da verilmiş olan S-kusunun Fark Dağılım Tablosu'nun en büyük değeri ((0, 0) konumu hariç) takip edildiği şekilde olmaktadır:*
İlgili S-kutusunun Fark Dağılım Tablosu Çizelge 2.17'de verilmiştir. Çizelge 2.17'ye göre ilgili S-kutusunun en büyük Fark Dağılım Tablosu değeri ((0, 0) hariç) ***2*** *olmaktadır.*

Çizelge 2.18. Fark Dağılım Tablosu Hesaplaması İçin 4 × 4 Boyutunda S-Kutusu

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
S(×)	2	9	0	F	A	C	D	7	B	1	4	8	5	6	E	3

$F_2^m \rightarrow F_2^m$'e tanımlı bir S-kutusunun Fark Dağılım Tablosu'nun oluşturulmasının zaman karmaşıklığı, $\mathcal{O}(2^{2m})$ olmaktadır (Cid vd., 2018).

Örnek 2.20. *Çizelge 2.18'de verilen* 4×4 *boyutunda olan S-kutusuna göre, DDT (A, E) konumdaki değer, takip edildiği gibi hesaplanmaktadır:*
Çizelge 2.19'a göre 2^m *diğer bir deyişle 16 adet işlem yapılır ve yapılan işlemlerin sonucundaki* ***E*** *(hesaplanmak istenen DDT (A, E)'ye ait çıktı değeri E olduğu için) değerlerinin toplam sayısı; Çizelge 2.18'de verilen S-kutusundan oluşan Fark Dağılım Tablosu'nun A. satır, E. sütun değeri olmaktadır. Bu hesaplama yapılırken, Eşitlik 2.7 kullanılmıştır.*
Çizelge 2.19'da, 0-F arasındaki değerler için işlemler yapılmıştır.
Çizelge 2.18'de verilen 4×4 *boyutunda olan S-kutusuna göre DDT (A, E) değeri* ***2*** *olmakta, ilgili konumda Çizelge 2.20'de koyu renk ile ifade edilmiştir..*

Çizelge 2.19. 4 × 4 Boyutlu S-Kutusunun DDT (A, E) Değeri Hesaplaması

$S(0) \oplus S(0 \oplus A) = S(0) \oplus S(A) = 2 \oplus 4 = 6$
$S(1) \oplus S(1 \oplus A) = S(1) \oplus S(B) = 9 \oplus 8 = 1$
$S(2) \oplus S(2 \oplus A) = S(2) \oplus S(8) = 0 \oplus B = B$
$S(3) \oplus S(3 \oplus A) = S(3) \oplus S(9) = F \oplus 1 = \mathbf{E}$
$S(4) \oplus S(4 \oplus A) = S(4) \oplus S(E) = A \oplus E = 4$
$S(5) \oplus S(5 \oplus A) = S(5) \oplus S(F) = C \oplus 3 = F$
$S(6) \oplus S(6 \oplus A) = S(6) \oplus S(C) = D \oplus 5 = 8$
$S(7) \oplus S(7 \oplus A) = S(7) \oplus S(D) = 7 \oplus 6 = 1$
$S(8) \oplus S(8 \oplus A) = S(8) \oplus S(2) = B \oplus 0 = B$
$S(9) \oplus S(9 \oplus A) = S(9) \oplus S(3) = 1 \oplus F = \mathbf{E}$
$S(A) \oplus S(A \oplus A) = S(A) \oplus S(0) = 4 \oplus 2 = 6$
$S(B) \oplus S(B \oplus A) = S(B) \oplus S(1) = 8 \oplus 9 = 1$
$S(C) \oplus S(C \oplus A) = S(C) \oplus S(6) = 5 \oplus D = 8$
$S(D) \oplus S(D \oplus A) = S(D) \oplus S(7) = 6 \oplus 7 = 1$
$S(E) \oplus S(E \oplus A) = S(E) \oplus S(4) = E \oplus A = 4$
$S(F) \oplus S(F \oplus A) = S(F) \oplus S(5) = 3 \oplus C = F$

Örnek 2.21. *Çizelge 2.18'de verilmiş olan S-kusunun Fark Dağılım Tablosu'nun en büyük değeri takip edildiği şekilde olmaktadır:*
İlgili S-kutusunun Fark Dağılım Tablosu Çizelge 2.20'de verilmiştir. Çizelge 2.20'ye göre ilgili S-kutusunun en büyük Fark Dağılım Tablosu değeri ***4*** *olmaktadır.*

Çizelge 2.20. 4 × 4 Boyutlu S-Kutusunun Fark Dağılım Tablosu (DDT)

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	2	0	0	2	0	0	0	4	2	2	2	0	2
2	0	0	2	0	0	2	2	2	0	2	0	4	0	0	0	2
3	0	2	0	2	0	2	2	0	2	2	0	0	0	4	0	0
4	0	0	0	0	0	2	0	2	4	0	2	2	0	2	2	0
5	0	0	2	2	2	0	2	4	0	0	0	0	0	2	2	0
6	0	2	2	2	0	2	0	0	0	0	2	0	0	0	4	2
7	0	0	2	0	2	4	0	0	2	0	0	0	2	2	0	2
8	0	0	0	2	4	0	0	2	2	2	2	0	0	0	0	2
9	0	0	2	2	0	0	0	0	2	4	0	2	2	0	2	0
A	0	4	0	0	2	0	2	0	2	0	0	2	0	0	**2**	2
B	0	2	4	0	2	0	0	0	0	2	2	2	0	2	0	0
C	0	2	0	0	0	0	0	2	0	2	0	0	2	2	2	4
D	0	2	0	4	2	2	0	2	0	0	0	2	2	0	0	0
E	0	0	0	0	2	2	4	0	0	2	2	0	2	0	2	0
F	0	2	2	0	0	0	2	2	2	0	2	0	4	0	0	0

2.2.5 Cebirsel Derece (Algebraic Degree - AD)

Blok şifrelemede tek doğrusal olmayan kısım olan yer değiştirme kutularının, cebirsel (algebraic) veya küp (cube) gibi saldırılara karşı dayanıklılığını ölçümlemek için *Cebirsel Derece (Algebraic Degree - AD)* kriptografik özelliği kullanılmaktadır (Tho, Thang, Nga & Hoang, 2018). Boyutu $m \times m$ olan S-kutusu, S: $F_2^m \rightarrow F_2^m$'e tanımlandığında; S-kutusunun giriş bitleri; $x = (x_m, x_{m-1}, x_{m-2}, \cdots, x_1)$ ve çıkış bitleri; $y = (y_m, y_{m-1}, y_{m-2}, \cdots, y_1)$ olmaktadır (Ashok & Bhaaskaran, 2018).

S: $F_2^m \rightarrow F_2^m$'e tanımlanan S-kutusunun; vektörel çıkış Boole fonksiyonlarının cebirsel derecelerinden, *en küçük* olan cebirsel derece seçilerek, S-kutusunu cebirsel derecesi hesaplanmaktadır (Tho vd., 2018).

Bir S-kutusunun her vektörel çıkış Boole fonksiyonunun cebirsel ifadesinde, çarpım durumunda bulunan en yüksek sayıdaki terim sayısı; vektörel çıkış Boole fonksiyonun cebirsel derecesini ifade etmektedir (Chen vd., 2022).

Yer değiştirme kutusunun cebirsel derecesi; haritalama sonucu oluşan çıkış Boole fonksiyonlarının, en küçük cebirsel derecesine eşit olmaktadır (Tho vd., 2018). S-kutusunun cebirsel derecesi, $deg(S)$ şeklinde gösterilmektedir. Eşitlik 2.8'deki gibi ifade edilebilir.

$$deg(S) = min\{deg(y_m, y_{m-1}, y_{m-2}, \cdots, y_1)\} \tag{2.8}$$

Piccolo S-kutusu, hafif sıklet blok şifrelemede kullanılmaktadır (Pehlivanoğulu, 2018).

Çizelge 2.21. Piccolo Hafif Sıklet Blok Şifreleme S-Kutusu

x_4	x_3	x_2	x_1	y_4	y_3	y_2	y_1
0	0	0	0	1	1	1	0
0	0	0	1	0	1	0	0
0	0	1	0	1	0	1	1
0	0	1	1	0	0	1	0
0	1	0	0	0	0	1	1
0	1	0	1	1	0	0	0
0	1	1	0	0	0	0	0
0	1	1	1	1	0	0	1
1	0	0	0	0	0	0	1
1	0	0	1	1	0	1	0
1	0	1	0	0	1	1	1
1	0	1	1	1	1	1	1
1	1	0	0	0	1	1	0
1	1	0	1	1	1	0	0
1	1	1	0	0	1	0	1
1	1	1	1	1	1	0	1

Piccolo'da kullanılan 4×4 boyutundaki yer değiştirme kutusunun $F_2^4 \rightarrow F_2^4$'e tanımlanan haritalanması, Çizelge 2.21'de gösterilmiştir. Piccolo'da kullanılan yer değiştirme kutusunun yüksek dereceden düşüğe doğru giriş bitleri; $\{ x_4 , x_3 , x_2 , x_1 \}$ şeklinde, çıkış bitleri; $\{ y_4 , y_3 , y_2 , y_1 \}$ şeklinde gösterilmiştir.

Çizelge 2.22. Piccolo S-Kutusu Vektörel Çıkış Boole Fonksiyonları Cebirsel İfadesi

Vektörel Çıkış Boole Fonksiyon	**Cebirsel İfadesi**	**Cebirsel Derece**
$y_1 = \{0,0,1,0,1,0,0,1,1,0,1,1,0,0,1,1\}$	$x_1x_2x_3 \oplus x_1x_2 \oplus x_1x_3 \oplus x_1x_4 \oplus x_2x_3x_4 \oplus x_2x_4 \oplus x_2 \oplus x_3 \oplus x_4$	3
$y_2 = \{1,0,1,1,1,0,0,0,0,1,1,1,1,1,0,0,0\}$	$x_1x_2 \oplus x_1 \oplus x_2x_3x_4 \oplus x_2x_3 \oplus x_2x_4 \oplus x_3x_4 \oplus x_4 \oplus 1$	3
$y_3 = \{1,1,0,0,0,0,0,0,0,0,1,1,1,1,1,1\}$	$x_1x_2 \oplus x_1 \oplus x_2 \oplus x_3 \oplus 1$	2
$y_4 = \{1,0,1,0,0,1,0,1,0,1,0,1,0,1,0,1\}$	$x_1 \oplus x_3x_4 \oplus x_3 \oplus x_4 \oplus 1$	2

Örnek 2.22. *Boyutu* 4×4 *olan Piccolo S-kutusunun cebirsel derecesi takip edildiği gibi hesaplanmaktadır:*

4 bit giriş ve 4 bit çıkış bijektif hafif sıklet Piccolo'nun yer değiştirme kutusunun haritalaması sonucu oluşan çıkış Boole fonksiyonlarının cebirsel ifadesi ve bunların cebirsel dereceleri Çizelge 2.22'de ifade edilmiştir (Tho vd., 2018).

S-kutusunun cebirsel derecesi, haritalama sonucu oluşan çıkış Boole fonksiyonları içerisinde bulunan, en küçük cebirsel derece olmaktadır. Bu sebeple, Piccolo hafif sıklet yer değiştirme kutusunun cebirsel derecesi ***2*** *olarak elde edilmektedir.*

2.2.6 Kötü Girdi Kötü Çıktı Örüntüsü (Bad Input Bad Output Pattern - BIBO Pattern - BIBO Örüntüsü)

Yer değiştirme kutularının kriptografik özellikleri incelenirken çoğu zaman diferansiyel tekdüzelik (differential uniformity), doğrusallık (linearity) değerleri analiz edilmektedir (H. Kim vd., 2021). *Kötü Girdi Kötü Çıktı Örüntüsü (Bad Input Bad Output Pattern - BIBO Pattern - BIBO Örüntüsü)*; hafif sıklet S-kutularının, diferansiyel ve doğrusal kriptoanaliz saldırına karşı dayanıklılığını ölçümlemek için incelenebilen kriptografik özelliklerinden biri olmaktadır (Bao vd., 2019).

Hafif sıklet S-kutularının BIBO örüntüsü; 2 bileşenin sayılarının toplamından oluşmaktadır (S. Kim vd., 2020). Bu bileşenler; **DDT** ve **LAT** için hesaplanan BIBO değerleridir (Lu vd., 2022).

$$\text{BIBO Örüntüsü} = \text{BIBO DDT Sayısı} + \text{BIBO LAT Sayısı} \tag{2.9}$$

Bir S-kutusunun BIBO örüntüsü, Eşitlik 2.9 kullanılarak hesaplanmaktadır (Bao vd., 2019).

2.2.6.1 BIBO DDT Sayısının Elde Edilmesi

Bir S-kutusunun Fark Dağılım Tablosu'ndaki giriş ve çıkış değerlerinin Hamming ağırlıklarının 1'e eşit olduğu konumlar içerisinde, 0'dan farklı olanların toplam sayısı; BIBO DDT sayısı olarak ifade edilmektedir. Bir S-kutusunun, giriş ve çıkış değerlerinin Hamming ağırlıklarının 1 değerine eşit olması; **1-1 bit Aktif Bit Tablosu (Single Active Bits Table)** olarak ifade edilebilmektedir (Lu vd., 2022).

Algorithm 2: Hamming Ağırlık Hesaplama Gösterimi

```
wt ← 0;
input ← hamming_weight_input;
character ← input_each_character;
while character ≠ EOF do
    if character == 1 then
        wt ← wt + 1;
HammingWeight(input) ← wt
```

İkili olarak verilen girdi değerindeki; '1' değerlerinin toplam sayısını, diğer bir deyişle girdi değerinin Hamming ağırlığını hesaplayacak algoritmanın sözde kodu, Algoritma 2'de özetlenmiştir.

$F_2^4 \rightarrow F_2^4$'e tanımlanan S-kutusunun, BIBO DDT sayısının hesaplanması için

S-kutusuna göre oluşturulan Fark Dağılım Tablosu'ndaki 0'dan farklı değerlerin olup olmadığının incelenmesi gereken ilgili alanlar, diğer bir deyişle 1-1 bit aktif bit tablosu, Çizelge 2.23'te gösterilmiştir. Çizelge 2.23'te verilen α, S-kutusunun girdi değerini; β, S-kutusunun çıktı değerini temsil etmektedir. Çizelge 2.23'te ilgili alanlar örnek olarak gösterilmiş olup, incelenmesi gereken konumlar vurgulanmıştır.

Çizelge 2.23. $F_2^4 \rightarrow F_2^4$'e Tanımlanan S-Kutusunun 1-1 Aktif Bit Tablosu

α/β	**1000**	**0100**	**0010**	**0001**
1000	×	×	×	×
0100	×	×	×	×
0010	×	×	×	×
0001	×	×	×	×

GIFT'e ait olan 4×4 boyutunda, bijektif S-kutusu, Çizelge 2.24'te verilmiştir (Cao & Zhang, 2019). GIFT'in yer değiştirme kutusuna göre, Eşitlik 2.7 kullanılarak hesaplanan Fark Dağılım Tablosu, Çizelge 2.25'te gösterilmiştir.

Çizelge 2.24. GIFT'in S-Kutusu

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
S(×)	1	A	4	C	6	F	3	9	2	D	B	7	5	0	8	E

Örnek 2.23. *Çizelge 2.24'te verilen GIFT'in S-kutusuna ait BIBO DDT sayısının hesaplanması takip edildiği gibi verilebilir (Banik vd., 2017):*
Çizelge 2.23'te belirtilen konumlar; Çizelge 2.25 üzerinde BIBO DDT sayısının hesaplanması için, daireler içine alınmıştır.
*Çizelge 2.25'te, daireler içerisinde 0'dan farklı olan konumların toplam sayısı 1 olduğu için, GIFT'in S-kutusu için BIBO DDT sayısı, **1** olmaktadır.*

2.2.6.2 BIBO LAT Sayısının Elde Edilmesi

Bir S-kutusunun Doğrusal Yaklaşım Tablosu'ndaki giriş ve çıkış değerlerinin Hamming ağırlıklarının 1'e eşit olduğu konumlarda 0'dan farklı değerlerin toplamı BIBO LAT sayısı olarak ifade edilmektedir (Bao vd., 2019). $F_2^4 \rightarrow F_2^4$'e tanımlanan bir S-kutusunun BIBO LAT sayısının hesaplanması, BIBO DDT sayısının hesaplaması ile benzerlik göstermektedir. Hesaplamada tek değişen nokta, incelenen tablolar olmaktadır. Bir S-kutusunun BIBO LAT sayısı için Fark Dağılım Tablosu değil Doğrusal Yaklaşım Tablosu incelenmektedir.

Örnek 2.24. *Çizelge 2.24'da verilen GIFT'in S-kutusuna ait BIBO LAT sayısının hesaplaması takip edildiği gibi olmaktadır:*

Çizelge 2.25. GIFT S-Kutusu BIBO DDT sayısı İncelemesi

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	⓪	⓪	0	⓪	2	2	0	②	2	2	2	2	0	0	2
2	0	⓪	⓪	0	⓪	4	4	0	⓪	2	2	0	0	2	2	0
3	0	0	0	0	0	2	2	0	2	0	0	2	2	2	2	2
4	0	⓪	⓪	2	⓪	4	0	6	⓪	2	0	0	0	2	0	0
5	0	0	2	0	0	2	0	0	2	0	0	0	2	2	2	4
6	0	0	4	6	0	0	0	2	0	0	2	0	0	0	2	0
7	0	0	2	0	0	2	0	0	2	2	2	4	2	0	0	0
8	0	⓪	⓪	4	⓪	0	0	4	⓪	0	0	4	0	0	0	4
9	0	2	0	2	0	0	2	2	2	0	2	0	2	2	0	0
A	0	4	0	0	0	0	4	0	0	2	2	0	0	2	2	0
B	0	2	0	2	0	0	2	2	2	2	0	0	2	0	2	0
C	0	0	4	0	4	0	0	0	2	0	2	0	2	0	2	0
D	0	2	2	0	4	0	0	0	0	0	2	2	0	2	0	2
E	0	4	0	0	4	0	0	0	2	2	0	0	2	2	0	0
F	0	2	2	0	4	0	0	0	0	2	0	2	0	0	2	2

Çizelge 2.26. GIFT S-Kutusu BIBO LAT Sayısı İncelemesi

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	⓪	⓪	0	②	-2	-2	2	④	0	0	-4	-2	-2	-2	-2
2	0	⓪	⓪	-4	⓪	4	0	0	②	2	2	-2	2	-2	2	2
3	0	0	0	-4	-2	-2	2	-2	2	-2	-2	-2	0	4	0	0
4	0	⓪	⓪	0	⓪	0	-4	-4	⓪	0	0	0	0	0	4	-4
5	0	0	0	0	2	-2	2	-2	0	4	4	0	2	2	-2	-2
6	0	0	0	-4	4	0	0	0	-2	-2	-2	2	2	-2	-2	-2
7	0	0	0	4	2	2	2	-2	2	-2	-2	-2	4	0	0	0
8	0	⓪	⓪	0	⓪	-4	0	-4	⓪	0	0	0	0	-4	0	4
9	0	0	0	0	-2	-2	2	2	4	0	0	4	2	-2	2	-2
A	0	0	-4	0	0	0	4	0	-2	-2	2	-2	-2	-2	2	-2
B	0	0	4	0	2	-2	2	2	-2	2	-2	-2	0	0	4	0
C	0	4	4	0	0	0	0	0	0	-4	4	0	0	0	0	0
D	0	-4	4	0	-2	2	2	-2	0	0	0	0	-2	-2	-2	-2
E	0	-4	0	0	4	0	0	0	2	-2	2	2	-2	2	2	2
F	0	-4	0	0	-2	-2	-2	2	-2	-2	2	-2	4	0	0	0

Çizelge 2.26'te verilen GIFT'e ait Doğrusal Yaklaşım Tablosu'nun 1-1 aktif bit konumlarında ki değerleri yuvarlak içinde alınmıştır. Yuvarlak içindeki konumlarda, 0'dan farklı olanların toplamı 3 olduğu için, GIFT'in S-kutusu için BIBO LAT sayısı, ***3*** *olmaktadır.*

Tablolar 2.25 ve 2.26'ya göre, GIFT'in S-kutusunun BIBO DDT sayısı 1 ve

BIBO LAT sayısı 3 olmaktadır. Eşitlik 2.9'a göre, GIFT S-kutusunun BIBO örüntüsü **4** olmaktadır.

BIBO Örüntü bileşenlerini oluşturan Fark Dağılım Tablosu ve Doğrusal Yaklaşım Tablosu hesaplamaları, farklı olarak isimlendirilebilmektedir. BIBO DDT sayısı için CardD1, BIBO LAT sayısı için CardL1 isimlendirilmesi kullanılabilmektedir (S. Kim vd., 2020).

Bao vd. (2019) kaynağına göre; S-kutuları için BIBO Örüntü değerinin 4'e eşit veya daha küçük olması, bu kriptografik özellikçe optimum değerler olarak kabul edilmektedir.

2.2.7 Dal Sayısı (Branch Number)

Bir S-kutusunun dal sayıları, doğrusal ve diferansiyel saldırılarına dayanıklılığı ölçümlemek için kriptografik özellik olarak incelenebilmektedir (H. Kim vd., 2021). Bir S-kutusunun 2 ayrı dal sayısı hesaplaması yapılabilmektedir (Manual, 2023). Bunlar; doğrusal ve diferansiyel dal sayılarıdır (Chen vd., 2022).

2.2.7.1 Doğrusal Dal Sayısı (Linear Branch Number - LBN)

Bir S-kutusunun Doğrusal Yaklaşım Tablosu'nun 0. satırı ve Doğrusal Yaklaşım Tablosu'nda bulunan 0'lar dışındaki giriş-çıkış değerlerinin toplam Hamming ağırlıklarının en küçük değeri; S-kutusunun *Doğrusal Dal Sayısını (Linear Branch Number - LBN)* ifade etmektedir (H. Kim vd., 2021).

$$LBN(S) = min_{LAT(\Gamma_A,\Gamma_B)\neq 0,\Gamma_A\neq 0}\{wt(\Gamma_A) + wt(\Gamma_B)\} \tag{2.10}$$

Boyutu $m \times m$ olan ve $F_2^m \rightarrow F_2^m$'e tanımlanan bir S-kutusunun Doğrusal Yaklaşım Tablosu'ndaki; Γ_A = *girdi değerini* ve Γ_B = *çıktı değerini* temsil ettiğinde, Doğrusal Yaklaşım Tablosu'nun her bir hücresi $LAT\ (\Gamma_A, \Gamma_A)$ olarak ifade edilmektedir (Sarkar, Mandal & Saha, 2019). S: $F_2^m \rightarrow F_2^m$'e tanımlanan, her $\Gamma_A, \Gamma_B \in F_2^m$ olduğunda, bir S-kutusunun doğrusal dal sayısı Eşitlik 2.10 ile hesaplanmaktadır. (Sarkar & Syed, 2018).

Bir S-kutusunun boyutu; *m*-bit giriş ve *m*-bit çıkış olduğunda, S-kutusunun doğrusal dal sayısının en yüksek değeri $m - 1$ olabilmektedir (Loebenberger & Nüsken, 2013).

Örnek 2.25. *Çizelge 2.10'da verilmiş olan, $F_2^3 \rightarrow F_2^3$'e tanımlı S-kutusunun doğrusal dal sayısı takip edildiği gibi hesaplanmaktadır:*
Doğrusal Yaklaşım Tablosu Çizelge 2.12'de verilmiş olan 3×3 *boyutlu S-kutusunun, Eşitlik 2.10'a göre hesaplamaları Çizelge 2.27'de incelenmiştir. Çizelge 2.27'de, Eşitlik 2.10'a göre hesaplamaya dahil edilmeyen değerler "✗" olarak ifade edilmiştir.*

*Eşitlik 2.10'a ve Çizelge 2.27'deki en küçük değere göre, Çizelge 2.12'de verilmiş olan S-kutusunun doğrusal dal sayısı **2** olarak tespit edilmiştir.*

Çizelge 2.27. 3 × 3 S-Kutusu Doğrusal Dal Sayısı İncelemesi

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**
0	✗	✗	✗	✗	✗	✗	✗	✗
1	✗	✗	✗	✗	2	3	3	4
2	✗	2	✗	3	✗	3	✗	4
3	✗	3	✗	4	3	✗	4	✗
4	✗	2	2	✗	2	✗	✗	4
5	✗	3	3	✗	✗	4	4	✗
6	✗	✗	3	4	3	4	✗	✗
7	✗	✗	4	5	✗	✗	5	6

Bir S-kutusunu byte dizisi şeklinde parametre olarak alıp, S-kutusunun doğrusal dal sayısını hesaplayan, C# programlama dili ile geliştirilme yapılmış kod bloğu aşağıda belirtilmiştir. Hamming ağırlıklarını hesaplamak için kullanılan dönüşümler, geliştirme algoritmasından kaynaklanmaktadır. Bir S-kutusunun, doğrusal dal sayısının hesaplanması için örnek algoritma olarak sunulmuştur.

```
public static int DogrusalDalSayisiHesabi(byte[] perm)
    {   int dogrusalDalSayisiDegeri = int.MaxValue;
        var check = LAT.GenerateLAT(perm);
        for (int i = 1; i < perm.Length; i++)
        {   for(int j = 0; j < perm.Length; j++)
            {   if (check[i,j] != 0)
                {
                    string girdiBinaryDegeri =
   hexCharacterToBinary[decimalToHexCharacter[i]];
                    string ciktiBinaryDegeri =
   hexCharacterToBinary[decimalToHexCharacter[j]];
                    int karsilastirmaDegeri = HammingWeight(
   girdiBinaryDegeri) + HammingWeight(ciktiBinaryDegeri);
                    if (karsilastirmaDegeri <
   dogrusalDalSayisiDegeri)
                    {
                        dogrusalDalSayisiDegeri =
   karsilastirmaDegeri;
                    }
                }
            }
        }
            return dogrusalDalSayisiDegeri;
        }
```

2.2.7.2 Diferansiyel Dal Sayısı (Differential Branch Number - DBN)

Boyutu $m \times m$ olan, $F_2^m \rightarrow F_2^m$'e tanımlı bir S-kutusunda $a, b \in F_2^m$ olduğunda; S-kutusunun *Diferansiyel Dal Sayısı (Differential Branch Number - DBN)* Eşitlik 2.11 ile ifade edilmektedir (Sarkar vd., 2019). Bir S-kutusunun diferansiyel dal sayısı, S-kutusunun Fark Dağılım Tablosu ve Doğrusal Yaklaşım Tablosu'ndan bağımsız olarak hesaplanmaktadır (H. Kim vd., 2021).

$$DBN(S) = min_{a \neq b}\{wt(a \oplus b) + wt(S(a) \oplus S(b))\} \tag{2.11}$$

Bir S-kutusunun boyutunun $m \times m$ olması durumunda, diferansiyel dal sayısının en büyük değeri $m-1$ şeklinde olmaktadır (Loebenberger & Nüsken, 2013).

Çizelge 2.28. 3 × 3 S-Kutusunun Diferansiyel Dal Sayısı İncelemesi ($a = [0-3]$)

$wt(0 \oplus 1) + wt(S(0) \oplus S(1)) = 1 + 2 = 3$
$wt(0 \oplus 2) + wt(S(0) \oplus S(2)) = 1 + 1 = 2$
$wt(0 \oplus 3) + wt(S(0) \oplus S(3)) = 2 + 2 = 4$
$wt(0 \oplus 4) + wt(S(0) \oplus S(4)) = 1 + 3 = 4$
$wt(0 \oplus 5) + wt(S(0) \oplus S(5)) = 2 + 2 = 4$
$wt(0 \oplus 6) + wt(S(0) \oplus S(6)) = 2 + 1 = 3$
$wt(0 \oplus 7) + wt(S(0) \oplus S(7)) = 3 + 1 = 4$
$wt(1 \oplus 0) + wt(S(1) \oplus S(0)) = 1 + 2 = 3$
$wt(1 \oplus 2) + wt(S(1) \oplus S(2)) = 2 + 1 = 3$
$wt(1 \oplus 3) + wt(S(1) \oplus S(3)) = 1 + 2 = 3$
$wt(1 \oplus 4) + wt(S(1) \oplus S(4)) = 2 + 1 = 3$
$wt(1 \oplus 5) + wt(S(1) \oplus S(5)) = 1 + 2 = 3$
$wt(1 \oplus 6) + wt(S(1) \oplus S(6)) = 3 + 1 = 4$
$wt(1 \oplus 7) + wt(S(1) \oplus S(7)) = 2 + 3 = 5$
$wt(2 \oplus 0) + wt(S(2) \oplus S(0)) = 1 + 1 = 2$
$wt(2 \oplus 1) + wt(S(2) \oplus S(1)) = 2 + 1 = 3$
$wt(2 \oplus 3) + wt(S(2) \oplus S(3)) = 1 + 1 = 2$
$wt(2 \oplus 4) + wt(S(2) \oplus S(4)) = 2 + 2 = 4$
$wt(2 \oplus 5) + wt(S(2) \oplus S(5)) = 3 + 3 = 6$
$wt(2 \oplus 6) + wt(S(2) \oplus S(6)) = 1 + 2 = 3$
$wt(2 \oplus 7) + wt(S(2) \oplus S(7)) = 2 + 2 = 4$
$wt(3 \oplus 0) + wt(S(3) \oplus S(0)) = 2 + 2 = 4$
$wt(3 \oplus 1) + wt(S(3) \oplus S(1)) = 1 + 2 = 3$
$wt(3 \oplus 2) + wt(S(3) \oplus S(2)) = 1 + 1 = 2$
$wt(3 \oplus 4) + wt(S(3) \oplus S(4)) = 3 + 1 = 4$
$wt(3 \oplus 5) + wt(S(3) \oplus S(5)) = 2 + 2 = 4$
$wt(3 \oplus 6) + wt(S(3) \oplus S(6)) = 2 + 3 = 5$
$wt(3 \oplus 7) + wt(S(3) \oplus S(7)) = 1 + 1 = 2$

Örnek 2.26. *Çizelge 2.10'da verilmiş olan,* $F_2^3 \rightarrow F_2^3$*'e tanımlı S-kutusunun diferansiyel dal sayısı takip edildiği gibi hesaplanmaktadır:*
Boyutu 3×3 *olan S-kutusunun* $a = [0-3]$ *ve* $a = [4-7]$ *değerleri için, Eşitlik 2.11'i kullanarak yapılan hesaplamalar sırasıyla Çizelge 2.28 ve Çizelge 2.29'da gösterilmiştir. Çizelge 2.28 ve Çizelge 2.29'daki hesaplamaların en küçük değerine göre, Çizelge 2.10'da verilmiş olan S-kutusunun diferansiyel dal sayısı* ***2*** *olarak tespit edilmiştir.*

Çizelge 2.29. 3×3 S-Kutusunun Diferansiyel Dal Sayısı İncelemesi ($a = [4-7]$)

$wt(4 \oplus 0) + wt(S(4) \oplus S(0)) = 1 + 3 = 4$
$wt(4 \oplus 1) + wt(S(4) \oplus S(1)) = 2 + 1 = 3$
$wt(4 \oplus 2) + wt(S(4) \oplus S(2)) = 2 + 2 = 4$
$wt(4 \oplus 3) + wt(S(4) \oplus S(3)) = 3 + 1 = 4$
$wt(4 \oplus 5) + wt(S(4) \oplus S(5)) = 1 + 1 = 2$
$wt(4 \oplus 6) + wt(S(4) \oplus S(6)) = 1 + 2 = 3$
$wt(4 \oplus 7) + wt(S(4) \oplus S(7)) = 2 + 2 = 4$
$wt(5 \oplus 0) + wt(S(5) \oplus S(0)) = 2 + 2 = 4$
$wt(5 \oplus 1) + wt(S(5) \oplus S(1)) = 1 + 2 = 3$
$wt(5 \oplus 2) + wt(S(5) \oplus S(2)) = 3 + 3 = 6$
$wt(5 \oplus 3) + wt(S(5) \oplus S(3)) = 2 + 2 = 4$
$wt(5 \oplus 4) + wt(S(5) \oplus S(4)) = 1 + 1 = 2$
$wt(5 \oplus 6) + wt(S(5) \oplus S(6)) = 2 + 1 = 3$
$wt(5 \oplus 7) + wt(S(5) \oplus S(7)) = 1 + 1 = 2$
$wt(6 \oplus 0) + wt(S(6) \oplus S(0)) = 2 + 1 = 3$
$wt(6 \oplus 1) + wt(S(6) \oplus S(1)) = 3 + 1 = 4$
$wt(6 \oplus 2) + wt(S(6) \oplus S(2)) = 1 + 2 = 3$
$wt(6 \oplus 3) + wt(S(6) \oplus S(3)) = 2 + 3 = 5$
$wt(6 \oplus 4) + wt(S(6) \oplus S(4)) = 1 + 2 = 3$
$wt(6 \oplus 5) + wt(S(6) \oplus S(5)) = 2 + 1 = 3$
$wt(6 \oplus 7) + wt(S(6) \oplus S(7)) = 1 + 2 = 3$
$wt(7 \oplus 0) + wt(S(7) \oplus S(0)) = 3 + 1 = 4$
$wt(7 \oplus 1) + wt(S(7) \oplus S(1)) = 2 + 3 = 5$
$wt(7 \oplus 2) + wt(S(7) \oplus S(2)) = 2 + 2 = 4$
$wt(7 \oplus 3) + wt(S(7) \oplus S(3)) = 1 + 1 = 2$
$wt(7 \oplus 4) + wt(S(7) \oplus S(4)) = 2 + 2 = 4$
$wt(7 \oplus 5) + wt(S(7) \oplus S(5)) = 1 + 1 = 2$
$wt(7 \oplus 6) + wt(S(7) \oplus S(6)) = 1 + 2 = 3$

Bir S-kutusunu byte dizisi şeklinde parametre olarak alıp, diferansiyel dal sayısını hesaplayıp, döndüren C# programlama dili ile geliştirilme yapılmış kod bloğu aşağıda gösterilmiştir. S-kutusunun, diferansiyel dal sayısının hesaplanması için örnek algoritma olarak sunulmuştur.

```
public static int DiferansiyelDalSayisi(byte[] perm)
    {
        int diferansiyelDalSayisiSayac = int.MaxValue;
        for (int i = 0; i < perm.Length; i++)
        {
            for(int j = 0;j < perm.Length; j++)
            {
                if (i != j)
                {
                    int girdiDecimalDeger = i;
                    int ciktiDecimalDeger = j;
                    int ilkHammingAgirlik = HammingWeight(
hexCharacterToBinary[decimalToHexCharacter[girdiDecimalDeger ^
 ciktiDecimalDeger]]);
                    girdiDecimalDeger = hexCharacterToDecimal[
Convert.ToChar(perm[girdiDecimalDeger])];
                    ciktiDecimalDeger = hexCharacterToDecimal[
Convert.ToChar(perm[ciktiDecimalDeger])];
                    int ikinciHammingAgirlik = HammingWeight(
hexCharacterToBinary[decimalToHexCharacter[girdiDecimalDeger ^
 ciktiDecimalDeger]]);
                    int karsilastirmaDeger = ilkHammingAgirlik +
ikinciHammingAgirlik;
                    if (karsilastirmaDeger <
diferansiyelDalSayisiSayac)
                    {
                        diferansiyelDalSayisiSayac =
karsilastirmaDeger;
                    }
                }
            }
        }
        return diferansiyelDalSayisiSayac;
    }
```

2.2.8 Frekans İncelemesi

Bir S-kutusunun; diferansiyel tekdüzelik ve doğrusallık frekanslarının incelenmesi; S-kutusunun diferansiyel ve doğrusal kriptoanaliz saldırılara karşı dayanıklılığını ölçümlemekte kullanılabilmektedir (Lu vd., 2022). Bir S-kutusunun diferansiyel tekdüzelik ve doğrusallık frekansları, tez çalışmasında incelenen kriptografik özelliklerdendir.

2.2.8.1 Diferansiyel Tekdüzelik Frekansı (Frequency of Differential Uniformity)

Bir S-kutusunun Fark Dağılım Tablosu'ndan elde edilen en yüksek değer ((0, 0) konumu hariç), S-kutusunun diferansiyel tekdüzeliği (differential uniformity) olmaktadır. Bir S-kutusunun diferansiyel tekdüzeliği; $\mathcal{U}(S)$ olarak temsil edilmektedir (Bao vd., 2019).

Bir S-kutusunun Fark Dağılım Tablosu'ndaki, diferansiyel tekdüzeliğin tekrar sayısı; *Diferansiyel Tekdüzelik Frekansı (Frequency of Differential Uniformity)* olarak ifade edilmektedir. Bir S-kutusunun diferansiyel tekdüzelik frekansı; $\#\mathcal{U}(S)$ olarak belirtilmektedir.

Boyutu $m \times m$ olan S-kutusunun; Fark Dağılım Tablosu'nda a giriş farkı satır değerine; b çıkış farkı sütun değerine karşılık gelmektedir. S: $F_2^m \rightarrow F_2^m$'e tanımlanan bir S-kutusunun diferansiyel tekdüzelik frekansı, Eşitlik 2.12'de ifade edilmiştir (Bao vd., 2019).

$$\#\mathcal{U}(S) = \#\{(a,b)|DDT(a,b) = \mathcal{U}(S), a, b \in F_2^m \setminus \{0\}\} \tag{2.12}$$

Örnek 2.27. *GIFT'in S-kutusunun diferansiyel tekdüzelik frekansı takip edildiği gibi hesaplanmaktadır:*
S-kutusu Çizelge 2.24'te verilmiş olan GIFT'in, Çizelge 2.30'a göre en büyük Fark Dağılım Tablosu değeri 6 olmaktadır.
Çizelge 2.30 üzerinde, GIFT'in diferansiyel tekdüzeliğinin tekrar ettiği konumlar, daire içinde gösterilmiştir.
*Çizelge 2.30'daki dairelerin toplam sayısından; GIFT'e ait S-kutusunun diferansiyel tekdüzelik frekansı **2** olarak elde edilmiştir.*

Giriş ve çıkışı m-bit olan bir S-kutusunu byte dizi girdisi olarak alan, S-kutusunun diferansiyel tekdüzelik frekansını hesaplayıp geri döndüren fonksiyonun, C# programlama dili ile kodlanmış hali aşağıda belirtilmiştir.

```
public static int DiferansiyelDagilimFrekansi(byte[] perm, int
   maxDDT)
        {    int frakansDDT = 0;
            var check = DDT.GenerateDDT(perm);
            for (int i = 0; i < perm.Length; i++)
            {   for (int j = 0; j < perm.Length; j++)
                {  if (!(i == 0 && j == 0) && check[i, j] ==
   maxDDT)
                    { frakansDDT++;}
                }
            }
            return frakansDDT;
        }
```

Çizelge 2.30. GIFT S-Kutusunun Diferansiyel Tekdüzelik Frekans İncelemesi

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	0	2	2	0	2	2	2	2	2	0	0	2
2	0	0	0	0	0	4	4	0	0	2	2	0	0	2	2	0
3	0	0	0	0	0	2	2	0	2	0	0	2	2	2	2	2
4	0	0	0	2	0	4	0	⑥	0	2	0	0	0	2	0	0
5	0	0	2	0	0	2	0	0	2	0	0	0	2	2	2	4
6	0	0	4	⑥	0	0	0	2	0	0	2	0	0	0	2	0
7	0	0	2	0	0	2	0	0	2	2	2	4	2	0	0	0
8	0	0	0	4	0	0	0	4	0	0	0	4	0	0	0	4
9	0	2	0	2	0	0	2	2	2	0	2	0	2	2	0	0
A	0	4	0	0	0	0	4	0	0	2	2	0	0	2	2	0
B	0	2	0	2	0	0	2	2	2	2	0	0	2	0	2	0
C	0	0	4	0	4	0	0	0	2	0	2	0	2	0	2	0
D	0	2	2	0	4	0	0	0	0	0	2	2	0	2	0	2
E	0	4	0	0	4	0	0	0	2	2	0	0	2	2	0	0
F	0	2	2	0	4	0	0	0	0	2	0	2	0	0	2	2

2.2.8.2 Doğrusallık Frekansı (Frequency of Linearity)

Boyutu $m \times m$ olan, $F_2^m \rightarrow F_2^m$'e tanımlı bir S-kutusunda, $\alpha \in F_2^m$ ve $\beta \in F_2^m$ olduğunda; S-kutusunun Walsh dönüşümü (Walsh transform) ve Walsh spektrumu (Walsh spectrum); $\mathcal{W}_S(\alpha, \beta)$ olmaktadır (Bao vd., 2019). $F_2^m \rightarrow F_2^m$'e tanımlı bir S-kutusunun Walsh dönüşümü ve Walsh spektrumu; Eşitlik 2.13'te gösterilmektedir.

$$\mathcal{W}_S(\alpha, \beta) = \sum_{x \in F_2^m} (-1)^{\alpha \cdot x \oplus \beta \cdot S(x)} \tag{2.13}$$

Bir S-kutusunun $\mathcal{W}_S(\alpha, \beta)$'den elde edilen en büyük mutlak değeri ((0, 0) konumu hariç), S-kutusunun doğrusallığı (linearity) olmaktadır. Bir S-kutusunun doğrusallığı; $\mathcal{L}(S)$ olarak temsil edilmektedir (Bao vd., 2019).

S: $F_2^m \rightarrow F_2^m$'e tanımlı, $\alpha \in F_2^m$ ve $\beta \in F_2^m$ ise; bir S-kutusunun doğrusallığı Eşitlik 2.14'te belirtilmiştir.

$$\mathcal{L}(S) = max_{\alpha,\beta \in F_2^m \setminus \{0\}} |\mathcal{W}_S(\alpha, \beta)| \tag{2.14}$$

Bir S-kutusunun doğrusallık frekansı; $\#\mathcal{L}(S)$ ile temsil edilmektedir. S: $F_2^m \rightarrow F_2^m$'e tanımlanan bir S-kutusunun doğrusallık frekansı, Eşitlik 2.15'te ifade edilmiştir (Bao vd., 2019).

$$\#\mathcal{L}(S) = \#\{(\alpha, \beta) | \mathcal{W}_S(\alpha, \beta) = \mathcal{L}(S), \alpha, \beta \in F_2^m \setminus \{0\}\} \tag{2.15}$$

Bir S-kutusunun Doğrusal Yaklaşım Tablosu'nun her bir satır ve sütunu sırasıyla; Γ_A, Γ_B olduğunda, $\mathcal{W}_S(\alpha, \beta)$ ile arasındaki ilişki Eşitlik 2.16'da ifade edilmiştir.

$$LAT(\Gamma_A, \Gamma_B) = \frac{1}{2}\mathcal{W}_S(\alpha, \beta) \tag{2.16}$$

Eşitlik 2.16'daki ilişkiye göre; $m \times m$ boyutlu bir S-kutusunun doğrusallık frekansı; Eşitlik 2.17 şeklinde de ifade edilebilmektedir.

$$\#\mathcal{L}(S) = \#\{(\Gamma_A, \Gamma_B) | LAT(\Gamma_A, \Gamma_B) = max_{\Gamma_A, \Gamma_B \in F_2^m \setminus \{0\}} |LAT(\Gamma_A, \Gamma_B))|\} \tag{2.17}$$

Eşitlik 2.17'ye göre tanımlaması $F_2^m \rightarrow F_2^m$'e olan, $m \times m$ boyutunda bir S-kutusunun doğrusallık frekansı; S-kutuna ait Doğrusal Yaklaşım Tablosu'ndaki en büyük mutlak değerin, Doğrusal Yaklaşım Tablosu'ndaki tekrar sayısına karşılık gelmektedir.

Örnek 2.28. *GIFT'in S-kutusunun doğrusallık frekansı, takip edildiği gibi hesaplanmaktadır:*
Çizelge 2.24'te S-kutusu verilmiş olan GIFT'in, Doğrusal Yaklaşım Tablosu'nda en büyük mutlak değeri 4 olduğundan dolayı, Çizelge 2.31'de, Doğrusal Yaklaşım Tablosu üzerindeki mutlak değeri 4 olan konumlar daireler ile gösterilmiştir.
Bu dairelerin toplam sayısına göre, GIFT S-kutusu için doğrusallık frekansı ***36*** *olarak elde edilmiştir.*

Boyutu $m \times m$ olan bir S-kutusunun, doğrusallık frekansının hesaplanmasının C# programlama dili ile kodlanmış hali aşağıda belirtilmiştir.

```
public static int DogrusallikFrekansi(byte[] perm, int maxLAT)
      {
          int frekansLAT = 0;
          var check = LAT.GenerateLAT(perm);
          for (int i = 0; i < perm.Length; i++)
          {   for (int j = 0; j < perm.Length; j++)
              {   if (!(i == 0 && j == 0) && Math.Abs(2 *
 check[i, j]) == Math.Abs(2 * maxLAT))
                      {frekansLAT++;}
              }
          }
          return frekansLAT;
      }
```

Çizelge 2.31. GIFT S-Kutusu Doğrusallık Frekans Değer İncelemesi

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	0	0	2	-2	-2	2	④	0	0	**-4**	-2	-2	-2	-2
2	0	0	0	**-4**	0	④	0	0	2	2	2	-2	2	-2	2	2
3	0	0	0	**-4**	-2	-2	2	-2	2	-2	-2	-2	0	④	0	0
4	0	0	0	0	0	0	**-4**	**-4**	0	0	0	0	0	0	④	**-4**
5	0	0	0	0	2	-2	2	-2	0	④	④	0	2	2	-2	-2
6	0	0	0	**-4**	④	0	0	0	-2	-2	-2	2	2	-2	-2	-2
7	0	0	0	④	2	2	2	-2	2	-2	-2	-2	④	0	0	0
8	0	0	0	0	0	**-4**	0	**-4**	0	0	0	0	0	**-4**	0	④
9	0	0	0	0	-2	-2	2	2	④	0	0	④	2	-2	2	-2
A	0	0	**-4**	0	0	0	④	0	-2	-2	2	-2	-2	-2	2	-2
B	0	0	④	0	2	-2	2	2	-2	2	-2	-2	0	0	④	0
C	0	④	④	0	0	0	0	0	0	**-4**	④	0	0	0	0	0
D	0	**-4**	④	0	-2	2	2	-2	0	0	0	0	-2	-2	-2	-2
E	0	**-4**	0	0	④	0	0	0	2	-2	2	2	-2	2	2	2
F	0	**-4**	0	0	-2	-2	-2	2	-2	-2	2	-2	④	0	0	0

2.2.9 Boomerang Bağlantı Tablosu (Boomerang Connectivity Table - BCT)

Bir S-kutusunun, diğer kriptografik özelliklerden bağımsız olarak booomerang özellikli ataklara karşı dayanıklılığını ölçümlemek için, *Boomerang Bağlantı Tablosu (Boomerang Connectivity Table - BCT)* kullanılmaktadır (Cid vd., 2018).

S-kutusunun boyutu $m \times m$ olduğunda, giriş ve çıkış değerleri kullanılarak $2^m \times 2^m$ boyutunda Boomerang Bağlantı Tablosu elde edilebilmektedir (Cid vd., 2018). $F_2^m \rightarrow F_2^m$'e tanımlı bir S-kutusunun Boomerang Bağlantı Tablosu'nun; girdi değeri (input difference) a, çıktı değeri (output difference) b, $a \in F_2^m$ ve $b \in F_2^m$ olarak ifade edilmektedir. Bir S-kutusunun Boomerang Bağlantı Tablosu'nun her hücresi; $\beta(a, b)$ olarak gösterilmektedir. Boomerang Bağlantı Tablosu'nun hücrelerinin hesaplanması için Eşitlik 2.18 kullanılmaktadır.

$$\beta(a, b) = \#\{x \in F_2^m | S^{-1}(S(x) \oplus b) \oplus S^{-1}(S(x \oplus a) \oplus b) = a\} \tag{2.18}$$

Eşitlik 2.18'de kullanılan, $F_2^m \rightarrow F_2^m$'e tanımlı, $a \in F_2^m$ ve $b \in F_2^m$ olması durumunda, bir S-kutusunun tersi alınırken her a ve b; $S(a) = b \Rightarrow S^{-1}(b) = a$ işlemlerinden geçirilmektedir (Muthavhine & Sumbwanyambe, 2022).

Örnek 2.29. *Serpent_S0 S-kutusu ve tersi Çizelge 2.32'de gösterilmiştir.*

Çizelge 2.32. Serpent_S0 S-Kutusu ve S-Kutusunun Tersi

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
S(×)	3	8	F	1	A	6	5	B	E	D	4	2	7	0	9	C
S^{-1}**(×)**	D	3	B	0	A	6	5	C	1	E	4	7	F	9	8	2

Boyutu $m \times m$ olan bir S-kutusunu, byte dizi girdisi olarak alan; S-kutusunun Boomerang Bağlantı Tablosu'nu hesaplayıp geri döndüren fonksiyonun, C# programlama dili ile kodlanmış hali aşağıda belirtilmiştir. Kullanılan dönüştürme işlemleri, algoritmanın ihtiyacından kaynaklanmaktadır.

```
public static int[,] BCT_Olustur(byte[] input)
      {
          int[,] BCT = new int[input.Length, input.Length];

          for (int p1 = 0; p1 < input.Length; p1++)
              for (int p2 = 0; p2 < input.Length; p2++)
              {
                var BCT_hucre_degeri = 0;
                for (int i = 0; i < input.Length; i++)
                  {
                      var dogrula1 = hexCharacterToDecimal[
 Convert.ToChar(input[i])] ^ p2;
                      var kontrol1 = hexCharacterToAscii[
 decimalToHexCharacter[dogrula1]];
                      var ilk = Array.FindIndex(input, element1
  => element1 == kontrol1);
                      var dogrula2 = hexCharacterToDecimal[
 Convert.ToChar(input[i ^ p1])] ^ p2;
                      var kontrol2 = hexCharacterToAscii[
 decimalToHexCharacter[dogrula2]];
                      var ikinci = Array.FindIndex(input,
 element2 => element2 == kontrol2);
                      var total = ilk ^ ikinci;
                      if(total == p1)
                      {
                          BCT_hucre_degeri++;
                      }
                  }
                  BCT[p1, p2] = BCT_hucre_degeri;
              }

          return output;
      }
```

Çizelge 2.33. Panda S-Kutusu

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(×)	0	1	3	2	F	C	9	B	A	6	8	7	5	E	D	4

Hafif sıklet blok şifre olan Panda'ya ait S-kutusu Çizelge 2.33'te verilmiştir (Peigen, 2023).

Çizelge 2.34. Panda S-Kutusu Fark Dağılım Tablosu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	4	2	2	0	0	0	0	0	2	0	2	2	0	0	2
2	0	2	2	4	0	0	2	2	2	0	2	0	0	0	0	0
3	0	2	4	2	2	2	0	0	0	0	0	0	0	2	2	0
4	0	0	0	2	0	2	0	0	2	2	2	0	0	2	0	4
5	0	0	0	2	2	0	0	0	2	0	2	2	4	0	2	0
6	0	0	2	0	0	0	0	2	0	4	2	0	2	2	2	0
7	0	0	2	0	0	0	2	0	2	0	0	4	0	2	2	2
8	0	0	2	0	2	2	0	2	0	0	4	2	0	0	0	2
9	0	2	0	0	2	0	4	0	0	2	2	2	0	2	0	0
A	0	0	2	0	2	2	2	0	4	2	0	0	2	0	0	0
B	0	2	0	0	0	2	0	4	2	2	0	2	0	0	2	0
C	0	2	0	0	0	4	2	0	0	0	2	0	2	0	2	2
D	0	0	0	2	2	0	2	2	0	2	0	0	0	0	4	2
E	0	0	0	2	0	2	2	2	0	0	0	2	2	4	0	0
F	0	2	0	0	4	0	0	2	2	0	0	0	2	2	0	2

Çizelge 2.33'te verilmiş olan Panda'nın S-kutusu için, her bir hücresi hesaplanırken Eşitlik 2.7 kullanıldığında oluşan Fark Dağılım Tablosu, Çizelge 2.34'te gösterilmiştir.

Örnek 2.30. *Panda S-kutusuna ait Boomerang Bağlantı Tablosu'nun hesaplanması takip edildiği gibi olmaktadır:*
S-kutusu Çizelge 2.33'te verilmiş olan Panda S-Kutusu için, Çizelge 2.35'te belirtilen Boomerang Bağlantı Tablosu'nun her bir hücresinin değeri hesaplanırken, Eşitlik 2.18 kullanılmıştır.

Çizelge 2.33'te verilen Panda S-Kutusu'nun Fark Dağılım Tablosu ve Boomerang Bağlantı Tablosu sırasıyla Çizelge 2.34 ve Çizelge 2.35'te gösterilmiştir. Tablolar incelendiğinde, Panda'ya ait S-kutusunun Fark Dağılım Tablosu'nda 0'dan farklı değer bulunduran konumların, Boomerang Bağlantı Tablosu'ndaki aynı konumdaki değeri, Fark Dağılım Tablosu'ndaki değere eşit veya daha büyüktür. Buna *S-box Switch* denilmektedir. Ek olarak, Boomerang Bağlantı Tablosu'ndaki ilk satır ve ilk sütun m-bit S-kutusu için 2^m değerini almaktadır (Cid vd., 2018).

Çizelge 2.35. Panda S-Kutusu Boomerang Bağlantı Tablosu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16	16
1	16	4	6	6	0	0	0	0	0	2	0	2	2	0	0	2
2	16	6	6	4	0	0	2	2	2	0	2	0	0	0	0	0
3	16	6	4	6	2	2	0	0	0	0	0	0	0	2	2	0
4	16	0	0	2	0	6	0	0	2	2	6	0	0	2	0	4
5	16	0	0	2	6	0	0	0	6	0	2	2	4	0	2	0
6	16	0	2	0	0	0	0	6	0	4	2	0	2	2	6	0
7	16	0	2	0	0	0	6	0	2	0	0	4	0	6	2	2
8	16	0	2	0	2	6	0	2	0	0	4	2	0	0	0	6
9	16	2	0	0	2	0	4	0	0	2	2	6	0	6	0	0
A	16	0	2	0	6	2	2	0	4	2	0	0	6	0	0	0
B	16	2	0	0	0	2	0	4	2	6	0	2	0	0	6	0
C	16	2	0	0	0	4	2	0	0	0	6	0	2	0	2	6
D	16	0	0	2	2	0	2	6	0	6	0	0	0	0	4	2
E	16	0	0	2	0	2	6	2	0	0	0	6	2	4	0	0
F	16	2	0	0	4	0	0	2	6	0	0	0	6	2	0	2

2.2.9.1 Boomerang Bağlantı Tablosu Tekdüzeliği (Boomerang Connectivity Table Uniformity - BCTU)

Boomerang Bağlantı Tablosu Tekdüzeliği (Boomerang Connectivity Table Uniformity - BCTU); bir S-kutusunun boomerang saldırılarına karşı dayanıklılığını ölçümlemek için incelenen kriptografik özellik olmaktadır (Boura & Canteaut, 2018). Bir S-kutusunun BCTU değeri, $\mathcal{BCTU}(S)$ olarak temsil edilmektedir.

$F_2^m \rightarrow F_2^m$'e tanımlı bir S-kutusunun, BCTU değerinin hesaplaması; Boomerang Bağlantı Tablosu'nun 0. satırı ve 0. sütununda bulunan değerlerin dışında, Boomerang Bağlantı Tablosu'nda bulunan değerlerden maksimum olanına karşılık gelmektedir. Boyutu $m \times m$ olan bir S-kutusunun BCTU değeri; Eşitlik 2.19'da belirtilmektedir.

$$\mathcal{BCTU}(S) = max_{a,b \in F_2^m, a \neq 0, b \neq 0} \beta(a,b) \tag{2.19}$$

Örnek 2.31. *Panda S-kutusuna ait BCTU değerinin hesaplanması takip edildiği gibi olmaktadır:*
*Çizelge 2.35'te verilen Boomerang Bağlantı Tablosu incelendiğinde, Eşitlik 2.19'a göre, Çizelge 2.33'te verilen hafif sıklet blok şifre olan Panda S-kutusunun BCTU değeri **6** olarak elde edilmektedir.*

2.2.10 Diferansiyel Doğrusal Bağlantı Tablosu (Differential Linear Connectivity Table - DLCT)

Bir S-kutusunun, diferansiyel-doğrusal kriptoanaliz saldırılarına karşı dayanıklılığını ölçümlemek için, *Diferansiyel Doğrusal Bağlantı Tablosu (Differential Linear Connectivity Table - DLCT)* kullanılmaktadır (Y. Liu vd., 2021).

S-kutusunun boyutu $m \times m$ olduğunda, giriş ve çıkış değerleri kullanılarak $2^m \times 2^m$ boyutunda Diferansiyel Doğrusal Bağlantı Tablosu oluşturulmaktadır (Bar-On vd., 2019). $F_2^m \rightarrow F_2^m$'e tanımlı bir S-kutusunun Diferansiyel Doğrusal Bağlantı Tablosu'nun; girdi değeri Δ, çıktı değeri λ, $\Delta \in F_2^m$ ve $\lambda \in F_2^m$ olarak ifade edilmektedir (Canteaut vd., 2019). Bir S-kutusunun Diferansiyel Doğrusal Bağlantı Tablosu'nun her hücresi; $DLCT_S(\Delta, \lambda)$ olarak temsil edilmektedir. Diferansiyel Doğrusal Bağlantı Tablosu'nun hücrelerinin hesaplanması için Eşitlik 2.20 kullanılmaktadır.

$$DLCT_S(\Delta, \lambda) = |\{x \in F_2^m | S(x) \cdot \lambda = S(x \oplus \Delta) \cdot \lambda\}| - 2^{m-1} \tag{2.20}$$

S: $F_2^m \rightarrow F_2^m$'e tanımlı bir S-kutusunu, byte dizi girdisi olarak alan, Diferansiyel Doğrusal Bağlantı Tablosu'nu hesaplayıp geri döndüren fonksiyonun, C# programlama dili ile kodlanmış hali aşağıda belirtilmiştir.

```
1       public static int[,] DLCT_Olustur(byte[] input)
2       {  int[,] DLCT = new int[input.Length, input.Length];
3           for(int p1 = 0; p1 < input.Length; p1++)
4           {   for(int p2 = 0; p2 < input.Length; p2++)
5               {   var DLCT_hucre_deger = 0;
6                   var DLCT_hucre_sayac = 0;
7                   for(int i = 0; i < input.Length; i++)
8                   {   byte kontrol1 = _dot((byte)p2,     (byte)
  hexCharacterToDecimal[Convert.ToChar(input[i])]);
9                       byte kontrol2 = _dot((byte)p2, (byte)
  hexCharacterToDecimal[Convert.ToChar(input[i ^ p1])]);
10                      if(kontrol1 == kontrol2)
11                          {DLCT_hucre_sayac++;}
12                  }
13                  DLCT_hucre_deger = (int)(DLCT_hucre_sayac - (
  Math.Pow(2, Math.Log2(input.Length) - 1)));
14                  DLCT[p1, p2] = DLCT_hucre_deger;
15              }
16          }
17          return DLCT;
18      }
```

2.2.10.1 Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği (Differential Linear Connectivity Table Uniformity - DLCTU)

Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği (Differential Linear Connectivity Table Uniformity - DLCTU); bir S-kutusunun diferansiyel-doğrusal saldırılarına karşı dayanıklılığını ölçümlemek için incelenen kriptografik özelliktir (Bar-On vd., 2019). Bir S-kutusunun DLCTU değeri $\mathcal{DLCTU}(S)$ olarak temsil edilmektedir.

$F_2^m \rightarrow F_2^m$'e tanımlı bir S-kutusunun, DLCTU değeri; Diferansiyel Doğrusal Bağlantı Tablosu'nun mutlak maksimum değerine karşılık gelmektedir (Tang, Mandal & Maitra, 2021). Boyutu $m \times m$ olan bir S-kutusunun DLCTU değeri, Eşitlik 2.21'de belirtilmektedir.

$$\mathcal{DLCTU}(S) = max_{\alpha,\beta \in F_2^m} |DLCT_S(\Delta, \lambda)| \tag{2.21}$$

Çizelge 2.36. KLEIN S-Kutusu

×	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S(×)	7	4	A	9	1	F	B	0	C	3	2	6	8	E	D	5

Örnek 2.32. *Hafif sıklet blok şifre olan KLEIN'in S-kutusuna ait Diferansiyel Doğrusal Bağlantı Tablosu'nun hesaplanması takip edildiği gibi olmaktadır:*
İnvolutif, 4×4 *boyutunda olan KLEIN'in S-kutusu Çizelge 2.36'da sunulmuştur (Peigen, 2023).*
KLEIN'in S-kutusuna ait Diferansiyel Doğrusal Bağlantı Tablosu, Çizelge 2.37'de gösterilmiştir.

Örnek 2.33. *KLEIN S-kutusuna ait DLCTU değerinin hesaplanması, takip edildiği gibi olmaktadır:*
Çizelge 2.37'de gösterilen Diferansiyel Doğrusal Bağlantı Tablosu'na ve Eşitlik 2.21'e göre; Diferansiyel Doğrusal Bağlantı Tablosu'nun mutlak değerce en büyük değeri, KLEIN S-kutusu için DLCTU ***8****'e karşılık gelmektedir.*

2.2.11 Bitslice Kapı Karmaşıklığı (Bitslice Gate Complexity - BGC)

Bitslice tekniğinin ilk uygulaması, DES algoritmasıyla ortaya çıkmıştır (Biham, 1997). Bitslice tekniğinin S-kutusu açısından değerlendirilmesinin temel amacı; $m \times m$ boyutunda olan bir S-kutusunun, mantıksal operatörler ile donanıma uygulanmasının maliyeti/karmaşıklığı hakkında analiz yapılabilmesini sağlamaktır (Bao vd., 2019).

Bir S-kutusunun *Bitslice Kapı Karmaşıklığı (Bitslice Gate Complexity - BGC)*, S-kutusunun donanıma uygulanmasındaki maliyeti hakkında ölçümleme yapmaya olanak

Çizelge 2.37. KLEIN S-Kutusunun Diferansiyel Doğrusal Bağlantı Tablosu

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
0	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	0	-4	4	0	-4	0	4	0	0	0	0	0	-4	-4	0
2	8	-4	0	-4	-4	4	-4	4	-4	0	4	0	0	0	0	0
3	8	0	0	-4	0	-4	0	0	0	-4	4	4	4	-4	0	-4
4	8	-4	0	0	0	-4	0	0	0	4	0	0	0	-4	0	0
5	8	0	-4	0	4	4	-4	0	0	0	0	-4	-4	4	0	-4
6	8	4	0	0	0	-4	0	0	0	0	0	-4	-4	-4	4	0
7	8	0	0	0	-4	0	4	0	-4	-4	0	0	0	4	-4	0
8	8	-4	0	0	0	0	4	0	0	0	0	-4	-4	0	0	0
9	8	0	0	4	-4	0	0	0	-4	0	0	0	0	0	0	-4
A	8	4	-4	-4	0	0	-4	0	0	-4	0	0	0	0	0	4
B	8	0	4	-4	0	0	0	0	4	0	0	-4	-4	0	-4	0
C	8	0	0	0	-4	0	0	-4	-4	0	-4	0	0	0	4	4
D	8	0	0	0	0	0	-4	-4	0	4	-4	0	4	0	-4	0
E	8	-4	-4	0	4	0	0	-4	4	-4	-4	4	0	0	0	0
F	8	0	4	0	0	0	0	-4	0	0	-4	0	0	0	0	-4

sağlamaktadır. S-kutusunun bitslice kapı karmaşıklığının düşük olması; yer değiştirme kutusunun uygulanmasında donanım maliyetinin düşük olması anlamına gelmektedir (Ullrich vd., 2011).

$F_2^m \rightarrow F_2^m$'e tanımlanan bir S-kutusunun, her vektörel çıkış Boole fonksiyonunun Cebirsel Gösterim Biçimi'ndeki XOR ve AND mantıksal kapı sayısının toplanmasıyla, S-kutusunun bitslice kapı karmaşıklığı hesaplanmaktadır.

Çizelge 2.38. Bitslice Kapı Karmaşıklığı Hesaplamak İçin S-Kutusu

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
S(×)	0	A	C	5	4	3	B	E	F	D	1	6	2	9	7	8

Örnek 2.34. *Çizelge 2.38'de verilen S-kutusunun, bitslice kapı karmaşıklığı hesaplaması takip edildiği gibi olmaktadır:*
Çizelge 2.38'de verilen, $F_2^4 \rightarrow F_2^4$'e tanımlı bir S-kutusuna ait olan doğruluk tablosu (truth table) Çizelge 2.39'da belirtilmiştir.
Çizelge 2.38'de verilen S-kutusunun, her vektörel çıkış Boole fonksiyonunun cebirsel ifadesi takip edildiği şekilde özetlenebilir:

$y_1(x_4, x_3, x_2, x_1) = x_1x_2 \oplus x_1x_3 \oplus x_2x_3 \oplus x_1x_2x_3 \oplus x_4 \oplus x_3x_4$
$y_2(x_4, x_3, x_2, x_1) = x_1 \oplus x_1x_2 \oplus x_2x_3 \oplus x_4 \oplus x_2x_4 \oplus x_1x_2x_4$
$y_3(x_4, x_3, x_2, x_1) = x_2 \oplus x_3 \oplus x_1x_3 \oplus x_4 \oplus x_1x_2x_4 \oplus x_1x_3x_4$
$y_4(x_4, x_3, x_2, x_1) = x_1 \oplus x_2 \oplus x_1x_3 \oplus x_4 \oplus x_1x_4 \oplus x_3x_4 \oplus x_2x_3x_4$

*S-kutusunun bitslice kapı karmaşıklığı hesabı yapılırken; ⊕ ifadesi **XOR** mantıksal kapısına, yan yana işlemler **AND** mantıksal kapısına (Örn: x_0x_2 için 1 AND mantıksal kapısı, $x_1x_2x_3$ için 2 AND mantıksal kapısı şeklinde) karşılık gelmektedir (Stoffelen, 2016).*
*Çizelge 2.38'de verilen S-kutusu için XOR mantıksal kapı sayısı toplamı **21** ve AND mantıksal kapı sayısı toplamı **21** olarak tespit edilmiştir.*
*Çizelge 2.38'de verilen S-kutusunun, AND ve XOR mantıksal kapı sayılarının toplamı diğer bir deyişle bitslice kapı karmaşıklığı **42** olmaktadır.*

Çizelge 2.39. Bitslice Kapı Karmaşıklığı Hesaplamak İçin S-Kutusu Doğruluk Tablosu

x_4	x_3	x_2	x_1	y_4	y_3	y_2	y_1
0	0	0	0	0	0	0	0
0	0	0	1	1	0	1	0
0	0	1	0	1	1	0	0
0	0	1	1	0	1	0	1
0	1	0	0	0	1	0	0
0	1	0	1	0	0	1	1
0	1	1	0	1	0	1	1
0	1	1	1	1	1	1	0
1	0	0	0	1	1	1	1
1	0	0	1	1	1	0	1
1	0	1	0	0	0	0	1
1	0	1	1	0	1	1	0
1	1	0	0	0	0	1	0
1	1	0	1	1	0	0	1
1	1	1	0	0	1	1	1
1	1	1	1	1	0	0	0

Tez çalışması kapsamında incelenmiş olan bitslice kapı karmaşıklığı; S-kutusunu vektörel çıkış Boole fonksiyonlarının cebirsel ifadelerinde, herhangi bir optimizasyon işleminden geçirilmeden oluşturulmuştur. S-kutusunun bitslice kapı karmaşıklığı için sadece XOR ve AND mantıksal kapıları işleme katılmıştır. İşleme katılan her iki mantıksal kapınında katsayı değeri "1" olarak kabul edilmiştir.

BÖLÜM 3

3 × 3 BOYUTUNDA TÜM İNVOLUTİF S-KUTULARININ KRİPTOGRAFİK ÖZELLİKLERİNİN İNCELEME SONUÇLARI

Tezin bu bölümünde, 3 × 3 boyutunda tüm involutif S-kutuları incelenmiş, kriptografik özelliklere göre karşılaştırılmalı sonuçlar özetlenmiştir. Kriptografik özelliklerine göre mümkün olan en iyi değerlere sahip olan, 3 × 3 boyutundaki involutif S-kutularının bitslice kapı karmaşıklıkları analiz edilmiştir.

3 × 3 boyutunda S-kutularının elde edilmesinde kullanılabilecek bijektif permütasyonlarının toplam sayısı $(2^3)! = 40,320$ kadar olmaktadır. Bölüm 2'de verilen, Şekil 2.2'deki hesaplamaya göre; $i(8) = 764$ tanesi involutif, bijektif permütasyon olmaktadır. Diğer bir deyişle, 3 × 3 boyutundaki olası tüm yer değiştirme kutuları içerisinden, $\%1,96$ kadarı involutif olma özelliğine sahiptir.

Çizelge 3.1. 3 × 3 Boyutunda İnvolutif S-Kutularının En Büyük Fark Dağılım Tablosu ve En Büyük Mutlak Doğrusal Yaklaşım Tablosu Değerleri Karşılaştırılması

S-Kutusu $m \times m$	**İnvolutif Permütasyonlar**	**İnvolutif Olma Özelliğine Sahip Permütasyonlar**		
		DDT-2 & LAT-2	**DDT-4 & LAT-4**	**DDT $\geqslant$ 6**
3 × 3	$i(8) = 764$	224	224	316

3 × 3 bijektif yer değiştirme kutularının (8!) permütasyonları incelenmiştir. Bu permütasyonlardan, involutif yapıda olanların; en büyük Fark Dağılım Tablosu değerleri ((0, 0) konumu hariç) ve en büyük mutlak Doğrusal Yaklaşım Tablosu değerleri ((0, 0) konumu hariç) açısından karşılaştırması, Çizelge 3.1'de sunulmuştur. Çizelge 3.1'de ifade edilen sonuçlar, takip edildiği şekilde özetlenebilir; 3 × 3 boyutunda 8! tane olan tüm bijektif S-kutusu permütasyonlarından, 764 tanesi involutif yapıda olmaktadır ve bunların içerisinden; en büyük Fark Dağılım Tablosu değeri/en büyük mutlak Doğrusal Yaklaşım

Tablosu değeri $2/2$ olan 224 tane, $4/4$ olan 224 tane S-kutusu tespit edilmiştir. Çizelge 3.1'deki son sütun; 316 tane involutif, 3×3 boyutunda S-kutularının, maksimum Fark Dağılım Tablosu değeri 6 ve 6'dan büyük olmaktadır.

S-kutuların doğrusal ve diferasiyel saldırılarına karşı dayanıklılığı için öncelikle en büyük Fark Dağılım Tablosu ve en büyük mutlak Doğrusal Yaklaşım Tablosu değerleri açısından mümkün olan en iyi S-kutularının seçilmesi gerekmektedir (Sağıroğlu vd., 2019). Boyutu $m \times m$ olan yer değiştirme kutusunun maksimum doğrusal olmama değeri; $2^{m-1} - 2^{m/2-1}$ şeklinde hesaplanmaktadır. Boyutu $m \times m$ olan bir yer değiştirme kutusunun doğrusal olmama durumu $NL_S = 2^{m-1} - |max(LAT_S)|$ eşitliği ile ortaya konulmaktadır (Sağıroğlu vd., 2019). Bijektif $m \times m$ boyutlu S-kutusu için, eşitliklerde m yerine 3 yazılıp gerekli hesaplamalar yapıldığında; en büyük mutlak Doğrusal Yaklaşım Tablosu değeri için 2 ve 4 değerlerinin, 3×3 boyutundaki S-kutusunun doğrusal olmama özelliğini koruması açısından kabul edilebilir olduğu hesaplanmıştır. Aynı zamanda S-kutusunun diferansiyel saldırılara dayanıklı olması için, en büyük Fark Dağılım Tablosu değerininde 2 ve 4 olması gerekmektedir. Bu sebeplerden dolayı 3×3 boyutunda, involutif S-kutularının en büyük Fark Dağılım Tablosu değeri/en büyük mutlak Doğrusal Yaklaşım Tablosu değeri; $2/2$ ve $4/4$ olanlar incelenmiştir.

Tez çalışmasında $F_2^m \rightarrow F_2^m$'e tanımlı S-kutularında, cebirsel derecenin $m-1$ olarak seçilip "Optimal" özelliklere dahil edilmesinin sebebi takip edildiği gibi özetlenmektedir: Cebirsel derecesi $m-1$'e eşit olan S-kutuları; cebirsel, küp vb. saldırılara karşı dayanıklı olduğu anlamına gelmektedir (Bao vd., 2019). S-kutularının doğrusal olmama (non-linear) özelliğinden dolayı tez kapsamında, "cebirsel derece < m-1" şeklinde olan S-kutuları incelenmemiştir. Yüksek cebirsel derecenin, S-kutusunu cebirsel saldırılara karşı daha dayanıklı hale getirmesi sebebiyle, tez çalışmasındaki incelemelerde *m*-bit S-kutuları için en yüksek cebirsel derece olan $m-1$ değerine odaklanılmıştır (Bao vd., 2019).

Tez kapsamında, en büyük Fark Dağılım Tablosu değeri, en büyük mutlak Doğrusal Yaklaşım Tablosu değeri ve cebirsel derece açısından en iyi değerlere sahip olan $m \times m$ boyutunda S-kutuları **Optimal** olarak değerlendirilmiştir. Bijektif, *m* bit giriş ve çıkış değerlerine sahip S-kutularının cebirsel derecesinin *"m - 1"* değerine eşit olması gerekmektedir (Bao vd., 2019). Bu sebeple S-kutuları, Çizelge 3.2'deki halleriyle incelenmiştir.

Çizelge 3.2. Fark Dağılım Tablosu, Doğrusal Yaklaşım Tablosu, Cebirsel Derece Açısından 3×3 Boyutunda İnvolutif S-Kutularının İncelenmesi

	AD = 1	**AD = 2**
DDT-2 & LAT-2	0	224
DDT-4 & LAT-4	224	0

Çizelge 3.3. 3 × 3 Boyutunda Optimal ve 2 Sabit Noktalı S-kutularının BIBO Örüntüsü İnceleme Sonuçları

BIBO Örüntü	**6**	**8**	**11**	**14**
#{S-kutusu}	32	48	96	48

Çizelge 3.2'de verilen sonuçlara göre tez çalışması kapsamında 3 × 3 boyutundaki involutif S-kutularının **"Optimal"** olarak tanımlanmasını sağlayan kriptografik özellikleri, takip edildiği şekilde olmaktadır:

- En büyük Fark Dağılım Tablosu değeri **2**
- En büyük mutlak Doğrusal Yaklaşım Tablosu değeri **2**
- Cebirsel derece **2**

Tez kapsamında, 3 × 3 boyutunda 224 tane, "optimal" diğer bir deyişle; en büyük Fark Dağılım Tablosu değeri **2**, en büyük mutlak Doğrusal Yaklaşım Tablosu değeri **2** ve cebirsel derece **2** olan S-kutuları belirlenmiştir. Bu S-kutuları diğer kriptografik özelliklere göre incelenerek, sonuçlar karşılaştırılmalı olarak analiz edilmiştir.

3.1 3 × 3 Boyutunda Optimal S-kutularının Sabit Nokta ve Doğrusal/Diferansiyel Dal Sayıları İnceleme Sonuçları

Tez kapsamında 3 × 3 boyutunda **"Optimal"** olarak tanımlanan S-kutularının tamamının 2 sabit noktası tespit edilmiştir. $F_2^3 \rightarrow F_2^3$'e tanımlı optimal S-kutularının tümünün, doğrusal dal sayısı 2 ve diferansiyel dal sayısı 2 olarak saptanmıştır. Sonuç olarak; incelenen 3 × 3 boyutunda optimal S-kutularının içerisinde; sabit nokta, doğrusal dal sayısı ve diferansiyel dal sayısı açısından 2'den farklı değere sahip S-kutusu bulunmamaktadır.

3.2 3 × 3 Boyutunda Optimal S-kutularının BIBO Örüntüsü İnceleme Sonuçları

3-bit giriş ve 3-bit çıkış olan S-kutuları içerisinde; involutif, en büyük Fark Dağılım Tablosu değeri 2, en büyük mutlak Doğrusal Yaklaşım Tablosu değeri 2, cebirsel derece 2, sabit nokta sayısı 2, doğrusal ve diferansiyel dal sayısı 2 olan S-kutuları içerisinde (224 tane S-kutusu) BIBO örüntüleri, Çizelge 3.3'te özetlenmiştir.

Çizelge 3.3'te ifade edilenlere göre; tez kapsamında incelenen 3-bit giriş ve çıkış değerlerine sahip, involutif, optimal, sabit nokta sayısı 2, doğrusal ve diferansiyel dal sayıları 2 olan S-kutularında; BIBO örüntüleri 6, 8, 11 ve 14 değerleri tespit edilmiştir.

3.3 3 × 3 Boyutunda Optimal S-kutularının Boomerang Bağlantı Tablosu Tekdüzeliği İnceleme Sonuçları

Tez çalışmasında incelenen 3-bit giriş ve çıkış değerlerine sahip, optimal S-kutuları içerisinde, BCTU sadece 2 değeri olarak tespit edilmiştir.

İncelenen 3-bit optimal S-kutularının 2 sabit nokta içeren, BIBO örüntü alt gruplarına göre BCTU değerlerinin incelenmesi, Çizelge 3.4'te sunulmuştur.

Çizelge 3.4. 3 × 3 Boyutunda Optimal 2 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri İnceleme Sonuçları

	#{BCTU = 2} S-Kutusu	**#{BIBO Örüntü} S-kutusu**
BIBO Örüntü = 6	32	32
BIBO Örüntü = 8	48	48
BIBO Örüntü = 11	96	96
BIBO Örüntü = 14	48	48

Çizelge 3.4'e göre; optimal özellikli, 3 × 3 boyutunda, doğrusal ve diferansiyel dal sayısı 2, sabit nokta sayısı 2 olan S-kutularının BCTU değerinin 2 olduğu ifade edilmektedir. Çizelge 3.4'ün ilk veri satırı takip edilen şekilde özetlenebilir: 3 × 3 boyutlu, optimal, sabit nokta sayısı 2 olan S-kutuları içerisinde 32 tanesinin BIBO örüntüsü 6 ve hepsinin BCTU değeri 2 olarak tespit edilmiştir.

3.4 3 × 3 Boyutunda Optimal S-kutularının BCTU Değeri ve Diferansiyel Tekdüzelik/Doğrusallık Frekans İnceleme Sonuçları

$F_2^3 \rightarrow F_2^3$'e tanımlı, involutif, 2 sabit noktalı S-kutularının, BIBO örüntü alt gruplarında BCTU değerlerine göre, diferansiyel tekdüzelik/doğrusallık frekanslarının incelenmesi Çizelge 3.5'te ifade edilmiştir.

Çizelge 3.5. 3 × 3 Boyutunda 2 Sabit Noktalı Optimal S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri ve Diferansiyel Tekdüzelik/Doğrusallık Frekanslarının İnceleme Sonuçları

	BCTU=2 & #{U}=28 & #{L}=28	**#{BIBO Örüntü & BCTU = 2}S-kutusu**
BIBO Örüntü = 6 & BCTU = 2	32	32
BIBO Örüntü = 8 & BCTU = 2	48	48
BIBO Örüntü = 11 & BCTU = 2	96	96
BIBO Örüntü = 14 & BCTU = 2	48	48

Tez çalışmasında incelenen; 3 × 3 boyutunda, involutif, optimal tüm S-kutularının BCTU değerleri 2 olarak tespit edilmiştir. Hepsinin diferansiyel tekdüzelik/doğrusallık frekanslarının $28/28$ olduğu saptanmıştır. Bu S-kutuları, Çizelge 3.5'te sunulmuştur.

Çizelge 3.5'e göre; BIBO örüntüsü 11 ve BCTU değeri 2 olan S-kutularının sonuçları, takip edilen şekilde özetlenebilir; 3-bit giriş-çıkış değerlerine sahip, optimal, sabit nokta sayısı 2, BCTU değeri 2, BIBO örüntüsü 11 olan 96 tane S-kutusunun; hepsinin diferansiyel tekdüzelik/doğrusallık frekansları $28/28$ olarak tespit edilmiştir.

3.5 3 × 3 Boyutunda Optimal S-kutularının DLCTU Değeri ve Diferansiyel Tekdüzelik/Doğrusallık Frekans İnceleme Sonuçları

3-bit involutif S-kutularının 2 sabit noktalı, BIBO örüntü alt gruplarına göre DLCTU değeri ve diferansiyel tekdüzelik/doğrusallık frekanslarının incelenmesi, Çizelge 3.6'da ifade edilmiştir.

Çizelge 3.6. 3 × 3 Boyutunda Optimal 2 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre DLCTU Değeri ve Diferansiyel Tekdüzelik/Doğrusallık Frekanslarının İnceleme Sonuçları

	DLCTU=4 & #{U}=28 & #{L}=28	**#{BIBO Örüntü & DLCTU = 4}S-kutusu**
BIBO Örüntü = 6 & DLCTU = 4	32	32
BIBO Örüntü = 8 & DLCTU = 4	48	48
BIBO Örüntü = 11 & DLCTU = 4	96	96
BIBO Örüntü = 14 & DLCTU = 4	48	48

Çizelge 3.6'ya göre; BIBO örüntüsü 8 ve DLCTU değeri 4 olan S-kutularının sonuçlarına yönelik özet takip edilen şekilde verilebilir; 3-bit giriş-çıkış değerlerine sahip, optimal, sabit nokta sayısı 2, DLCTU değeri 4, BIBO örüntüsü 8 olan 46 tane S-kutusunun; hepsinin diferansiyel tekdüzelik/doğrusallık frekansları $28/28$ olarak tespit edilmiştir.

Tez çalışmasında incelenen; 3 × 3 boyutunda, involutif, optimal tüm S-kutularının DLCTU değeri 4 olarak saptanmıştır. Tamamının diferansiyel tekdüzelik/doğrusallık frekansları $28/28$ olarak tespit edilmiştir.

3.6 3 × 3 Boyutunda Optimal S-kutularının Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği İnceleme Sonuçları

Tez çalışmasında incelenen 3-bit optimal S-kutuları içerisinde, DLCTU sadece 4 değerini almaktadır. 3-bit optimal S-kutularının 2 sabit nokta içeren, BIBO örüntü alt gruplarına göre DLCTU değerinin incelenmesi Çizelge 3.7'de sunulmuştur.

Çizelge 3.7'ye göre; optimal özellikli, 3-bit giriş-çıkış değerlerine sahip, doğrusal ve diferansiyel dal sayısı 2, sabit nokta sayısı 2 olan S-kutularının DLCTU değerinin 4 olduğu ifade edilmektedir. Çizelge 3.7'nin ilk veri satırı takip edildiği şekilde özetlenebilir: 3 × 3 boyutlu, optimal, sabit nokta sayısı 2 olan S-kutuları içerisinde 32 tanesinin BIBO örüntüsü 6 ve hepsinin DLCTU değeri 4 olarak tespit edilmiştir.

Çizelge 3.7. 3 × 3 Boyutunda 2 Sabit Noktalı Optimal S-kutularının BIBO Örüntü Gruplarına Göre DLCTU Değeri İnceleme Sonuçları

	#{DLCTU = 4} S-Kutusu	**#{BIBO Örüntü} S-kutusu**
BIBO Örüntü = 6	32	32
BIBO Örüntü = 8	48	48
BIBO Örüntü = 11	96	96
BIBO Örüntü = 14	48	48

3.7 3 × 3 Boyutunda 10 Kriptografik Özelliğe Göre En İyi Değerlere Sahip S-kutusu Örneği İncelemesi

Tez kapsamında incelenen 3 × 3 boyutunda involutif S-kutularının içerisinde; sabit nokta sayısı, doğrusal dal sayısı, diferansiyel dal sayısı, BCTU değeri, DLCTU değeri, diferansiyel tekdüzelik frekansı ve doğrusallık frekansı açısından her kriptografik özellik için tek değere sahip S-kutuları tespit edilmiştir. Bu S-kutularının tek değişen kriptografik özelliği, BIBO örüntüsü olmaktadır. Tez kapsamında, 3×3 boyutunda S-kutularında BIBO örüntüsünün mümkün olan en düşük değerinin seçilmesi hedeflenmiştir (Lu vd., 2022). Bu sebeple, kriptografik özelliklere göre en iyi değerlere (BIBO örüntüsü 6) sahip olan, 32 tane S-kutusu içerisinden seçilen S-kutusu örneği, Çizelge 3.8'de verilmiştir. Çizelge 3.8'de verilen S-kutusunun kriptografik özellikleri aşağıdaki gibi özetlenebilir:

- Fark Dağılım Tablosu en büyük değeri **2**
- Doğrusal Yaklaşım Tablosu mutlak en büyük değeri **2**
- Cebirsel derece **2**
- Doğrusal dal sayısı **2**
- Diferansiyel dal sayısı **2**
- BIBO Örüntüsü **6**
- Diferansiyel tekdüzelik frekansı **28**
- Doğrusallık frekansı **28**
- BCTU Değeri **2**
- DLCTU Değeri **4**

Çizelge 3.8. 3 × 3 Optimal S-Kutusu Örneği

×	0	1	2	3	4	5	6	7
S(×)	7	4	2	3	1	6	5	0

3.8 3 × 3 Boyutunda 10 Kriptografik Özelliğe Göre En İyi S-Kutularının Bitslice Kapı Karmaşıklığı İnceleme Sonuçları

3 × 3 boyutundaki S-kutularında; optimal ve BIBO örüntüsü 6 olanlar kriptografik özelliklere göre en iyi 32 adet S-kutusu olarak saptanmıştır. Bu 32 adet S-kutusu, bitslice kapı karmaşıklığı açısından incelenip sonuçları Çizelge 3.9'da özetlenmiştir.

Çizelge 3.9. 3 × 3 Boyutunda 10 Kriptografik Özelliğe Göre En İyi S-Kutularının Bitslice Kapı Karmaşıklığı Sonuçları

Bitslice Kapı Karmaşıklığı	Toplam S-Kutusu Sayısı
9	8
10	6
11	12
12	6

Çizelge 3.9 takip edildiği şekilde özetlenebilir: Tez çalışmasında incelenen, 3 × 3 boyutunda kriptografik özelliklere göre mümkün olan en iyi değerlere sahip olan 32 adet S-kutusunun; 8 tanesinin bitslice kapı karmaşıklığı 9, 6 tanesinin 10, 12 tanesinin 11, 6 tanesinin 12 olduğu tespit edilmiştir.

Çizelge 3.10. 3 × 3 Boyutunda 10 Kriptografik Özelliğe Göre En İyi ve Bitslice Kapı Karmaşıklığı En Az Olan S-Kutuları

×	0	1	2	3	4	5	6	7
S_1(×)	0	3	6	1	5	4	2	7
S_2(×)	0	5	3	2	6	1	4	7
S_3(×)	0	7	5	6	4	2	3	1
S_4(×)	0	1	5	6	7	2	3	4
S_5(×)	0	6	2	5	7	3	1	4
S_6(×)	0	1	7	4	3	6	5	2
S_7(×)	0	7	2	4	3	6	5	1
S_8(×)	0	6	7	5	4	3	1	2

Çizelge 3.9'da gösterilen sonuçlar içerisinde bulunan, hem mümkün olan en iyi kriptografik özelliklere sahip hem de bitslice kapı karmaşıklığı en düşük olan 3 × 3 boyutunda 8 adet S-kutusu, Çizelge 3.10'da sunulmuştur. Bu özelliklere göre değerlendirildiğinde, tercih edilebilirliği en yüksek olan S-kutuları olmaktadırlar.

3.9 3 × 3 Boyutunda Literatürde Bulunan 4 Tane S-Kutusunun 10 Kriptografik Özelliğinin İncelenme Sonuçları

Literatürde mevcut olan 3 × 3 boyutunda S-kutularının içinde involutif olan bulunmadığı için, Çizelge 3.11'de involutif olmayan 4 tane 3 × 3 boyutunda S-kutusu, tez kapsamında incelenen kriptografik özelliklere göre incelenmiştir (Peigen, 2023). İncelemenin karşılaştırmalı sonuçları Çizelge 3.11'de sunulmuştur (Bao vd., 2019). Çizelge 3.11'de verilen S-kutularının, incelenen kriptografik özelliklere göre tek değişen değerleri BIBO örüntüsü olarak tespit edilmiştir (Tez kapsamında sabit nokta sayısı incelenmiş ancak kriptografik özelliklere dahil edilmemiştir.). Çizelge 3.11'de incelenen "PRINTcipher" S-kutusu, tez çalışmasında incelenen 10 kriptografik özelliğe göre en iyi değerlere sahip olan 32 adet 3 × 3 boyutunda S-kutusu ile aynı kriptografik özelliklere (involutif olmaması durumu hariç) sahiptir.

Çizelge 3.11. 3 × 3 Boyutunda Literatürde Bulunan İnvolutif Olmayan 4 S-Kutusunun Kriptografik Özellikleri

S-Kutusu	DDT	LAT	AD	FP	BIBO Örüntü	LBN	DBN	$\#\mathcal{U}$	$\#\mathcal{L}$	BCTU	DLCTU
PRINTcipher	2	2	2	2	6	2	2	28	28	2	4
SEA	2	2	2	2	8	2	2	28	28	2	4
ctc2	2	2	2	1	10	2	2	28	28	2	4
3-way	2	2	2	0	6	2	2	28	28	2	4

Tez çalışmasında sunulan 3 × 3 boyundaki S-kutuları, hem involutif özelliği sağlaması hem de iyi kriptografik özelliklere sahip olmalarından dolayı literatüre yeni 3 × 3 boyutundaki involutif S-kutuları olarak katkıda bulunulmuştur.

BÖLÜM 4

4 × 4 BOYUTUNDA İNVOLUTİF S-KUTULARININ KRİPTOGRAFİK ÖZELLİKLERİNİN İNCELEME SONUÇLARI

Tezin bu bölümünde, 4×4 boyutunda tüm involutif S-kutuları incelenmiş, kriptografik özelliklere göre karşılaştırılmalı sonuçları özetlenmiştir. Kriptografik özelliklerine göre mümkün olan en iyi değerlere sahip olan 4×4 boyutundaki involutif S-kutularının, bitslice kapı karmaşıklıkları analiz edilmiştir. Tez çalışmasında incelenen kriptografik özelliklere göre, literatürde bulunan involutif 4×4 boyutundaki S-kutuları karşılaştırılmıştır.

Bölüm 2'de verilen, Şekil 2.2'deki hesaplamaya göre; 4×4 boyutunda bijektif permütasyonlarının toplam sayısı $(2^4)! = 20,922,789,888,000$'nin içerisinden, $i(16) = 46,206,736$ tanesi involutif, bijektif permütasyon olmaktadır. Bu da 4-bit giriş ve çıkış değerlerine sahip olan tüm S-kutusu permütasyonları içerisinden $\%0,0002$ oranına karşılık gelmektedir.

4×4 boyutunda bijektif yapıdaki bütün S-kutusu permütasyonu sayısı $16!$ olmaktadır. Bu uzay çok geniş olduğu için, tez çalışmasında involutif yapıda olan 4-bit S-kutularına odaklanılarak uzay daraltılmıştır.

Çizelge 4.1. 4×4 Boyutunda İnvolutif S-Kutularının En Büyük Fark Dağılım Tablosu ve En Büyük Mutlak Doğrusal Yaklaşım Tablosu Değerleri Karşılaştırılması

S-Kutusu $m \times m$	**İnvolutif Permütasyonlar**	**İnvolutif Olma Özelliğine Sahip Permütasyonlar**		
		DDT-2 & LAT-2	**DDT-4 & LAT-4**	**DDT $\geqslant$ 6 veya LAT $\geqslant$ 6**
4×4	$i(16) = 46,206,736$	0	2,795,520	43,411,216

Çizelge 4.1'e göre, S-kutusunun diferansiyel, doğrusal saldırılara dayanıklı olması için en büyük Fark Dağılım Tablosu değerinin 4 ve en büyük mutlak Doğrusal Yaklaşım Tablosu değerinin 4 olduğu; 2,795,520 adet 4×4 boyutunda S-kutusuna odaklanılmıştır.

Çizelge 4.2. Fark Dağılım Tablosu, Doğrusal Yaklaşım Tablosu, Cebirsel Derece Açısından 4 × 4 Boyutunda S-Kutularının İncelenmesi

	AD = 2	**AD = 3**
DDT-2 & LAT-2	0	0
DDT-4 & LAT-4	374,784	2,420,736

Gösterilen Çizelge 4.1'de özellikleri verilen; en büyük Fark Dağılım Tablosu 4 ve en büyük mutlak Doğrusal Yaklaşım Tablosu değeri 4'e odaklanılan 2,795,520 adet S-kutusunun; Çizelge 4.2'den elde edilen sonuçlara göre 374,784 adet S-kutusunun cebirsel derecesi 3'ten küçük olduğu için, tez çalışmasındaki inceleme kapsamına alınmamıştır. Çizelge 4.2'de sunulanlara göre, tez çalışmasında; en büyük Fark Dağılım Tablosu, en büyük mutlak Doğrusal Yaklaşım Tablosu değerlerince ve cebirsel derece açısından en iyi değerlere sahip olan 4 × 4 boyutunda S-kutuları üzerine incelemeler yapılmıştır.

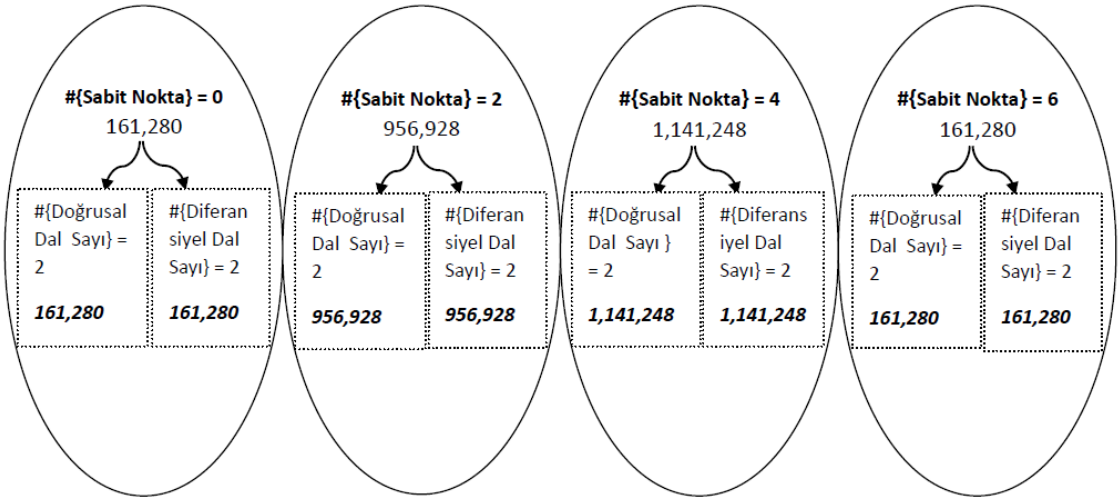
Tez çalışması kapsamında, 4 × 4 boyutundaki involutif S-kutularının **"Optimal"** olarak tanımlanmasını sağlayan kriptografik özellikleri, takip edildiği şekilde özetlenebilir:

- En büyük Fark Dağılım Tablosu ((0, 0) konumu hariç) değeri **4**
- En büyük mutlak Doğrusal Yaklaşım Tablosu ((0, 0) konumu hariç) değeri **4**
- Cebirsel derece **3**

4.1 4 × 4 Boyutunda Optimal S-kutularının Sabit Nokta ve Doğrusal/Diferansiyel Dal Sayıları İnceleme Sonuçları

Tez kapsamında, 4 × 4 boyutunda **"Optimal"** olarak tanımlanan S-kutularının, *Sabit Nokta Sayısı* ve *Doğrusal/Diferansiyel Dal Sayıları* açısından incelenmesi Şekil 4.1'de özetlenmiştir.

Şekil 4.1'de belirtilen sonuçlara göre; 4-bit giriş ve çıkış değerlerine sahip, optimal S-kutularının içerisinde; sabit nokta sayısı sadece 0, 2, 4 ve 6 olan S-kutuları tespit edilmiştir. Tez çalışmasında tanımlan 4 × 4 boyutunda, optimal S-kutularının içerisinde; sabit nokta sayısı 0 olan S-kutusu sayısı toplamı 161,280 tane, sabit nokta sayısı 2 olan S-kutusu sayısı toplamı 956,928 tane, sabit nokta sayısı 4 olan S-kutusu sayısı toplamı 1,141,248 tane ve sabit nokta sayısı 6 olan S-kutusu sayılarının toplamı 161,280 tane olarak saptanmıştır. 4 × 4 boyutunda optimal S-kutuları, sabit nokta sayısınca 4 gruba ayrıldığında, her gruptaki bütün S-kutularının doğrusal dal sayısı 2 ve diferansiyel dal saysı 2 olarak tespit edilmiştir. Diğer bir deyişle, tez çalışmasında incelenen, 4 × 4 boyutunda



Şekil 4.1. 4 × 4 Boyutunda Optimal S-Kutuları Sabit Nokta ve Dal Sayılarının İncelenmesi

optimal tüm S-kutularının doğrusal ve diferansiyel dal sayıları aynı ve 2 değerine eşit olmaktadır.

4.2 4 × 4 Boyutunda Optimal S-kutularının BIBO Örüntüsü İnceleme Sonuçları

4-bit giriş ve 4-bit çıkış olan S-kutuları içerisinde; involutif, en büyük Fark Dağılım Tablosu değeri 4, en büyük mutlak Doğrusal Yaklaşım Tablosu değeri 4, cebirsel derece 3, sabit nokta sayısı 0, doğrusal ve diferansiyel dal sayısı 2 olan S-kutularının (161,280 tane S-kutusu) BIBO örüntüleri Çizelge 4.3'te özetlenmiştir.

Çizelge 4.3. 4 × 4 Boyutunda Optimal ve 0 Sabit Noktalı S-kutularının BIBO Örüntü İnceleme Sonuçları

BIBO Örüntü	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**
#{S-kutusu}	384	1,536	2,688	4,608	4,608	13,824	13,440	17,472	19,200	14,976
BIBO Örüntü	**19**	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	
#{S-Kutusu}	17,664	21,120	9,216	9,600	5,760	3,648	384	768	384	

Çizelge 4.3'te ifade edilenlere göre; tez kapsamında incelenen 4-bit giriş ve çıkış değerlerine sahip, involutif, optimal, sabit nokta barındırmayan S-kutularının BIBO örüntülerinin, $9-27$ aralığında olduğu tespit edilmiştir.

Tez çalışmasında belirtilen optimal, 4 × 4 boyutunda S-kutularının içerisinde, 2 tane sabit nokta barındıran, doğrusal ve diferansiyel dal sayısı 2'ye eşit olan S-kutularının (956,928 tane S-kutusu) BIBO örüntüleri Çizelge 4.4'te özetlenmiştir.

Çizelge 4.4'e göre; 2 tane sabit nokta barındıran optimal, 4 × 4 boyutunda S-kutularının, BIBO örüntülerinin $8-30$ aralığında olduğu saptanmıştır. Sabit nokta

Çizelge 4.4. 4 × 4 Boyutunda Optimal ve 2 Sabit Noktalı S-kutularının BIBO Örüntü İnceleme Sonuçları

BIBO Örüntü	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
#{S-kutusu}	1,152	768	4,992	8,064	23,040	26,112	46,080	62,208	79,872	100,608	107,328	106,752
BIBO Örüntü	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	**30**	
#{S-Kutusu}	109,440	83,328	81,024	46,080	35,712	19,584	10,560	1,920	1,152	768	384	

barındırmayan optimal 4 × 4 boyutundaki S-kutularının, BIBO örüntülerinin sunulduğu Çizelge 4.3 ile karşılaştırıldığında, daha küçük olan 8 değerini barındıran 1,152 tane S-kutusu mevcuttur.

Tez çalışmasında belirtilen, optimal 4 × 4 boyutunda S-kutularının içerisinde, 4 tane sabit noktalı, doğrusal ve diferansiyel dal sayısı 2 olan S-kutularının (1,141,248 tane S-kutusu) BIBO örüntüleri Çizelge 4.5'te özetlenmiştir.

Çizelge 4.5. 4 × 4 Boyutunda Optimal ve 4 Sabit Noktalı S-kutularının BIBO Örüntü İnceleme Sonuçları

BIBO Örüntü	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**	**17**	**18**	**19**
#{S-kutusu}	1,152	5,376	9,216	13,440	22,656	41,088	54,912	88,896	96,000	124,416	140,160
BIBO Örüntü	**20**	**21**	**22**	**23**	**24**	**25**	**26**	**27**	**28**	**29**	
#{S-Kutusu}	125,568	125,952	87,552	86,400	48,960	37,248	16,512	11,904	2,688	1,152	

Çizelge 4.5'e göre; 4 tane sabit nokta barındıran optimal, 4 × 4 boyutunda S-kutularının, BIBO örüntülerinin $9-29$ aralığında olduğu tespit edilmiştir.

Tez çalışmasında belirtilen optimal, 4 × 4 boyutunda S-kutularının içerisinde, 6 tane sabit noktalı, doğrusal ve diferansiyel dal sayısı 2 olan S-kutularının (161,280 tane S-kutusu) BIBO örüntüleri Çizelge 4.6'da özetlenmiştir.

Çizelge 4.6. 4 × 4 Boyutunda Optimal ve 6 Sabit Noktalı S-kutularının BIBO Örüntüsü İnceleme Sonuçları

BIBO Örüntü	**13**	**14**	**15**	**16**	**17**	**18**	**19**	**20**
#{S-kutusu}	1,152	7,680	5,760	8,448	13,440	17,472	19,584	25,728
BIBO Örüntü	**21**	**22**	**23**	**24**	**25**	**26**	**27**	
#{S-Kutusu}	18,816	9,600	14,592	5,760	7,296	2,112	3,840	

Çizelge 4.6'ya göre; 6 tane sabit nokta barındıran optimal, 4 × 4 boyutunda S-kutularının, BIBO örüntülerinin $13-27$ aralığında olduğu tespit edilmiştir.

Bao vd. (2019) çalışmasına göre; BIBO Örüntüsü için 4 × 4 boyutunda, bijektif S-kutuları permütasyon uzayı içerisinde, doğrusal dal sayısının 2'den büyük olduğu durumlarda BIBO Örüntüsünün optimal değeri (BIBO Örüntü <= 4) olmadığı belirtilmektedir. Tez çalışmasında "Optimal" özelliklere sahip olan involutif 4 × 4 boyutunda S-kutularının doğrusal ve diferansiyel dal sayısı 2'ye eşit olması sebebiyle, optimal BIBO Örüntüsü değerine ulaşılamaması paralellik göstermektedir.

4.3 4 × 4 Boyutunda Optimal S-kutularının Boomerang Bağlantı Tablosu Tekdüzeliği İnceleme Sonuçları

Tez çalışmasında incelenen 4-bit giriş ve çıkış değerlerine sahip olan optimal, involutif S-kutuları içerisinde, BCTU 6, 8, 10 ve 16 değerleri tespit edilmiştir. S-kutusunun, Boomerang ataklara karşı dayanıklılığını saptamak için BCT tekdüzelik değerinin incelenmesi gerektiği savunulmaktadır (Bao vd., 2019). Bir S-kutusunun Boomerang ataklara karşı dayanıklılığı için BCT tekdüzelik değerinin küçük olması tercih edilmektedir (Cid vd., 2018). Bu sebeple tez çalışmasında, BCT tekdüzelik değerleri incelenerek küçük değerlere sahip S-kutularının seçilmesi sağlanmıştır.

4 × 4 boyutunda, optimal, involutif S-kutularının sabit nokta içermeyenlerinin, BIBO örüntü alt gruplarına göre BCTU değerlerinin incelenmesi Çizelge 4.7'de sunulmuştur.

Çizelge 4.7. 4 × 4 Boyutunda Optimal 0 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri İnceleme Sonuçları

	#{BCTU = 10} S-Kutusu	**#{BIBO Örüntü} S-kutusu**
BIBO Örüntü = 9	384	384
BIBO Örüntü = 10	1,536	1,536
BIBO Örüntü = 11	2,688	2,688
BIBO Örüntü = 12	4,608	4,608
BIBO Örüntü = 13	4,608	4,608
BIBO Örüntü = 14	13,824	13,824
BIBO Örüntü = 15	13,440	13,440
BIBO Örüntü = 16	17,472	17,472
BIBO Örüntü = 17	19,200	19,200
BIBO Örüntü = 18	14,976	14,976
BIBO Örüntü = 19	17,664	17,664
BIBO Örüntü = 20	21,120	21,120
BIBO Örüntü = 21	9,216	9,216
BIBO Örüntü = 22	9,600	9,600
BIBO Örüntü = 23	5,760	5,760
BIBO Örüntü = 24	3,684	3,684
BIBO Örüntü = 25	384	384
BIBO Örüntü = 26	768	768
BIBO Örüntü = 27	384	384

Çizelge 4.7'ye göre; optimal özellikli, 4-bit giriş-çıkış değerlerine sahip, doğrusal ve diferansiyel dal sayısı 2 olan, sabit nokta içermeyen bütün S-kutularının BCTU değerinin 10 olduğu tespit edilmiştir. Çizelge 4.7'nin ilk veri satırı takip edildiği gibi

özetlenebilir; 4 × 4 boyutlu, optimal, sabit nokta sayısı 0 olan S-kutuları içerisinde 384 tanesinin BIBO örüntüsü 9 ve hepsinin BCTU değeri 10 olmaktadır.

4-bit giriş-çıkış değerlerine sahip, optimal, 2 sabit noktalı S-kutularının BIBO örüntü alt gruplarına göre BCTU değerlerinin incelenmesi Çizelge 4.8'de sunulmuştur.

Çizelge 4.8. 4 × 4 Boyutunda Optimal 2 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri İnceleme Sonuçları

	#{BCTU = 6}	**#{BCTU = 8}**	**#{BCTU = 10}**	**#{BIBO Örüntü} S-kutusu**
BIBO Örüntü = 8	384	768	0	1,152
BIBO Örüntü = 9	384	384	0	768
BIBO Örüntü = 10	384	384	4,224	4,992
BIBO Örüntü = 11	1,152	768	6,144	8,064
BIBO Örüntü = 12	2,304	2,304	18,432	23,040
BIBO Örüntü = 13	3,840	2,688	19,584	26,112
BIBO Örüntü = 14	3,456	4,992	37,632	46,080
BIBO Örüntü = 15	6,144	6,912	49,152	62,208
BIBO Örüntü = 16	5,760	4,922	69,120	79,802
BIBO Örüntü = 17	8,832	10,368	81,408	100,608
BIBO Örüntü = 18	10,752	7,488	89,088	107,328
BIBO Örüntü = 19	9,600	9,216	87,936	106,752
BIBO Örüntü = 20	6,144	8,064	95,232	109,440
BIBO Örüntü = 21	6,144	5,376	71,808	83,328
BIBO Örüntü = 22	7,296	8,064	65,664	81,024
BIBO Örüntü = 23	4,608	4,992	36,480	46,080
BIBO Örüntü = 24	1,920	1,152	32,640	35,712
BIBO Örüntü = 25	1,536	1,152	16,896	19,584
BIBO Örüntü = 26	0	192	10,368	10,560
BIBO Örüntü = 27	0	384	1,536	1,920
BIBO Örüntü = 28	0	0	1,152	1,152
BIBO Örüntü = 29	0	0	768	768
BIBO Örüntü = 30	0	0	384	384

Çizelge 4.8'e göre; optimal özellikli, 4-bit giriş-çıkış değerlerine sahip, doğrusal ve diferansiyel dal sayısı 2, sabit nokta sayı 2 olan S-kutularının BCTU değerleri değişkenlik göstermektedir. Çizelge 4.8'e göre BCTU açısından; 6, 8 ve 10 değerleri tespit edilmiştir. Çizelge 4.8'in BIBO örüntüsü 13 olan satırı takip edilen şekilde özetlenebilir: 4 × 4 boyutlu, involutif, optimal, doğrusal ve diferansiyel dal sayısı 2, 2 sabit nokta içeren, BIBO örüntüsü 13 olan 26,112 adet S-kutusundan; 3,840 tanesinin BCTU değeri 6 olmakta, 2,688 tanesinin BCTU değeri 8 ve 19,584 tanesini BCTU değeri 10 olarak saptanmıştır.

4 × 4 boyutunda, involutif S-kutularının 4 sabit noktalı, BIBO örüntü alt gruplarına göre BCTU değerlerinin incelenmesi, Çizelge 4.9'da ifade edilmiştir.

Çizelge 4.9'a göre; optimal özellikli, 4-bit giriş-çıkış değerlerine sahip, doğrusal ve diferansiyel dal sayısı 2, sabit nokta sayı 4 olan bütün S-kutularının BCTU değerleri incelenmiştir. BCTU açısından; 6, 10 ve 16 değerleri tespit edilmiştir. Çizelge 4.9'un

Çizelge 4.9. 4 × 4 Boyutunda Optimal 4 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri İnceleme Sonuçları

	#{BCTU = 6}	#{BCTU = 10}	#{BCTU = 16}	#{BIBO Örüntü} S-kutusu
BIBO Örüntü = 9	768	384	0	1,152
BIBO Örüntü = 10	2,688	2,304	384	5,376
BIBO Örüntü = 11	3,456	4,608	1,152	9,216
BIBO Örüntü = 12	2,688	10,368	384	13,440
BIBO Örüntü = 13	5,760	16,512	384	22,656
BIBO Örüntü = 14	8,448	32,256	384	41,088
BIBO Örüntü = 15	9,216	43,008	2,688	54,912
BIBO Örüntü = 16	23,424	58,560	6,912	88,896
BIBO Örüntü = 17	19,200	66,432	10,368	96,000
BIBO Örüntü = 18	28,032	85,248	11,136	124,416
BIBO Örüntü = 19	19,200	103,680	17,280	140,160
BIBO Örüntü = 20	26,880	86,016	12,672	125,568
BIBO Örüntü = 21	22,272	93,696	9,984	125,952
BIBO Örüntü = 22	19,200	56,832	11,520	87,552
BIBO Örüntü = 23	9,216	61,056	16,128	86,400
BIBO Örüntü = 24	6,144	33,216	9,600	48,960
BIBO Örüntü = 25	4,224	27,648	5,376	37,248
BIBO Örüntü = 26	1,536	13,056	1,920	16,512
BIBO Örüntü = 27	1,920	8,832	1,152	11,904
BIBO Örüntü = 28	768	1,536	384	2,688
BIBO Örüntü = 29	0	1,152	0	1,152

BIBO örüntüsü 28 olan satırı, takip edilen şekilde özetlenebilir: 4 × 4 boyutlu, involutif, optimal, doğrusal ve diferansiyel dal sayısı 2, 4 sabit nokta içeren, BIBO örüntüsü 28 olan, 2,688 adet S-kutusundan; 768 tanesinin BCTU değeri 6 olmakta, 1,536 tanesinin BCTU değeri 10 ve 384 tanesini BCTU değeri 16 olmaktadır.

4 × 4 boyutunda, involutif, optimal, 6 sabit noktalı S-kutularının BIBO örüntü alt gruplarına göre BCTU değerlerinin incelenmesi Çizelge 4.10'da sunulmuştur.

Çizelge 4.10'a göre; optimal özellikli, 4 × 4 boyutlu, doğrusal ve diferansiyel dal sayısı 2 olan, 6 sabit noktalı bütün S-kutularının BCTU değerinin 6 ve 8 arasında değişkenlik gösterdiği tespit edilmiştir. Çizelge 4.10'un BIBO örüntüsü 20 için verilen satırı takip edilen şekilde özetlenebilir: 4 × 4 boyutlu, optimal, sabit nokta sayısı 6 olan S-kutuları içerisinde 25,728 tanesinin BIBO örüntüsü 20 ve bu S-kutularının; 2,304 tanesinin BCTU değeri 6 olmakta, 23,424 tanesinin BCTU değeri 8 olmaktadır.

4.4 4 × 4 Boyutunda Optimal S-kutularının Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği İnceleme Sonuçları

S-kutularının tez çalışmasında incelenen kriptografik özelliklerinden olan DLCTU değerinin, S-kutusunda optimal doğrusal olmama (non-linearity) için *düşük* olması

Çizelge 4.10. 4 × 4 Boyutunda Optimal 6 Sabit Noktalı S-kutularının BIBO Örüntü Gruplarına Göre BCTU Değeri İnceleme Sonuçları

	#{BCTU = 6} S-Kutusu	#{BCTU = 8} S-Kutusu	#{BIBO Örüntü} S-kutusu
BIBO Örüntü = 13	0	1,152	1,152
BIBO Örüntü = 14	1,152	6,528	7,680
BIBO Örüntü = 15	1,152	4,608	5,760
BIBO Örüntü = 16	0	8,448	8,448
BIBO Örüntü = 17	384	13,056	13,440
BIBO Örüntü = 18	2,304	15,168	17,472
BIBO Örüntü = 19	2,304	17,280	19,584
BIBO Örüntü = 20	2,304	23,424	25,728
BIBO Örüntü = 21	2,304	16,512	18,816
BIBO Örüntü = 22	1,536	8,064	9,600
BIBO Örüntü = 23	768	13,824	14,592
BIBO Örüntü = 24	384	5,376	5,760
BIBO Örüntü = 25	1,152	6,144	7,296
BIBO Örüntü = 26	0	2,112	2,112
BIBO Örüntü = 27	384	3,456	3,840

gerektiği belirtilmiştir (Bar-On vd., 2019). Ancak en düşük DLCTU değeri ifade edilmemiştir (Tang vd., 2021). 4×4 boyutunda tüm optimal S-kutuları içerisinde, DLCTU değeri sadece **8** tespit edilmiştir.

DLCTU değerinin şifreleme *anahtarının tahmin edilebilmesi* hakkında analiz yapılmasına yardımcı olduğu savunulmuştur (Muthavhine & Sumbwanyambe, 2022). Bir S-kutusu $m \times m$ boyutunda olduğunda, $\mathbf{DLCTU\ /\ 2^m}$ olasılığı ile şifreleme anahtar tahminlemesi yapılabilmektedir. Bu sebeple; $m \times m$ boyutundaki S-kutusunun DLCTU değerinin düşük olması, gizli olan şifreleme anahtarının tahmin edilme olasılığını düşürmektedir. Diğer bir deyişle, şifreleme anahtarının tahmin edilme olasılığını düşürmek için, DLCTU değerini mümkün olan en küçük değer olarak seçmek gerekmektedir.

4.5 4 × 4 Boyutunda Optimal S-kutularının DLCTU ve Diferansiyel Tekdüzelik/-Doğrusallık Frekans İnceleme Sonuçları

Tez çalışmasında incelenen; 4×4 boyutlu, optimal, sabit noktası bulunmayan tüm S-kutularının DLCTU değeri 8 ve diferansiyel tekdüzelik/doğrusallık frekansları $15/30$ olarak tespit edilmiştir.

4-bit giriş-çıkış değerlerine sahip involutif, 2 sabit noktalı S-kutularının BIBO örüntü alt gruplarında DLCTU değerine göre diferansiyel tekdüzelik/doğrusallık frekanslarının incelenmesi Çizelge 4.11'de ifade edilmiştir.

Tez çalışmasında incelenen; 4×4 boyutunda, involutif, optimal tüm S-kutularının DLCTU değeri 8 olarak tespit edilmiştir. Bu özelliklere sahip ve 2 sabit noktası bulunan

Çizelge 4.11. 4 × 4 Boyutunda Optimal 2 Sabit Noktalı S-kutularının DLCTU değerinin 8 Olduğu BIBO Örüntü Gruplarına Göre Diferansiyel Tekdüzelik/Doğrusallık Frekanslarının İnceleme Sonuçları

	#{DLCTU = 8 & #U =15 & #L =30 }	#{DLCTU = 8 & #U =18 & #L =32 }	#{BIBO & DLCTU = 8}S-kutusu
BIBO Örüntü = 8	1,152	0	1,152
BIBO Örüntü = 9	768	0	768
BIBO Örüntü = 10	1,152	3,840	4,992
BIBO Örüntü = 11	5,376	2,688	8,064
BIBO Örüntü = 12	9,216	13,824	23,040
BIBO Örüntü = 13	16,896	9,216	26,112
BIBO Örüntü = 14	21,120	24,960	46,080
BIBO Örüntü = 15	31,872	30,336	62,208
BIBO Örüntü = 16	34,560	45,312	79,872
BIBO Örüntü = 17	55,680	44,928	100,608
BIBO Örüntü = 18	48576	58752	107,328
BIBO Örüntü = 19	55,680	51,072	106,752
BIBO Örüntü = 20	53,760	55,680	109,440
BIBO Örüntü = 21	41,472	41,856	83,328
BIBO Örüntü = 22	45,312	35,712	81,024
BIBO Örüntü = 23	25,728	20,352	46,080
BIBO Örüntü = 24	15,744	19,968	35,712
BIBO Örüntü = 25	11,904	7,680	19,584
BIBO Örüntü = 26	4,800	5,760	10,560
BIBO Örüntü = 27	1,152	768	1,920
BIBO Örüntü = 28	768	384	1,152
BIBO Örüntü = 29	768	0	768
BIBO Örüntü = 30	384	0	384

S-kutuları, BIBO örüntülerine göre alt gruplara ayrıldıklarında; DLCTU 8 değerine sahip S-kutuları BIBO örüntülerinin $10-28$ aralığında olduğu belirlenen, diferansiyel tekdüzelik/doğrusallık frekansları $15/30$ ve $18/32$ değerlerine sahip S-kutuları tespit edilmiştir. Bu S-kutuları, Çizelge 4.11'de sunulmuştur. Çizelge 4.11'e göre; BIBO örüntüsü 14 ve DLCTU değeri 8 olan S-kutularının sonuçlarına yönelik özet takip edilen şekilde verilebilir: 4-bit giriş-çıkış değerlerine sahip, optimal, sabit nokta sayısı 2, DLCTU değeri 8, BIBO örüntüsü 14 olan 46,080 tane S-kutusunun; 21,120 tanesinin diferansiyel tekdüzelik/doğrusallık frekansı $15/30$ olmakta, 24,960 tanesinin diferansiyel tekdüzelik/doğrusallık frekansı $18/32$ olmaktadır.

4-bit giriş-çıkış değerlerine sahip, involutif S-kutularının 4 sabit noktalı, BIBO örüntü alt gruplarına göre DLCTU değerinin diferansiyel tekdüzelik/doğrusallık frekanslarının incelenmesi Çizelge 4.12'de ifade edilmiştir.

Boyutu 4×4, involutif, optimal, sabit nokta sayısı 4 olan S-kutularının hiçbirinin, diferansiyel tekdüzelik/doğrusallık frekansları $18/32$ olmamaktadır. Çizelge 4.12'de BIBO örüntülerine göre, DLCTU değeri ve frekans incelemeleri sunulmuştur. BIBO örüntüsü $9-29$ aralığında olduğu belirlenen S-kutularının DLCTU 8 olanlarının, diferansiyel tekdüzelik/doğrusallık frekanslarının $15/30$ ve $24/36$ arasında değişkenlik gösterdiği tespit edilmiştir. Çizelge 4.12'nin BIBO örüntüsü 25 ve DLCTU 8 olan S-kutularının sonuçlarına yönelik özet takip edilen şekilde verilebilir; 4-bit giriş-çıkış değerlerine sahip, optimal, sabit nokta sayısı 4, DLCTU değeri 8, BIBO örüntüsü 25 olan

Çizelge 4.12. 4 × 4 Boyutunda Optimal 4 Sabit Noktalı S-kutularının DLCTU Değerinin 8 Olduğu BIBO Örüntü Gruplarına Göre Diferansiyel Tekdüzelik/Doğrusallık Frekanslarının İnceleme Sonuçları

	#{DLCTU = 8 & #U =15 & #L =30 }	#{DLCTU = 8 & #U =24 & #L =36 }	#{BIBO & DLCTU = 8}S-kutusu
BIBO Örüntü = 9	1,152	0	1,152
BIBO Örüntü = 10	4,992	384	5,376
BIBO Örüntü = 11	8,064	1,152	9,216
BIBO Örüntü = 12	13,056	384	13,440
BIBO Örüntü = 13	22,272	384	22,656
BIBO Örüntü = 14	40,704	384	41,088
BIBO Örüntü = 15	52,224	2,688	54,912
BIBO Örüntü = 16	81,984	6,912	88,896
BIBO Örüntü = 17	85,632	10,368	96,000
BIBO Örüntü = 18	113,280	11,136	124,416
BIBO Örüntü = 19	122,880	17,280	140,160
BIBO Örüntü = 20	112,896	12,672	125,568
BIBO Örüntü = 21	115,968	9,984	125,952
BIBO Örüntü = 22	76,032	11,520	87,552
BIBO Örüntü = 23	70,272	16,128	86,400
BIBO Örüntü = 24	39,360	9,600	48,960
BIBO Örüntü = 25	31,872	5,376	37,248
BIBO Örüntü = 26	14,592	1,920	16,512
BIBO Örüntü = 27	10,752	1,152	11,904
BIBO Örüntü = 28	2,304	384	2,688
BIBO Örüntü = 29	1,152	0	1,152

37,248 tane S-kutusundan; 31,872 tanesinin diferansiyel tekdüzelik/doğrusallık frekansı $15/30$ olmakta, 5,376 tanesinin diferansiyel tekdüzelik/doğrusallık frekansının $18/32$ olduğu saptanmıştır.

Tez çalışmasında incelenen; 4×4 boyutlu, optimal, sabit noktası 6 olan tüm S-kutularının DLCTU değeri 8 ve diferansiyel tekdüzelik/doğrusallık frekansları $15/30$ olarak tespit edilmiştir.

4.6 4 × 4 Boyutunda Optimal S-kutularının BCTU Değeri ve Diferansiyel Tekdüzelik/Doğrusallık Frekans İnceleme Sonuçları

Tez çalışmasında incelenen 4-bit giriş-çıkış değerlerine sahip, involutif, optimal, sabit noktası bulunmayan bütün S-kutularının; BCTU değeri 10 ve bu S-kutularının diferansiyel tekdüzelik frekansının 15, doğrusallık frekansının 30 olduğu tespit edilmiştir.

4×4 boyutunda, optimal, 2 sabit noktası bulunan S-kutularının diferansiyel tekdüzelik/doğrusallık frekansları $15/30$ ve $18/32$ değer ikililerinden oluşmaktadır.

4-bit giriş-çıkış değerlerine sahip olan optimal, involutif, 2 sabit noktalı S-kutularının, BIBO örüntüleri ve BCTU değerlerine göre diferansiyel tekdüzelik/doğrusallık frekanslarının incelenmesi, Çizelge 4.13'te ifade edilmiştir.

4×4 boyutunda optimal, 2 sabit noktalı S-kutularından, BIBO örüntülerine göre BCTU 6 ve 8 değerlerine sahip S-kutularının diferansiyel tekdüzelik frekansı 15, doğrusallık frekansı 30 olarak tespit edilmiştir. Ancak 4-bit giriş-çıkış değerlerine

Çizelge 4.13. 4 × 4 Boyutunda Optimal 2 Sabit Noktalı BCTU Değerinin 10 Olduğu S-Kutularının BIBO Örüntülerine Göre Diferansiyel Tekdüzelik/Doğrusallık Frekanslarının İnceleme Sonuçları

	#{BCTU = 10 & #U =15 & #L =30 }	#{BCTU = 10 & #U =18 & #L =32 }	#{BIBO & BCTU = 10}S-kutusu
BIBO Örüntü = 8	0	0	0
BIBO Örüntü = 9	0	0	0
BIBO Örüntü = 10	384	3,840	4,224
BIBO Örüntü = 11	3,456	2,688	6,144
BIBO Örüntü = 12	4,608	13,824	18,432
BIBO Örüntü = 13	10,368	9,216	19,584
BIBO Örüntü = 14	12,672	24,960	37,632
BIBO Örüntü = 15	18,816	30,336	49,152
BIBO Örüntü = 16	23,808	45,312	69,120
BIBO Örüntü = 17	36,480	44,928	81,408
BIBO Örüntü = 18	30,336	58,752	89,088
BIBO Örüntü = 19	36,864	51,072	87,936
BIBO Örüntü = 20	39,552	55,680	95,232
BIBO Örüntü = 21	29,952	41,856	71,808
BIBO Örüntü = 22	29,952	35,712	65,664
BIBO Örüntü = 23	16,128	20,352	36,480
BIBO Örüntü = 24	12,672	19,968	32,640
BIBO Örüntü = 25	9,216	7,680	16,896
BIBO Örüntü = 26	4,608	5,760	10,368
BIBO Örüntü = 27	768	768	1,536
BIBO Örüntü = 28	768	384	1,152
BIBO Örüntü = 29	768	0	768
BIBO Örüntü = 30	384	0	384

sahip olan, optimal, sabit nokta sayısı 2 olan S-kutularının BCTU değerinin 10 olması durumunda; diferansiyel tekdüzelik/doğrusalık frekanslarının $15/30$ ve $18/32$ olduğu S-kutuları tespit edilip, Çizelge 4.13'te gösterilmiştir. Çizelge 4.13'te, BIBO örüntüsü 15 ve BCTU değeri 10 değerlerini gösteren satır takip edildiği şekilde özetlenebilir; 4-bit giriş-çıkış değerlerine sahip, involutif, optimal, sabit nokta sayısı 2, BIBO örüntüsü 15 ve BCTU değeri 10 olan 49,152 tane S-kutusundan; 18,816 tanesinin diferansiyel tekdüzelik/doğrusallık frekanslarının $15/30$ olduğu, 30,336 tanesinin diferansiyel tekdüzelik/doğrusallık frekanslarının $18/32$ olduğu saptanmıştır.

Tez kapsamında incelenen 4-bit giriş ve çıkış değerlerine sahip olan, optimal, 4 sabit noktalı tüm S-kutularının, bütün BIBO örüntülerindeki BCTU 6 ve 10 değerlerine sahip S-kutularının diferansiyel tekdüzelik/doğrusallık frekanslarının $15/30$ olduğu, BCTU 16 değerine sahip olan tüm S-kutularının diferansiyel tekdüzelik/doğrusallık frekanslarının $24/36$ olduğu tespit edilmiştir.

4×4 boyutunda optimal, 6 sabit noktalı S-kutularının, tüm BIBO örüntülerinde, BCTU 6 ve 8 değerlerindeki bütün S-kutularının diferansiyel tekdüzelik/doğrusallık frekans değerleri $15/30$ olarak saptanıştır.

4.7 4 × 4 Boyutunda 10 Kriptografik Özelliğe Göre En İyi Değerlere Sahip S-kutusu Örneği İncelemesi

Tez kapsamında incelenen 4 × 4 boyutunda involutif S-kutularının içerisinden; 10 kriptografik özelliğe göre, Bölüm 6'da "KRİTERLER-2" olarak incelenen S-kutuları en iyi değerlere sahip olanlarıdır. Bu sebeple, 4 × 4 boyutunda, involutif, sabit nokta sayısı 2, kriptografik özelliklere göre en iyi değerlere sahip olan 384 tane S-kutusu içerisinden seçilen S-kutusu örneği; Çizelge 4.15'te verilen **S_4(×)** olmaktadır. Bu S-kutusunun kriptografik özellikleri takip edildiği şekilde özetlenebilir:

- Fark Dağılım Tablosu en büyük değeri **4**
- Doğrusal Yaklaşım Tablosu mutlak en büyük değeri **4**
- Cebirsel derece **3**
- Doğrusal dal sayısı **2**
- Diferansiyel dal sayısı **2**
- BIBO Örüntüsü **8**
- Diferansiyel tekdüzelik frekansı **15**
- Doğrusallık frekansı **30**
- BCTU değeri **6**
- DLCTU değeri **8**

4.8 4 × 4 Boyutunda 10 Kriptografik Özelliğe Göre En İyi S-Kutularının Bitslice Kapı Karmaşıklığı İnceleme Sonuçları

Tez çalışması kapsamında, kriptografik özelliklere göre iyi olarak tespit edilen, 4 × 4 boyutunda 384 adet (Bölüm 6 KRİTERLER-2) S-kutusunun, mantıksal kapı maliyetini ortaya koymak amacıyla bitslice kapı karmaşıklığı incelenmiştir. Bu incelemede, S-kutularının vektörel çıkış Boole fonksiyonların cebirsel ifadelerinin optimize edilmesi yapılmadan, bitslice kapı karmaşıklığı tespit edilmiştir (Bao vd., 2019).

Bölüm 6'da "KRİTERLER-2" olarak incelenen S-kutularının; bijektif, involutif, 4 × 4 boyutunda S-kutusu permütasyonları içerisinde, mümkün olan en iyi kriptografik özelliklere sahip olduğu tespit edilmiştir. Bu 384 adet S-kutusu bitslice kapı karmaşıklığı açısından incelenip, sonuçları Çizelge 4.14'te gösterilmiştir.

Çizelge 4.14. 4 × 4 Boyutunda Kriptografik Özelliklere Göre En İyi S-Kutularının Bitslice Kapı Karmaşıklığı Sonuçları

Bitslice Kapı Karmaşıklığı	Toplam S-Kutusu Sayısı
42	48
43	72
44	24
45	48
46	48
47	120
48	24

Belirtilen Çizelge 4.14 takip edildiği şekilde özetlenebilir: Bölüm 6'da "KRİTERLER-2" olarak tez çalışmasında incelenen, 4 × 4 boyutunda 10 kriptografik özelliğe göre mümkün olan en iyi değerlere sahip olan 384 adet S-kutusunun; 48 tanesinin bitslice kapı karmaşıklığı 42, 72 tanesinin 43, 24 tanesinin 44, 48 tanesinin 45, 48 tanesinin 46, 120 tanesinin 47 ve 24 tanesinin 48 olduğu tespit edilmiştir.

Çizelge 4.14'te belirtilen sonuçlar içerisinde; hem incelenen 10 kriptografik özelliğe göre mümkün olan en iyi değerlere sahip hem de bitslice kapı karmaşıklığı en düşük olan 4×4 boyutunda 48 adet S-kutusu Çizelge 4.15 ve Çizelge 4.16'da sunulmuştur (Kolay okunabilirliği sağlamak amacıyla 2 tabloya bölünmüştür.). 10 kriptografik özellik ve bitslice kapı karmaşıklığı değerlendirildiğinde, tercih edilebilirliği en yüksek olan S-kutuları olduğu tespit edilmiştir.

4.9 4 × 4 Boyutunda Literatürde Bulunan 17 İnvolutif S-Kutusunun 10 Kriptografik Özelliğe Göre İncelenme Sonuçları

Literatürde mevcut olan 4 × 4 boyutunda S-kutularının involutif olanları, tez çalışması kapsamındaki kriptografik özelliklere göre incelenmiştir (Peigen, 2023). İncelemelerin karşılaştırmalı sonuçları Çizelge 4.17'de sunulmuştur (Sovyn, Opirskyy & Mykhaylova, 2023).

Çizelge 4.17'de verilen S-kutularının tez kapsamında incelenen kriptografik özelliklere göre değişmeyen değerleri; maksimum Fark Dağılım Tablosu değeri, maksimum mutlak Doğrusal Yaklaşım Tablosu değeri ve DLCTU değeri olarak tespit edilmiştir (Tez kapsamında, S-kutularının sabit nokta sayısı incelenmiş ancak kriptografik özelliklere dahil edilmemiştir.). Çizelge 4.17'de incelenen "Panda" S-kutusu, tez çalışmasında incelenen 10 kriptografik özelliğe göre en iyi değerlere sahip olan, 384 adet 4 × 4 boyutunda involutif S-kutusu ile benzer (Sadece BIBO örüntü değeri farklılaşmaktadır.) kriptografik özelliklere sahiptir. Tez çalışmasında sunulan 4 × 4

Çizelge 4.15. 4 × 4 Boyutunda 10 Kriptografik Özelliğe Göre En İyi ve Bitslice Kapı Karmaşıklığı En Az Olan S-Kutuları (İlk 20)

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
S_1(×)	0	C	9	6	4	B	3	D	F	2	E	5	1	7	A	8
S_2(×)	1	0	F	8	A	6	5	B	3	E	4	7	C	D	9	2
S_3(×)	2	F	0	4	3	8	D	B	5	A	9	7	C	6	E	1
S_4(×)	0	A	F	7	4	9	8	3	6	5	1	C	B	E	D	2
S_5(×)	0	6	F	B	A	9	1	C	8	5	4	3	7	E	D	2
S_6(×)	2	A	0	D	9	5	C	7	F	4	1	E	6	3	B	8
S_7(×)	8	6	C	3	F	9	1	A	0	5	7	B	2	E	D	4
S_8(×)	8	F	5	A	9	2	6	C	0	4	3	D	7	B	E	1
S_9(×)	1	0	9	E	A	C	6	7	F	2	4	D	5	B	3	8
S_10(×)	0	1	C	6	9	E	3	D	F	4	B	A	2	7	5	8
S_11(×)	8	A	F	4	3	5	C	9	0	7	1	E	6	D	B	2
S_12(×)	0	6	C	9	F	D	1	A	8	3	7	E	2	5	B	4
S_13(×)	0	A	C	5	4	3	B	E	F	D	1	6	2	9	7	8
S_14(×)	4	6	F	8	0	B	1	E	3	9	C	5	A	D	7	2
S_15(×)	1	0	C	A	9	E	6	7	F	4	3	D	2	B	5	8
S_16(×)	0	A	F	4	3	C	E	9	8	7	1	D	5	B	6	2
S_17(×)	2	C	0	9	A	5	D	7	F	3	4	E	1	6	B	8
S_18(×)	1	0	5	E	F	2	8	D	6	C	A	B	9	7	3	4
S_19(×)	1	0	F	4	3	E	8	B	6	A	9	7	C	D	5	2
S_20(×)	0	F	9	7	4	8	A	3	5	2	6	C	B	E	D	1

boyundaki 10 kriptografik özelliğe göre mümkün olan en iyi değerlere sahip S-kutularının (Bölüm 6'da "KRİTERLER-2" olarak belirtilmiştir.), BIBO Örüntüleri 8 olduğu için "Panda" S-kutusuna göre, daha iyi kriptografik özelliklere sahip oldukları tespit edilmiştir.

Tez çalışmasının sonuçlarına göre; 4 × 4 boyutuda hem involutif hem de incelenen 10 kriptografik özelliğe göre mümkün olan en iyi değerlere sahip olan S-kutuları sunulmuştur. Tez kapsamındaki çalışmalar ile literatürde bulunan 4×4 boyutunda involutif S-kutularından, 10 kriptografik özelliğe göre daha iyi değerlere sahip olan S-kutuları tespit edilerek literatüre katkıda bulunulmuştur.

Çizelge 4.16. 4 × 4 Boyutunda 10 Kriptografik Özelliğe Göre En İyi ve Bitslice Kapı Karmaşıklığı En Az Olan S-Kutuları (Son 28)

×	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**A**	**B**	**C**	**D**	**E**	**F**
S_21(×)	0	A	2	D	9	6	5	B	F	4	1	7	E	3	C	8
S_22(×)	4	A	C	3	0	9	B	7	F	5	1	6	2	E	D	8
S_23(×)	0	F	5	B	9	2	A	C	8	4	6	3	7	E	D	1
S_24(×)	2	F	0	8	9	6	5	B	3	4	D	7	C	A	E	1
S_25(×)	0	F	2	8	9	7	C	5	3	4	D	E	6	A	B	1
S_26(×)	8	6	F	9	A	5	1	C	0	3	4	E	7	D	B	2
S_27(×)	0	F	9	4	3	D	C	A	8	2	7	E	6	5	B	1
S_28(×)	0	F	5	8	4	2	B	E	3	D	C	6	A	9	7	1
S_29(×)	0	C	2	5	A	3	D	E	F	B	4	9	1	6	7	8
S_30(×)	0	C	2	9	F	7	8	5	6	3	D	E	1	A	B	4
S_31(×)	0	F	2	4	3	8	D	E	5	B	C	9	A	6	7	1
S_32(×)	0	1	F	4	3	E	8	D	6	C	B	A	9	7	5	2
S_33(×)	4	F	9	6	0	8	3	D	5	2	A	C	B	7	E	1
S_34(×)	0	1	C	A	F	8	7	6	5	E	3	D	2	B	9	4
S_35(×)	1	0	C	6	F	8	3	D	5	E	A	B	2	7	9	4
S_36(×)	4	F	5	8	0	2	B	D	3	C	A	6	9	7	E	1
S_37(×)	2	6	0	D	F	8	1	E	5	9	C	B	A	3	7	4
S_38(×)	0	6	F	8	4	B	1	D	3	C	E	5	9	7	A	2
S_39(×)	8	F	9	4	3	C	6	A	0	2	7	D	5	B	E	1
S_40(×)	0	C	5	A	F	2	E	9	8	7	3	D	1	B	6	4
S_41(×)	0	1	9	E	A	6	5	B	F	2	4	7	D	C	3	8
S_42(×)	4	C	9	3	0	B	A	7	F	2	6	5	1	E	D	8
S_43(×)	4	A	F	5	0	3	8	E	6	9	1	C	B	D	7	2
S_44(×)	0	1	F	8	A	C	7	6	3	E	4	D	5	B	9	2
S_45(×)	2	C	0	5	F	3	8	E	6	9	D	B	1	A	7	4
S_46(×)	0	1	5	E	F	2	8	B	6	A	9	7	D	C	3	4
S_47(×)	8	C	5	3	F	2	A	9	0	7	6	B	1	E	D	4
S_48(×)	0	6	2	D	F	8	1	B	5	A	9	7	E	3	C	4

Çizelge 4.17. 4 × 4 Boyutunda Literatürde Bulunan İnvolutif 17 S-Kutusunu Kriptografik Özellikleri

S-Kutusu	DDT	LAT	AD	FP	BIBO Örüntü	LBN	DBN	$\#\mathcal{U}$	$\#\mathcal{L}$	BCTU	DLCTU
Pride	4	4	2	4	13	2	2	24	36	16	8
Prost	4	4	2	4	13	2	2	24	36	16	8
Panda	4	4	3	2	20	2	2	15	30	6	8
KLEIN	4	4	3	0	14	2	2	15	30	10	8
Qarma_sigma0	4	4	2	2	26	2	2	18	32	10	8
Qarma_sigma1	4	4	3	0	20	2	2	15	30	10	8
Midori_Sb0	4	4	2	4	27	2	2	24	36	16	8
Midori_Sb1	4	4	3	4	27	2	2	15	30	10	8
Noekeon	4	4	2	4	13	2	2	24	36	16	8
MANTIS	4	4	2	4	27	2	2	24	36	16	8
Iceberg_S0	4	4	3	0	14	2	2	15	30	10	8
Iceberg_S1	4	4	3	0	16	2	2	15	30	10	8
Anubis_S0	4	4	3	0	14	2	2	15	30	10	8
Anubis_S1	4	4	3	0	16	2	2	15	30	10	8
Khazad_P	4	4	3	0	12	2	2	15	30	10	8
Khazad_Q	4	4	3	0	15	2	2	15	30	10	8
Minalpher	4	4	3	0	16	2	2	15	30	10	8

BÖLÜM 5

GENETİK ALGORİTMA İLE 5 × 5 BOYUTUNDA ELDE EDİLEN S-KUTULARININ KRİPTOGRAFİK ÖZELLİKLERİNİN İNCELENMESİ

Tezin bu bölümünde, 5 × 5 boyutunda genetik algoritma ile ortaya konulan S-kutuları incelenmiş, kriptografik özelliklere göre karşılaştırılmalı sonuçları özetlenmiştir. Literatürde bulunan 5 × 5 boyutundaki S-kutuları ile tez çalışmasından elde edilen 5 × 5 boyutunda involutif S-kutuları karşılaştırılmıştır.

Tez çalışması kapsamında, 5 × 5 boyutunda tüm bijektif S-kutusu permütasyon sayısı 32! olduğu için ölçeklenebilir zamanda involutif olan tüm S-kutularının incelenmesi mümkün olmamaktadır. Bu sebeple genetik algoritma ile 5 × 5 boyutunda; en büyük Fark Dağılım Tablosu değeri, en büyük mutlak Doğrusal Yaklaşım Tablosu değeri ve cebirsel derece açısından diferansiyel, doğrusal ve cebirsel saldırılara dayanıklı değerlere sahip, involutif 2 adet $F_2^5 \rightarrow F_2^5$'e tanımlı S-kutusu tespit edilmiştir.

Genetik algoritma ile 5 × 5 boyutunda S-kutusu saptanmasını gösteren sözde (psuedo) kod takip edildiği şekilde özetlenebilir.

```
fonksiyon genetik_algoritma(populasyon, arama_secenegi,
   mutasyon_orani, mutasyon_tekrar, cikti_dosya_adi, sabit_nokta)
   :
    fitness = fitness_hesapla(populasyon)  # Baslangic
   populasyonu icin fitness hesapla

    benzerlik_sayaci = 0  # Benzerlik izlemek icin sayac

    while dogru:
        eski_populasyon = kopyala(populasyon)  # Mevcut
   populasyonu kopyala
```

```
8       strs = kume()  # Mevcut populasyonu saklamak icin kume
9
10      # Populasyonun tamami icin fitness hesapla (paralel islem
    )
11      her_icin_paralel(populasyon):
12          fitness[i] = fitFunc(populasyon[i])
13
14      # Strs kumesini guncelle
15      strs.update(populasyon)
16
17      # DdtLatOptList'i optimal cozumlerle guncelle
18      ddt_lat_opt_listesini_guncelle(populasyon, fitness,
    arama_secenegi)
19
20      # Benzerlik temelinde konverjans  kontrol et eger strs
    eski_populasyona benziyorsa:
21          benzerlik_sayaci += 1
22          eger benzerlik_sayaci == 1000 ise:
23              kiril  # Cok uzun sure benzer kalmissa donguyu
    kir aksi takdirde:
24          benzerlik_sayaci = 0
25
26      # Mevcut iterasyon hakkinda bilgiyi goruntule
27      iterasyon_bilgisini_goruntule(fitness, strs,
    eski_populasyon)
28
29      # Ebeveynleri fitness'e dayanarak sec
30      ebeveynler = ebeveyn_sec(populasyon, fitness, populasyon.
    boyutu / 2)
31
32      # Caprazlama yaparak soy nesil olustur
33      soy_nesil_crossover = caprazlama(ebeveynler, sabit_nokta)
34
35      # Soy nesil uzerinde mutasyon yap
36      soy_nesil_mutasyon = mutasyon(soy_nesil_crossover,
    mutasyon_orani, mutasyon_tekrar, sabit_nokta)
37
38      # Populasyonu ebeveynler ve mutasyonlu soy nesil ile
    guncelle
39      populasyonu_guncelle(populasyon, ebeveynler,
    soy_nesil_mutasyon)
40
41   # Son ddtLatOptList'ini bir dosyaya yaz
42   dosyaya_yaz(cikti_dosya_adi, ddtLatOptList)
43
```

```
fonksiyon ddt_lat_opt_listesini_guncelle(populasyon, fitness, arama_secenegi):
    her_i in 0'dan populasyon.boyutu'na kadar:
        min_fitness = arama_secenegi - (arama_secenegi % 10000)
        max_fitness = arama_secenegi
        eger fitness[i] <= max_fitness ve fitness[i] >= min_fitness ve populasyon[i] ddtLatOptList icinde degilse:
            lat_max = GenerateLAT(populasyon[i])'nin en yuksek degerini al
            eger lat_max <= 6 ise:
                ddtLatOptList'e populasyon[i]'yi ekle

fonksiyon iterasyon_bilgisini_goruntule(fitness, strs, eski_populasyon):
    min_fitness = min(fitness)
    benzersiz_populasyon = len(strs)
    degisim_miktari = len(strs - eski_populasyon)
    yaz("Min DDT - Min LAT:", min_fitness, "Benzersiz populasyon:", benzersiz_populasyon, "Degisim miktari:", degisim_miktari)

fonksiyon populasyonu_guncelle(populasyon, ebeveynler, soy_nesil_mutasyon):
    her_icin aralik(ebeveynler.boyutu):
        populasyon[i] = ebeveynler[i]

    her_i in aralik(ebeveynler.boyutu, ebeveynler.boyutu + soy_nesil_mutasyon.boyutu):
        populasyon[i] = soy_nesil_mutasyon[i - ebeveynler.boyutu]
```

Çizelge 5.1. 5 × 5 Boyutunda S-Kutusu-1

×	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
S(×)	6	20	22	3	15	19	0	31	26	9	27	23	17	18	25	4	28	12	13	5	1	24	2	11	21	14	8	10	16	30	29	7

Tez çalışması kapsamında; 5 × 5 boyutunda en büyük Fark Dağılım Tablosu değeri, en büyük mutlak Doğrusal Yaklaşım Tablosu değeri ve cebirsel derece açısından kriptografik özellik olarak iyi değerlere sahip olan 2 sabit noktalı, involutif, Çizelge 5.1'de verilen S-kutusunun kriptografik özellikleri takip edildiği şekilde özetlenebilir:

- Fark Dağılım Tablosu en büyük değeri **2**
- Doğrusal Yaklaşım Tablosu mutlak en büyük değeri **6**
- Cebirsel derece **4**
- Doğrusal dal sayısı **2**

- Diferansiyel dal sayısı **2**
- BIBO Örüntüsü **32**
- Diferansiyel tekdüzelik frekansı **496**
- Doğrusallık frekansı **31**
- BCTU değeri **2**
- DLCTU değeri **16**

Çizelge 5.1'de verilen S-kutusunun, bitslice kapı karmaşıklığı **182** olmaktadır.

Çizelge 5.2. 5 × 5 Boyutunda S-Kutusu-2

×	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
S(×)	8	26	6	31	25	20	2	19	0	10	9	30	13	12	14	22	21	17	24	7	5	16	15	28	18	4	1	29	23	27	11	3

Tez çalışması kapsamında; 5 × 5 boyutunda, 2 sabit noktalı, involutif, Çizelge 5.2'de Çizelge 5.1'den farklı olarak verilen S-kutusunun, kriptografik özellikleri takip edildiği şekilde özetlenebilir:

- Fark Dağılım Tablosu en büyük değeri ((0, 0) konumu hariç) **2**
- Doğrusal Yaklaşım Tablosu mutlak en büyük değeri ((0, 0) konumu hariç) **6**
- Cebirsel derece **4**
- Doğrusal dal sayısı **2**
- Diferansiyel dal sayısı **2**
- BIBO Örüntüsü **32**
- Diferansiyel tekdüzelik frekansı **496**
- Doğrusallık frekansı **31**
- BCTU değeri **2**
- DLCTU değeri **16**

Çizelge 5.2'de verilen S-kutusunun, bitslice kapı karmaşıklığı **190** olmaktadır.

Çizelge 5.3. 5 × 5 Boyutunda Literatürde Bulunan 10 İnvolutif Olmayan S-Kutusunun Kriptografik Özelliklerinin İncelenmesi

S-Kutusu	DDT	LAT	AD	FP	BIBO Örüntü	LBN	DBN	$\#\mathcal{U}$	$\#\mathcal{L}$	BCTU	DLCTU
keccak	8	8	2	2	10	2	2	20	40	16	16
Ascon	8	8	2	0	0	3	3	20	40	16	16
Fides_5	2	4	2	0	22	2	2	496	496	2	16
SC2000_5	2	4	3	0	27	2	2	496	496	2	16
icepole	8	8	2	0	30	2	2	10	30	18	16
APN_S0	2	6	4	3	33	2	2	496	31	2	16
APN_S1	2	4	3	3	28	2	2	496	496	2	16
APN_S2	2	4	3	3	30	2	2	496	496	2	16
APN_S3	2	4	2	4	30	2	2	496	496	2	16
APN_S4	2	4	2	3	28	2	2	496	496	2	16

5.1 5 × 5 Boyutunda Literatürde Bulunan 10 İnvolutif Olmayan S-Kutusunun Kriptografik Özelliklerinin İncelenme Sonuçları

Literatürde 5 × 5 boyutunda involutif S-kutuları bulunmadığı için, literatürde mevcut olan 5 × 5 boyutunda involutif olmayan S-kutuları, tez çalışması kapsamındaki kriptografik özelliklere göre incelenmiştir (Peigen, 2023). İnceleme sonuçlarının karşılaştırmaları, Çizelge 5.3'te sunulmuştur (Bao vd., 2019)

Çizelge 5.3'te verilen S-kutularına göre, tez kapsamında incelenen kriptografik özelliklere göre en iyi değerlere sahip olan S-kutusunun "APN_S0" olduğu saptanmıştır.

Çizelge 5.3'te, belirtilen "APN_S0" S-kutusu, tez çalışmasında genetik algoritma ile elde edilen 2 tane 5×5 boyutunda S-kutusu ile benzer (BIBO Örüntü değeri ve involutif özelliği farklılaşmaktadır.) kriptografik özelliklere sahip olmaktadır. Tez çalışmasında sunulan 5 × 5 boyundaki 2 tane S-kutusunun, BIBO örüntüsü 32 olduğu için Çizelge 5.3'te belirtilen "APN_S0" S-kutusuna göre daha iyi kriptografik özelliklere sahip olduğu tespit edilmiştir. Tez çalışmasında genetik algoritma ile elde edilen 2 tane 5×5 boyutundaki S-kutusu, aynı zamanda involutif özelliği de sağlamaktadır.

Sonuç olarak, tez çalışmasında sunulan 5 × 5 boyundaki S-kutularının, hem involutif özelliği sağlama durumlarından hem de iyi kriptografik özelliklere sahip olmalarından dolayı; literatüre yeni 5 × 5 boyutundaki involutif S-kutuları olarak katkıda bulunulmuştur.

BÖLÜM 6

SONUÇ VE GELECEK ÇALIŞMALAR

Tez çalışmasının bu bölümünde; involutif, optimal tüm 3×3, 4×4 boyutundaki ve genetik algoritma ile elde edilen 5×5 boyutunda olan S-kutularının, 10 kriptografik özelliğine göre karşılaştırılmalı analizleri yapılmıştır. İncelenen S-kutularından, mümkün olan en iyi kriptografik özelliklere sahip olan S-kutuları belirtilmiştir.

Yer değiştirme kutuları incelenirken her kriptografik özellik, başka bir kriptografik saldırıya karşı dayanıklılığı ölçümlemekte kullanılmaktadır (Bao vd., 2019). Her kriptografik özelliğe göre mümkün olan en iyi değerlere sahip olan S-kutularının saptanmasında amaçlanmaktadır.

Tez çalışması kapsamında S-kutularının incelenen 10 kriptografik özelliği aşağıdaki gibi belirlenmiştir:

- En Büyük Fark Dağılım Tablosu Değeri ((0, 0) konumu hariç)
- En Büyük Mutlak Doğrusal Yaklaşım Tablosu Değeri ((0, 0) konumu hariç)
- Cebirsel Derece
- BIBO Örüntüsü
- Doğrusal Dal Sayısı
- Diferansiyel Dal Sayısı
- Diferansiyel Tekdüzelik Frekansı
- Doğrusallık Frekansı

- Boomerang Bağlantı Tablosu Tekdüzeliği
- Diferansiyel Doğrusal Bağlantı Tablosu Tekdüzeliği

Toplamda 10 adet kriptografik özelliğe göre tüm involutif 3×3, 4×4 boyutundaki S-kutuları ve genetik algoritma ile bulunan 5×5 boyutundaki involutif S-kutuları incelenmiştir. "İnvolutif" özelliği ve "Sabit Nokta Sayısı" tez çalışmasındaki incelemelere dahil edilmiş ancak kriptografik özellik olarak nitelendirilmemiştir.

6.1 3×3 Boyutunda S-Kutularının Kriptografik Özelliklere Göre Karşılaştırmaları

Tez çalışmasında elde edilen sonuçlara göre; 3×3 boyutunda S-kutularının en iyi kriptografik özellikleri, takip edildiği şekilde özetlenebilir:

- En Büyük Fark Dağılım Tablosu Değeri **2**
- En Büyük Mutlak Doğrusal Yaklaşım Tablosu Değeri **2**
- Cebirsel Derece **2**
- BIBO Örüntüsü **6**
- Sabit Nokta Sayısı **2**
- Doğrusal Dal sayısı **2**
- Diferansiyel Dal Sayısı **2**
- Diferansiyel Tekdüzelik Frekansı **28**
- Doğrusallık Frekansı **28**
- BCTU Değeri **2**
- DLCTU Değeri **4**

3-bit giriş ve çıkış değerlerine sahip olan optimal S-kutularının alt gruplara ayrılmasını sağlayan tek kriptogrfik özelliği; BIBO örüntüsü olmaktadır.

6.2 4×4 Boyutunda S-Kutularının Kriptografik Özelliklere Göre Karşılaştırmaları

Tez çalışmasındaki incelemelerde; 4×4 boyutundaki optimal S-kutularının, sabit nokta sayılarına göre kriptografik özellikleri incelenmiştir. İnceleme sonuçları; sabit nokta sayılarına alt gruplar halinde karşılaştırılmalı olarak analiz edilmiştir.

6.2.1 4×4 Boyutunda Sabit Nokta Sayısı 0 Olan Alt Grubun S-Kutularının Karşılaştırması

Bu alt grubun içerisindeki BIBO örüntüleri, $9 - 27$ aralığında bulunmaktadır. İncelenen alt gruptaki tüm S-kutularının diferansiyel tekdüzelik frekansı 15 ve doğrusallık frekansı 30 olarak tespit edilmiştir. Grubun içerisinde tüm S-kutularının BCTU değeri 10 ve DLCTU değeri 8 olarak saptanmıştır. Bu incelenen "Optimal" alt gruptan, diğer bir deyişle; involutif, en büyük Fark Dağılım Tablosu değeri 4, en büyük mutlak Doğrusal Yaklaşım Tablosu değeri 4, cebirsel derece 3 olan 4×4 boyutunda S-kutuları içerisinden, sabit nokta sayısı 0 olması koşuluyla kriptografik özelliklere göre iyi olanları; BIBO örüntüsü 9 olan (S-kutusunun BIBO örüntüsünün düşük olması tercih edilir (Bao vd., 2019).) 384 tane S-kutusu olmaktadır. Bu özelliklere sahip olan 4×4 boyutunda S-kutuları, "KRİTERLER-1" olarak tanımlanmıştır.

KRİTERLER-1: #{İnvolutif, En Büyük Fark Dağılım Tablosu Değeri 4, En Büyük Mutlak Doğrusal Yaklaşım Tablosu Değeri 4, Cebirsel Derece 3, Sabit Nokta 0, Diferansiyel Tekdüzelik Frekansı 15, Doğrusallık Frekansı 30, BIBO Örüntüsü 9, Doğrusal Dal Sayısı 2, Diferansiyel Dal Sayısı 2, BCTU Değeri 10, DLCTU Değeri 8} = 384

6.2.2 4×4 Boyutunda Sabit Nokta Sayısı 2 Olan Alt Grubun S-Kutularının Karşılaştırması

Tez çalışma sonuçlarının bir diğer karşılaştırması Bölüm 4'te belirtilen Çizelge 4.11 ve Çizelge 4.13'te sunulmuştur. Bu alt grupta; "Optimal" özelliklere sahip olmalarına ek olarak, 2 tane sabit nokta barındıran 4×4 boyutunda S-kutularına yoğunlaşılmıştır. Alt gruptaki S-kutularının BIBO örüntülerinin, $8 - 30$ arasında olduğu tespit edilmiştir. İncelenenler arasında, diferansiyel tekdüzelik frekans değeri 24 ve doğrusallık frekans değeri 36 olan hiçbir S-kutusu bulunmamasına rağmen, farklı BIBO örüntülerde diferansiyel tekdüzelik/doğrusallık frekansları $15/30$ ve $18/32$ olan S-kutuları tespit edilmiştir. S-kutularının diferansiyel tekdüzelik ve doğrusallık frekans değerlerine göre, karşılaştırmalı olarak küçük olması tercih edilmektedir (Saarinen, 2012). Diğer bir deyişle, S-kutusunun frekans değerlerince küçük olması durumunda, S-kutusu doğrusal ve diferansiyel saldırılara daha dayanıklı hale gelmektedir (Saarinen, 2012). Bu alt grupta, BIBO örüntüsünün 28, 29 ve 30 haricindekilerde; BCTU 6, 8 ve 10 değerlerinde S-kutuları bulunmaktadır. Sabit nokta sayısı 0, 2, 4 ve 6 olan bütün 4×4 boyutundaki S-kutuların DLCTU değeri 8 olarak tespit edilmiştir. Bu alt grubun içerisinde; tez çalışmasında incelenen 10 kriptografik özelliğe göre en iyi S-kutularının BIBO Örüntüsü 8 ve BCTU değeri 6 (S-kutularında, BCTU değerinin karşılaştırılmalı olarak düşük olması gerektiği

savunulmaktadır (Bao vd., 2019).) olmaktadır. Bu alt grupta, en iyi kriptografik özelliklere sahip 384 tane S-kutusu belirlenmiştir.

Bu alt grupta elde edilen kriptografik özelliklere göre en iyi 4×4 boyutunda S-kutuları, tez çalışması kapsamında ortaya konulmuş ve önerilmiş olan en iyi 4×4 boyutunda S-kutuları olmaktadır. Bu özelliklere sahip olan 4×4 boyutunda S-kutuları, "KRİTERLER-2" olarak tanımlanmıştır.

KRİTERLER-2: #{İnvolutif, En Büyük Fark Dağılım Tablosu Değeri 4, En Büyük Mutlak Doğrusal Yaklaşım Tablosu Değeri 4, Cebirsel Derece 3, Sabit Nokta 2, Diferansiyel Tekdüzelik Frekansı 15, Doğrusallık Frekansı 30, BIBO Örüntüsü 8, Doğrusal Dal Sayısı 2, Diferansiyel Dal Sayısı 2, BCTU Değeri 6, DLCTU Değeri 8} = 384

6.2.3 4×4 Boyutunda Sabit Nokta Sayısı 4 Olan Alt Grubun S-Kutularının Karşılaştırması

Sabit nokta sayısının 4 olduğu durumlardaki optimal 4×4 boyutunda S-kutularının incelenmeleri, Bölüm 4'te belirtilen Çizelge 4.12'de ifade edilmiştir. İncelenen S-kutularının BIBO örüntüleri $9 - 29$ aralığında olmaktadır. Bu alt grupta incelenen S-kutularının tümünün DLCTU değeri 8 olarak tespit edilmiştir. S-kutularının BCTU değeri 6, 10 veya 16 olabilmektedir. Bu alt gruptaki bütün S-kutularının içerisinde diferansiyel tekdüzelik/doğrusallık frekansları $18/32$ olan hiçbir S-kutusu bulunmamasının yanısıra, bu alt gruptaki S-kutularının diferansiyel tekdüzelik/doğrusallık frekansları; $15/30$ veya $24/36$ değerlerini almaktadır. BIBO örüntüsünün en küçük, BCTU değerinin en küçük ve frekans dağılımı açısından $15/30$ değerlerine sahip 768 adet S-kutusu, bu alt grubun incelenen kriptografik özelliklere göre en iyileri olmaktadır. Bu özelliklere sahip olan 4×4 boyutunda S-kutuları, "KRİTERLER-3" olarak tanımlanmıştır.

KRİTERLER-3: #{İnvolutif, En Büyük Fark Dağılım Tablosu Değeri 4, En Büyük Mutlak Doğrusal Yaklaşım Tablosu Değeri 4, Cebirsel Derece 3, Sabit Nokta 4, Diferansiyel Tekdüzelik Frekansı 15, Doğrusallık Frekansı 30, BIBO Örüntüsü 9, Doğrusal Dal Sayısı 2, Diferansiyel Dal Sayısı 2, BCTU Değeri 6, DLCTU Değeri 8} = 768

6.2.4 4×4 Boyutunda Sabit Nokta Sayısı 6 Olan Alt Grubun S-Kutularının Karşılaştırması

Sabit nokta sayısının 6 olduğu durumlardaki 4×4 boyutundaki optimal S-kutularının, BIBO örüntüleri $13 - 27$ aralığında olmaktadır. İncelenen bu alt grubun içerisindeki tüm S-kutularının diferansiyel tekdüzelik/doğrusallık frekansı tek değer olup,

15/30'dur. Tüm S-kutularının DLCTU değeri 8 olmaktadır. Bu alt grubun S-kutularının BCTU değeri 6 ve 8 olarak tespit edilmiştir. Ancak bazı BIBO örüntü gruplarında (BIBO örüntü 13, 16, 26) BCTU değeri 6 olan S-kutuları bulunmamaktadır. Bu alt gruptaki en iyi S-kutularının kriptografik özellikleri takip edildiği şekilde özetlenebilir: BIBO örüntüsü 13, DLCTU değeri 8, BCTU değeri 8 ve diferansiyel tekdüzelik/doğrusallık frekansları 15/30. Bu kriptografik özelliklere sahip olan, 4×4 boyutunda 1,152 tane S-kutusu tespit edilmiştir. Bu özelliklere sahip olan 4×4 boyutunda S-kutuları, "KRİTERLER-4" olarak tanımlanmıştır.

KRİTERLER-4: #{İnvolutif, En Büyük Fark Dağılım Tablosu Değeri 4, En Büyük Mutlak Doğrusal Yaklaşım Tablosu Değeri 4, Cebirsel Derece 3, Sabit Nokta 6, Diferansiyel Tekdüzelik Frekansı 15, Doğrusallık Frekansı 30, BIBO Örüntüsü 13, Doğrusal Dal Sayısı 2, Diferansiyel Dal Sayısı 2, BCTU Değeri 8, DLCTU Değeri 8} = 1,152

6.3 Bitslice Kapı Karmaşıklığı (Bitslice Gate Complexity) Karşılaştırma

Tez kapsamındaki çalışma; yazılım tabanlı olduğu için S-kutularının bitslice kapı maliyeti/karmaşıklığı, her mantıksal kapının (XOR, AND) maliyetini aynı kabul edip, S-kutularının vektörel çıkış Boole fonksiyonlarının cebirsel ifadelerinde herhangi bir optimizasyon işlemi uygulanmadan hesaplanmıştır.

İncelenen S-kutularının sadece saldırılara karşı dayanıklı olması değil, aynı zamanda S-kutusunun uygulanmasındaki (implementation) maliyetini de ölçümlemek gerekmektedir. Bu sebeple, incelenen S-kutularının bitslice kapı karmaşıklıkları analiz edilmiştir (Ullrich vd., 2011).

Bölüm 3 ve 4'te sırasıyla 3×3 ve 4×4 boyutlarındaki, tez çalışmasında incelenen 10 kriptografik özelliğe göre en iyi değerlere sahip olan S-kutularının bitslice kapı karmaşıkları analiz edilmiştir. İncelenen bu S-kutularından, en az kapı karmaşıklığına sahip olan S-kutuları, Bölüm 3 ve 4'te sunulmuştur.

Bölüm 5'te genetik algoritma ile bulunan 5×5 boyutunda S-kutularının, bitslice kapı karmaşıklıkları incelenerek ilgili bölümde sunulmuştur.

Gelecek çalışmalarda; S-kutularına ait olan yeni kriptografik özelliklerin ortaya çıkması durumunda, bu tez çalışmasında değerlendirilen kriterlerin genişletilmesi beklenebilir. İleri zamanlarda yapılacak çalışmalarda, farklı boyutlarda S-kutularının kriptografik özellikleri incelenerek, araştırmalar detaylandırılabilir.

KAYNAKLAR

Al-Shabi, M. (2019). A survey on symmetric and asymmetric cryptography algorithms in information security. *International Journal of Scientific and Research Publications (IJSRP)*, *9*(3), 576–589.

Ashok, P. & Bhaaskaran, V. s. k. (2018). Lightweight S-Box Architecture for Secure Internet of Things. *Information*, *9*, 13. https://doi.org/10.3390/info9010013

Banik, S., Pandey, S. K., Peyrin, T., Sasaki, Y., Sim, S. M. & Todo, Y. (2017). GIFT: A Small Present. İçinde W. Fischer & N. Homma (Ed.), *Cryptographic Hardware and Embedded Systems – CHES 2017* (ss. 321–345). Springer International Publishing.

Bao, Z., Guo, J., Ling, S. & Sasaki, Y. (2019). SoK: Peigen – a Platform for Evaluation, Implementation, and Generation of S-boxes [https://eprint.iacr.org/2019/209]. https://eprint.iacr.org/2019/209

Bar-On, A., Dunkelman, O., Keller, N. & Weizman, A. (2019). *DLCT: A New Tool for Differential-Linear Cryptanalysis* (International Edition). Alan R. Apt.

Bhanot, R. & Hans, R. (2015). A review and comparative analysis of various encryption algorithms. *International Journal of Security and Its Applications*, *9*(4), 289–306.

Biham, E. (1997). A fast new DES implementation in software. *Fast Software Encryption: 4th International Workshop, FSE'97 Haifa, Israel, January 20–22 1997 Proceedings 4*, 260–272.

Blondeau, C. & Nyberg, K. (2013). New links between differential and linear cryptanalysis. *Advances in Cryptology–EUROCRYPT 2013: 32nd Annual International Conference on the Theory and Applications of Cryptographic Techniques, Athens, Greece, May 26-30, 2013. Proceedings 32*, 388–404.

Boura, C. & Canteaut, A. (2018). On the Boomerang Uniformity of Cryptographic Sboxes. *IACR Transactions on Symmetric Cryptology*, *2018*. https://doi.org/10.13154/tosc.v2018.i3.290-310

Braeken, A. (2006). *Cryptographic Properties of Boolean Functions and S-boxes* (dok. tezi). Katholieke Universiteit Leuven.

Buchmann, J. (2004). *Introduction to cryptography* (C. 335). Springer.

Canard, S., Pointcheval, D., Santos, Q. & Traoré, J. (2018). Privacy-preserving plaintext-equality of low-entropy inputs. *Applied Cryptography and Network Security: 16th International Conference, ACNS 2018, Leuven, Belgium, July 2-4, 2018, Proceedings 16*, 262–279.

Canteaut, A., Kölsch, L., Li, C., Li, C., Li, K., Qu, L. & Wiemer, F. (2019). On the Differential-Linear Connectivity Table of Vectorial Boolean Functions.

Cao, M. & Zhang, W. (2019). Related-Key Differential Cryptanalysis of the Reduced-Round Block Cipher GIFT. *IEEE Access*, *7*, 175769–175778. https://doi.org/10.1109/ACCESS.2019.2957581

Center, C. S. R. (2023). *Lightweight Cryptography Standardization Process: NIST Selects Ascon*. https://csrc.nist.gov/News/2023/lightweight-cryptography-nist-selects-ascon

Chen, J., Gong, Z., Tang, Y. & Dong, X. (2022). A comprehensive analysis of lightweight 8-bit sboxes from iterative structures. *Journal of Information Security and Applications*, *70*, 103302. https://doi.org/https://doi.org/10.1016/j.jisa.2022.103302

Cid, C., Huang, T., Peyrin, T., Sasaki, Y. & Song, L. (2018). Boomerang Connectivity Table: A New Cryptanalysis Tool. İçinde J. B. Nielsen & V. Rijmen (Ed.), *Advances in Cryptology – EUROCRYPT 2018* (ss. 683–714). Springer International Publishing.

Bahceci, Y. S. & Özkaynak, F. (2020). Rasgele Seçim Tabanlı Yer Değiştirme Kutularının Performans İyileştirmesi için Son İşlem Algoritmaları. *Bilgisayar Bilimleri ve Teknolojileri Dergisi*, *1*(1), 16–21.

Dinur, I. & Shamir, A. (2009). Cube attacks on tweakable black box polynomials. *Advances in Cryptology-EUROCRYPT 2009: 28th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Cologne, Germany, April 26-30, 2009. Proceedings 28*, 278–299.

Dutta, I. K., Ghosh, B. & Bayoumi, M. (2019). Lightweight cryptography for internet of insecure things: A survey. *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 0475–0481.

Forouzan, B. A. (2008). *Introduction to Cryptography and Network Security* (International Edition). Alan R. Apt.

Fu, S. & Feng, X. (2019). Involutory differentially 4-uniform permutations from known constructions. *Designs, Codes and Cryptography*, *87*, 31–56.

Fuhr, T. (2010). Finding second preimages of short messages for Hamsi-256. *Advances in Cryptology-ASIACRYPT 2010: 16th International Conference on the Theory and Application of Cryptology and Information Security, Singapore, December 5-9, 2010. Proceedings 16*, 20–37.

Galbraith, S. D. (2012). *Mathematics of public key cryptography*. Cambridge University Press.

Hellman, M. E. (2002). An overview of public key cryptography. *IEEE Communications Magazine*, *40*(5), 42–49.

Jangra, M. & Singh, B. (2022). Substitution Box for Encryption in Internet of Things. *2022 IEEE IAS Global Conference on Emerging Technologies (GlobConET)*, 1130–1137. https://doi.org/10.1109/GlobConET53749.2022.9872343

Jiao, S., Lei, T., Gao, Y., Xie, Z. & Yuan, X. (2019). Known-plaintext attack and ciphertext-only attack for encrypted single-pixel imaging. *IEEE Access*, *7*, 119557–119565.

Kim, H., Jeon, Y., Kim, G., Kim, J., Sim, B.-Y., Han, D.-G., Seo, H., Kim, S., Hong, S., Sung, J. & Hong, D. (2021). A New Method for Designing Lightweight S-Boxes With High Differential and Linear Branch Numbers, and its Application. *IEEE Access*, *9*, 150592. https://doi.org/10.1109/ACCESS.2021.3126008

Kim, S., Hong, D., Sung, J. & Hong, S. (2020). Classification of 4-bit S-Boxes for BOGI Permutation. *IEEE Access*, *8*, 210935–210949. https://doi.org/10.1109/ACCESS.2020.3039273

Li, L., Liu, J., Guo, Y. & Liu, B. (2022). A new S-box construction method meeting strict avalanche criterion. *Journal of Information Security and Applications*, *66*, 103135. https://doi.org/https://doi.org/10.1016/j.jisa.2022.103135

Liu, B., Gong, Z., Qiu, W. & Zheng, D. (2011). On the security of 4-bit involutive s-boxes for lightweight designs. *International Conference on Information Security Practice and Experience*, 247–256.

Liu, M., Lu, X. & Lin, D. (2021). Differential-Linear Cryptanalysis from an Algebraic Perspective. İçinde T. Malkin & C. Peikert (Ed.), *Advances in Cryptology – CRYPTO 2021* (ss. 247–277). Springer International Publishing.

Liu, Y., Sun, S. & Li, C. (2021). Rotational Cryptanalysis from a Differential-Linear Perspective. İçinde A. Canteaut & F.-X. Standaert (Ed.), *Advances in Cryptology – EUROCRYPT 2021* (ss. 741–770). Springer International Publishing.

Loebenberger, D. & Nüsken, M. (2013). A family of 6-to-4-bit S-boxes with large linear branch number [https://eprint.iacr.org/2013/188]. https://eprint.iacr.org/2013/188

Lu, Z., Mesnager, S., Cui, T., Fan, Y. & Wang, M. (2022). An STP-based model toward designing S-boxes with good cryptographic properties. *Des. Codes Cryptogr.*, *90*. https://doi.org/https://doi.org/10.1007/s10623-022-01034-2

Manual, S. 1. R. (2023). *S-Boxes and Their Algebraic Representations*. https://doc.sagemath.org/html/en/reference/cryptography/sage/crypto/sbox.html

Menezes, A. J., Van Oorschot, P. C. & Vanstone, S. A. (2018). *Handbook of applied cryptography*. CRC press.

Mousavi, M. & Sadeghiyan, B. (2021). A new image encryption scheme with Feistel like structure using chaotic S-box and Rubik cube based P-box. *Multimedia Tools and Applications*, *80*, 13157–13177.

Muir, T. (1960). *A treatise on the theory of determinants, 1933*. reprinted by Dover, New York.

Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A. & Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. *International Journal of Advanced Computer Science and Applications*, *8*(11).

Muthavhine, K. & Sumbwanyambe, M. (2022). Securing IoT Devices against Differential-Linear (DL) Attack Used on Serpent Algorithm. *Future Internet*, *14*(2). https://doi.org/10.3390/fi14020055

Nechvatal, J., Barker, E., Bassham, L., Burr, W., Dworkin, M., Foti, J. & Roback, E. (2001). Report on the development of the Advanced Encryption Standard (AES). *Journal of research of the National Institute of Standards and Technology*, *106*(3), 511.

Nist. (2023). *Nist*. https://www.nist.gov

Oeis. (2023). *Oeis*. https://oeis.org/A000085

Pehlivanoğulu, M. K. (2018). *Maksimum Uzaklıkta Ayrılabilen Matrislerin Elde Edilebilmesi İçin Yeni Bir Matris Formu ve Bir Hafif Sıklet Blok Şifreye Uygulaması* (dok. tezi). Kocaeli Üniversitesi Fen Bilimleri Enstitüsü.

Peigen. (2023). *Peigen*. https://github.com/peigen-sboxes/PEIGEN/tree/master

Petitcolas, F. A. (2023). Kerckhoffs' principle. *Encyclopedia of Cryptography, Security and Privacy* (ss. 1–2). Springer.

Saarinen, M.-J. O. (2012). Cryptographic Analysis of All 4 × 4-Bit S-Boxes. İçinde A. Miri & S. Vaudenay (Ed.), *Selected Areas in Cryptography* (ss. 118–133). Springer Berlin Heidelberg.

Sağıroğlu, Ş., Şenol, M., Bayındır, R., Bilge, Y., Bensghir, T. K., Akleylek, S., Sakallı, M. T., Cenk, M., Doğru, Ö. Ü. İ. A., Dörterler, M. vd. (2019). *Siber Güvenlik ve Savunma: Problemler ve Çözümler*.

Sarkar, S., Mandal, K. & Saha, D. (2019). On the Relationship Between Resilient Boolean Functions and Linear Branch Number of S-Boxes. https://doi.org/10.1007/978-3-030-35423-7_18

Sarkar, S. & Syed, H. (2018). Bounds on Differential and Linear Branch Number of Permutations. İçinde W. Susilo & G. Yang (Ed.), *Information Security and Privacy* (ss. 207–224). Springer International Publishing.

Sharma, N. vd. (2017). A Review of Information Security using Cryptography Technique. *International Journal of Advanced Research in Computer Science*, *8*(4).

Shree, D., Ahlawat, S. vd. (2017). A Review on Cryptography, Attacks and Cyber Security. *International Journal of Advanced Research in Computer Science*, *8*(5).

Sklavos, N. & Zaharakis, I. D. (2016). Cryptography and security in internet of things (iots): Models, schemes, and implementations. *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 1–2.

Smith, R. E. (1997). *Internet cryptography*. Addison-Wesley Longman Publishing Co., Inc.

Sovyn, Y., Opirskyy, I. & Mykhaylova, O. (2023). Finding a Bit-Sliced Representation of 4× 4 S-Boxes based on Typical Logic Processor Instructions.

Stinson, D. R. (2005). *Cryptography: theory and practice*. Chapman; Hall/CRC.

Stoffelen, K. (2016). Optimizing s-box implementations for several criteria using SAT solvers. *International Conference on Fast Software Encryption*, 140–160.

Tang, D., Mandal, B. & Maitra, S. (2021). Construction of balanced vectorial Boolean functions with almost optimal nonlinearity and very low differential-linear uniformity. *Finite Fields and Their Applications*, *76*, 101903. https://doi.org/10.1016/j.ffa.2021.101903

Tho, H., Thang, N., Nga, N. & Hoang, P. (2018). An Algorithm for Improving Algebraic Degree of S-Box Coordinate Boolean Functions Based on Affine Equivalence Transformation. *Journal of Informatics and Mathematical Sciences*, *10*, 339–350. https://doi.org/10.26713/jims.v10i1-2.662

Tiwari, G., Nandi, D. & Mishra, M. (2013). Cryptography and cryptanalysis: a review. *International Journal of Engineering Research & Technology*, *2*(10), 1898–1902.

Tuncay, G. (2015). *Kriptografik ve uygulama özellikleri iyi olan ikili matrislerin üretilmesi için yeni bir arama yöntemi* (yük. lis. tezi). Trakya Üniversitesi Fen Bilimleri Enstitüsü.

Tuncay, G. (2021). *Blok Şifrelerde Kullanilan İkili Ve Mds Matrisler İçin Yeni Tasarim Teknikleri* (dok. tezi). Trakya Üniversitesi Fen Bilimleri Enstitüsü.

Turan, M. S., McKay, K., Chang, D., Bassham, L. E., Kang, J., Waller, N. D., Kelsey, J. M. & Hong, D. (2023). Status Report on the Final Round of the NIST Lightweight Cryptography Standardization Process.

Ullrich, M., De Canniere, C., Indesteege, S., Küçük, O., Mouha, N. & Preneel, B. (2011). Finding Optimal Bitsliced Implementations of 4 × 4-bit S-boxes.

EK A

3 × 3 BOYUTUNDA 10 KRİPTOGRAFİK ÖZELLİĞE GÖRE EN İYİ DEĞERLERE SAHİP 32 TANE S-KUTUSU

Bu bölümde; 3 × 3 boyutunda, involutif, tez kapsamında incelenen 10 kriptografik özelliğe göre mümkün olan en iyi değelere sahip olan, Bölüm 3'te ifade edilen 32 tane S-kutusu verilmiştir.

	0	1	2	3	4	5	6	7
1	2	1	0	7	5	4	6	3
2	4	3	2	1	0	5	7	6
3	6	1	7	4	3	5	0	2
4	6	4	5	3	1	2	0	7
5	0	3	6	1	5	4	2	7
6	3	4	5	0	1	2	6	7
7	0	5	3	2	6	1	4	7
8	7	1	4	3	2	6	5	0
9	7	1	4	6	2	5	3	0
10	7	4	2	5	1	3	6	0
11	0	7	5	6	4	2	3	1
12	0	1	5	6	7	2	3	4
13	6	1	5	3	7	2	0	4
14	0	6	2	5	7	3	1	4
15	5	2	1	4	3	0	6	7
16	5	7	2	4	3	0	6	1
17	3	6	7	0	4	5	1	2
18	7	2	1	5	4	3	6	0
19	0	1	7	4	3	6	5	2
20	6	2	1	4	3	5	0	7
21	7	2	1	6	4	5	3	0
22	0	7	2	4	3	6	5	1
23	7	4	2	3	1	6	5	0

24	5	6	2	3	7	0	1	4
25	4	1	3	2	0	7	6	5
26	5	6	4	3	2	0	1	7
27	2	5	0	3	4	1	7	6
28	3	7	5	0	4	2	6	1
29	0	6	7	5	4	3	1	2
30	1	0	6	3	4	7	2	5
31	3	6	4	0	2	5	1	7
32	1	0	2	7	6	5	4	3

EK B

4 × 4 BOYUTUNDA 10 KRİPTOGRAFİK ÖZELLİĞE GÖRE EN İYİ DEĞERLERE SAHİP 384 TANE S-KUTUSU

Bu bölümde; 4 × 4 boyutunda, involutif, tez kapsamında incelenen 10 kriptografik özelliğe göre mümkün olan en iyi değelere sahip olan, Bölüm 6'da 'KRİTERLER-2' grubunda belirtilen 384 tane S-kutusu verilmiştir.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	0	1	5	E	F	2	C	9	D	7	B	A	6	8	3	4
2	6	F	9	4	3	8	0	E	5	2	B	A	C	D	7	1
3	B	1	7	E	C	F	8	2	6	9	D	0	4	A	3	5
4	7	A	E	D	9	6	5	0	C	4	1	B	8	3	2	F
5	5	F	2	3	E	0	D	A	9	8	7	C	B	6	4	1
6	E	3	5	1	D	2	B	C	8	F	A	6	7	4	0	9
7	A	4	F	8	1	B	7	6	3	E	0	5	C	D	9	2
8	5	B	2	D	F	0	6	A	C	E	7	1	8	3	9	4
9	D	A	2	3	5	4	8	E	6	F	1	C	B	0	7	9
10	0	C	9	6	4	B	3	D	F	2	E	5	1	7	A	8
11	D	2	1	4	3	E	A	9	C	7	6	B	8	0	5	F
12	A	F	9	4	3	8	6	7	5	2	0	E	D	C	B	1
13	E	9	B	4	3	8	D	7	5	1	C	2	A	6	0	F
14	E	1	A	4	3	8	D	B	5	9	2	7	F	6	0	C
15	E	5	9	4	3	1	C	A	D	2	7	B	6	8	0	F
16	7	A	2	D	9	C	6	0	E	4	1	F	5	3	8	B
17	5	C	8	3	F	0	E	9	2	7	D	B	1	A	6	4
18	1	0	F	8	A	6	5	B	3	E	4	7	C	D	9	2
19	C	2	1	D	F	8	7	6	5	E	A	B	0	3	9	4
20	C	F	9	4	3	8	7	6	5	2	A	B	0	E	D	1
21	7	2	1	E	A	9	D	0	8	5	4	F	C	6	3	B
22	D	2	1	F	4	E	6	9	A	7	8	C	B	0	5	3
23	A	1	F	3	6	B	4	C	D	E	0	5	7	8	9	2

24	3	C	E	0	F	5	8	7	6	B	D	9	1	A	2	4
25	5	C	9	3	A	0	E	D	F	2	4	B	1	7	6	8
26	E	8	9	5	6	3	4	A	1	2	7	C	B	D	0	F
27	7	8	6	D	9	E	2	0	1	4	C	B	A	3	5	F
28	D	8	2	5	A	3	6	C	1	E	4	F	7	0	9	B
29	B	C	5	7	D	2	8	3	6	F	A	0	1	4	E	9
30	7	A	C	F	5	4	B	0	8	9	1	6	2	E	D	3
31	B	9	4	E	2	C	8	7	6	1	D	0	5	A	3	F
32	E	4	5	9	1	2	B	C	A	3	8	6	7	D	0	F
33	A	6	C	3	F	8	1	7	5	D	0	E	2	9	B	4
34	E	5	7	8	9	1	C	2	3	4	D	B	6	A	0	F
35	2	F	0	4	3	8	D	B	5	A	9	7	C	6	E	1
36	B	8	5	E	4	2	6	9	1	7	C	0	A	F	3	D
37	9	6	F	8	A	7	1	5	3	0	4	D	C	B	E	2
38	B	2	1	E	4	9	8	F	6	5	D	0	C	A	3	7
39	E	9	5	8	D	2	B	7	3	1	C	6	A	4	0	F
40	D	A	E	4	3	5	8	7	6	B	1	9	F	0	2	C
41	0	A	F	7	4	9	8	3	6	5	1	C	B	E	D	2
42	0	1	7	D	F	8	C	2	5	E	B	A	6	3	9	4
43	5	F	8	4	3	0	D	A	2	B	7	9	C	6	E	1
44	E	3	5	1	9	2	A	C	B	4	6	8	7	D	0	F
45	E	3	9	1	7	8	A	4	5	2	6	C	B	D	0	F
46	D	A	6	4	3	C	2	9	E	7	1	B	5	0	8	F
47	3	F	5	0	8	2	B	C	4	D	A	6	7	9	E	1
48	B	6	E	D	C	8	1	7	5	A	9	0	4	3	2	F
49	B	2	1	D	4	8	A	F	5	E	6	0	C	3	9	7
50	0	6	F	B	A	9	1	C	8	5	4	3	7	E	D	2
51	E	1	5	3	8	2	B	C	4	A	9	6	7	F	0	D
52	2	7	0	E	A	C	D	1	F	9	4	B	5	6	3	8
53	8	C	B	5	F	3	6	9	0	7	D	2	1	A	E	4
54	E	D	5	8	9	2	7	6	3	4	A	B	F	1	0	C
55	1	0	F	4	3	E	C	9	D	7	A	B	6	8	5	2
56	B	D	5	E	6	2	4	9	8	7	A	0	F	1	3	C
57	3	A	C	0	9	5	E	B	F	4	1	7	2	D	6	8
58	3	D	F	0	4	B	6	C	A	E	8	5	7	1	9	2
59	7	A	C	9	4	5	B	0	D	3	1	6	2	8	F	E
60	7	A	E	D	4	5	B	0	9	8	1	6	F	3	2	C
61	E	7	9	4	3	8	F	1	5	2	A	B	D	C	0	6
62	D	A	E	4	3	6	5	9	8	7	1	F	C	0	2	B
63	D	B	6	4	3	E	2	9	8	7	F	1	C	0	5	A
64	2	A	0	D	9	5	C	7	F	4	1	E	6	3	B	8
65	6	F	B	8	9	5	0	7	3	4	D	2	E	A	C	1
66	D	4	2	8	1	B	C	F	3	E	A	5	6	0	9	7
67	D	4	2	9	1	E	8	F	6	3	A	C	B	0	5	7
68	0	7	2	E	F	C	8	1	6	B	D	9	5	A	3	4
69	6	1	F	3	D	E	0	9	A	7	8	C	B	4	5	2

70	8	6	C	3	F	9	1	A	0	5	7	B	2	E	D	4
71	8	D	F	3	A	6	5	C	0	E	4	B	7	1	9	2
72	6	8	C	3	F	D	0	A	1	E	7	B	2	5	9	4
73	B	6	C	9	5	4	1	A	D	3	7	0	2	8	E	F
74	3	6	F	0	8	B	1	C	4	9	E	5	7	D	A	2
75	E	D	9	4	3	6	5	A	8	2	7	F	C	1	0	B
76	8	F	5	A	9	2	6	C	0	4	3	D	7	B	E	1
77	7	5	9	E	A	1	F	0	8	2	4	D	C	B	3	6
78	E	7	2	8	9	C	6	1	3	4	D	F	5	A	0	B
79	D	A	B	4	3	7	8	5	6	F	1	2	C	0	E	9
80	E	B	5	8	9	2	6	7	3	4	F	1	D	C	0	A
81	B	6	E	D	5	4	1	A	8	9	7	0	F	3	2	C
82	2	F	0	8	E	5	B	7	3	C	D	6	9	A	4	1
83	7	1	9	E	A	5	C	0	D	2	4	F	6	8	3	B
84	6	3	F	1	D	B	0	C	8	E	A	5	7	4	9	2
85	7	3	C	1	9	E	F	0	8	4	A	D	2	B	5	6
86	D	2	1	8	C	B	A	7	3	E	6	5	4	0	9	F
87	5	F	3	2	E	0	B	C	8	9	D	6	7	A	4	1
88	6	F	9	3	D	8	0	7	5	2	E	C	B	4	A	1
89	A	6	7	D	F	8	1	2	5	B	0	9	C	3	E	4
90	E	2	1	F	5	4	B	C	8	9	D	6	7	A	0	3
91	9	A	F	4	3	5	8	7	6	0	1	D	E	B	C	2
92	D	1	8	3	6	E	4	9	2	7	F	C	B	0	5	A
93	4	F	5	A	0	2	B	C	E	9	3	6	7	D	8	1
94	1	0	9	E	A	C	6	7	F	2	4	D	5	B	3	8
95	8	B	C	6	F	5	3	A	0	E	7	1	2	D	9	4
96	E	8	2	3	5	4	D	A	1	F	7	C	B	6	0	9
97	0	1	C	6	9	E	3	D	F	4	B	A	2	7	5	8
98	E	5	B	4	3	1	D	A	8	F	7	2	C	6	0	9
99	8	F	9	6	E	5	3	A	0	2	7	C	B	D	4	1
100	D	6	A	8	E	B	1	7	3	C	2	5	9	0	4	F
101	D	1	7	8	A	5	C	2	3	E	4	F	6	0	9	B
102	1	0	B	D	F	8	6	7	5	E	C	2	A	3	9	4
103	7	C	9	F	6	B	4	0	8	2	A	5	1	E	D	3
104	5	B	F	8	A	0	6	7	3	E	4	1	D	C	9	2
105	C	F	5	8	7	2	B	4	3	9	E	6	0	D	A	1
106	8	A	F	4	3	5	C	9	0	7	1	E	6	D	B	2
107	9	F	4	7	2	8	D	3	5	0	A	C	B	6	E	1
108	E	9	7	8	4	F	B	2	3	1	D	6	C	A	0	5
109	6	1	B	E	F	5	0	9	C	7	D	2	8	A	3	4
110	D	7	A	8	4	B	F	1	3	E	2	5	C	0	9	6
111	2	B	0	E	F	5	8	7	6	C	D	1	9	A	3	4
112	2	A	0	D	7	9	B	4	F	5	1	6	C	3	E	8
113	1	0	7	D	9	E	C	2	F	4	A	B	6	3	5	8
114	A	4	C	3	1	E	B	7	F	D	0	6	2	9	5	8
115	0	6	C	9	F	D	1	A	8	3	7	E	2	5	B	4

116 B 5 2 D 8 1 6 A 4 E 7 0 F 3 9 C
117 0 6 2 D F C 1 A E B 7 9 5 3 8 4
118 B C 2 3 5 4 F 9 E 7 D 0 1 A 8 6
119 B C 2 3 7 9 8 4 6 5 D 0 1 A F E
120 0 C E 7 4 B D 3 F A 9 5 1 6 2 8
121 C 1 A D 7 E B 4 F 9 2 6 0 3 5 8
122 0 A C 5 4 3 B E F D 1 6 2 9 7 8
123 0 1 B D 9 E 7 6 F 4 C 2 A 3 5 8
124 0 A F 6 E D 3 9 8 7 1 C B 5 4 2
125 0 1 F 8 7 B A 4 3 E 6 5 D C 9 2
126 B C 5 A 6 2 4 9 E 7 3 0 1 D 8 F
127 7 C 9 6 E B 3 0 A 2 8 5 1 D 4 F
128 B 3 C 1 4 8 6 D 5 E F 0 2 7 9 A
129 A C 5 7 F 2 8 3 6 9 0 E 1 D B 4
130 B C 5 F 7 2 8 4 6 9 E 0 1 D A 3
131 B 6 4 D 2 C 1 A 9 8 7 0 5 3 E F
132 C 6 F 8 7 B 1 4 3 D A 5 0 9 E 2
133 A 4 9 E 1 B 6 7 F 2 0 5 D C 3 8
134 D 6 2 8 C B 1 E 3 F A 5 4 0 7 9
135 0 B 2 E A 7 D 5 F C 4 1 9 6 3 8
136 8 F E 3 9 6 5 C 0 4 D B 7 A 2 1
137 4 6 F 8 0 B 1 E 3 9 C 5 A D 7 2
138 7 9 8 E 4 B D 0 2 1 F 5 C 6 3 A
139 D 6 2 3 8 B 1 C 4 A 9 5 7 0 F E
140 D 6 2 3 A F 1 C 9 8 4 E 7 0 B 5
141 B 1 5 E D 2 8 F 6 9 C 0 A 4 3 7
142 B 1 4 D 2 5 F A C E 7 0 8 3 9 6
143 B 4 6 D 1 F 2 A 8 E 7 0 C 3 9 5
144 1 0 C A 9 E 6 7 F 4 3 D 2 B 5 8
145 D A 2 3 8 6 5 9 4 7 1 C B 0 F E
146 7 8 2 E C B D 0 1 F A 5 4 6 3 9
147 E 3 9 1 4 F 6 A D 2 7 C B 8 0 5
148 7 1 B E A 5 D 0 C F 4 2 8 6 3 9
149 7 C 9 3 A D F 0 E 2 4 B 1 5 8 6
150 E 1 8 4 3 5 D A 2 C 7 F 9 6 0 B
151 E 1 6 8 9 5 2 B 3 4 D 7 F A 0 C
152 5 A C 7 E 0 B 3 F 9 1 6 2 D 4 8
153 7 B 2 D 9 E 6 0 C 4 F 1 8 3 5 A
154 7 1 8 D C E B 0 2 9 F 6 4 3 5 A
155 9 C 4 3 2 B D 7 F 0 E 5 1 6 A 8
156 D A 2 4 3 F 6 9 C 7 1 E 8 0 B 5
157 B C 7 9 5 4 8 2 6 3 D 0 1 A E F
158 5 A F 3 E 0 8 7 6 D 1 C B 9 4 2
159 0 A F 4 3 C E 9 8 7 1 D 5 B 6 2
160 0 D C 7 4 E B 3 F A 9 6 2 1 5 8
161 2 C 0 9 A 5 D 7 F 3 4 E 1 6 B 8

162	E	1	9	3	6	8	4	D	5	2	F	C	B	7	0	A
163	5	6	F	8	A	0	1	D	3	9	4	B	E	7	C	2
164	3	F	9	0	8	D	6	A	4	2	7	C	B	5	E	1
165	3	A	F	0	8	5	E	9	4	7	1	C	B	D	6	2
166	9	F	2	3	5	4	B	C	E	0	D	6	7	A	8	1
167	0	B	F	6	A	D	3	C	8	E	4	1	7	5	9	2
168	E	7	9	A	4	8	6	1	5	2	3	C	B	F	0	D
169	D	A	3	2	7	9	8	4	6	5	1	C	B	0	E	F
170	D	A	8	6	5	4	3	9	2	7	1	C	B	0	E	F
171	1	0	5	E	F	2	8	D	6	C	A	B	9	7	3	4
172	A	F	7	4	3	8	D	2	5	9	0	B	E	6	C	1
173	D	6	B	5	A	3	1	C	8	9	4	2	7	0	F	E
174	9	6	C	B	F	5	1	A	E	0	7	3	2	D	8	4
175	1	0	9	E	7	B	A	4	F	2	6	5	C	D	3	8
176	1	0	F	4	3	E	8	B	6	A	9	7	C	D	5	2
177	7	5	8	E	A	1	D	0	2	C	4	B	9	6	3	F
178	C	2	1	D	9	E	6	7	F	4	B	A	0	3	5	8
179	9	7	A	E	4	B	D	1	F	0	2	5	C	6	3	8
180	0	F	9	7	4	8	A	3	5	2	6	C	B	E	D	1
181	3	C	5	0	F	2	8	B	6	D	A	7	1	9	E	4
182	B	6	C	5	D	3	1	A	8	9	7	0	2	4	F	E
183	9	7	5	E	F	2	8	1	6	0	B	A	C	D	3	4
184	B	6	2	D	E	8	1	F	5	C	A	0	9	3	4	7
185	E	1	4	A	2	8	D	F	5	9	3	C	B	6	0	7
186	0	A	2	D	9	6	5	B	F	4	1	7	E	3	C	8
187	7	A	8	D	5	4	B	0	2	C	1	6	9	3	E	F
188	D	A	7	4	3	F	8	2	6	9	1	B	E	0	C	5
189	3	D	F	0	6	E	4	9	8	7	A	C	B	1	5	2
190	B	8	C	5	4	3	6	A	1	E	7	0	2	F	9	D
191	B	D	5	E	C	2	8	7	6	A	9	0	4	1	3	F
192	C	F	5	8	9	2	6	7	3	4	B	A	0	E	D	1
193	9	F	3	2	4	5	D	A	E	0	7	C	B	6	8	1
194	D	5	2	8	A	1	6	B	3	E	4	7	F	0	9	C
195	D	6	3	2	E	B	1	C	8	9	F	5	7	0	4	A
196	B	1	C	3	7	8	A	4	5	E	6	0	2	F	9	D
197	0	A	2	D	E	7	B	5	F	C	1	6	9	3	4	8
198	D	5	8	6	A	1	3	C	2	E	4	B	7	0	9	F
199	7	A	C	B	9	5	F	0	E	4	1	3	2	D	8	6
200	7	8	A	D	4	E	B	0	1	F	2	6	C	3	5	9
201	9	6	F	3	A	D	1	C	E	0	4	B	7	5	8	2
202	4	A	C	3	0	9	B	7	F	5	1	6	2	E	D	8
203	6	5	B	D	F	1	0	A	8	E	7	2	C	3	9	4
204	B	C	5	3	E	2	8	7	6	D	F	0	1	9	4	A
205	1	0	F	8	D	B	6	7	3	E	C	5	A	4	9	2
206	7	A	C	F	9	D	6	0	B	4	1	8	2	5	E	3
207	7	C	2	3	A	9	D	0	B	5	4	8	1	6	F	E

208 7 C 2 3 E B D 0 9 8 F 5 1 6 4 A
209 3 C E 0 A 7 D 5 F 9 4 B 1 6 2 8
210 5 A F 4 3 0 8 D 6 B 1 9 C 7 E 2
211 C 1 6 D F 5 2 A B E 7 8 0 3 9 4
212 B C 5 F 4 2 6 9 A 7 8 0 1 E D 3
213 7 4 9 E 1 B C 0 8 2 A 5 6 F 3 D
214 0 F 5 B 9 2 A C 8 4 6 3 7 E D 1
215 2 F 0 8 9 6 5 B 3 4 D 7 C A E 1
216 6 8 F 4 3 E 0 9 1 7 B A C D 5 2
217 5 F 8 B 9 0 6 C 2 4 D 3 7 A E 1
218 E 1 5 3 9 2 F C A 4 8 D 7 B 0 6
219 0 F 5 9 4 2 B C D 3 E 6 7 8 A 1
220 7 C 9 B A F 6 0 D 2 4 3 1 8 E 5
221 3 D C 0 F 8 6 7 5 E B A 2 1 9 4
222 E D 5 8 4 2 B F 3 A 9 6 C 1 0 7
223 6 A C 3 9 D 0 E F 4 1 B 2 5 7 8
224 2 6 0 D F 9 1 A B 5 7 8 C 3 E 4
225 1 0 5 E F 2 A 9 B 7 6 8 C D 3 4
226 7 2 1 D 9 E A 0 8 4 6 F C 3 5 B
227 C 2 1 E A 5 D 7 F B 4 9 0 6 3 8
228 7 C 9 A 4 B 6 0 E 2 3 5 1 F 8 D
229 B 6 8 D 4 5 1 A 2 C 7 0 9 3 F E
230 B C 3 2 4 5 8 E 6 F D 0 1 A 7 9
231 D 8 2 4 3 E 6 9 1 7 C F A 0 5 B
232 0 F 2 8 9 7 C 5 3 4 D E 6 A B 1
233 4 D F 3 0 E 8 7 6 A 9 C B 1 5 2
234 A 1 7 E C B D 2 F 9 0 5 4 6 3 8
235 E 1 4 8 2 C B F 3 9 D 6 5 A 0 7
236 D 6 4 A 2 B 1 C 9 8 3 5 7 0 E F
237 7 B C 6 9 E 3 0 A 4 8 1 2 D 5 F
238 D 7 6 8 A C 2 1 3 E 4 B 5 0 9 F
239 8 6 F 9 A 5 1 C 0 3 4 E 7 D B 2
240 7 1 C 3 9 E A 0 B 4 6 8 2 F 5 D
241 6 C 9 B A 5 0 E F 2 4 3 1 D 7 8
242 6 8 5 E F 2 0 9 1 7 A B D C 3 4
243 D 9 4 A 2 E 8 7 6 1 3 C B 0 5 F
244 7 A C 3 9 F E 0 D 4 1 B 2 8 6 5
245 E 1 9 4 3 5 F A C 2 7 D 8 B 0 6
246 7 1 C 3 D E B 0 A F 8 6 2 4 5 9
247 E 4 3 2 1 F D A 8 9 7 C B 6 0 5
248 0 F 9 4 3 D C A 8 2 7 E 6 5 B 1
249 0 F 9 5 D 3 E A 8 2 7 C B 4 6 1
250 A 3 F 1 4 E 6 9 D 7 0 C B 8 5 2
251 0 F 5 8 4 2 B E 3 D C 6 A 9 7 1
252 3 6 C 0 F 8 1 B 5 9 E 7 2 D A 4
253 E 2 1 8 C 9 B 7 3 5 D 6 4 A 0 F

254 D 1 B 4 3 E 8 F 6 9 C 2 A 0 5 7
255 D 6 3 2 A 9 1 C B 5 4 8 7 0 E F
256 3 D C 0 9 E 7 6 F 4 A B 2 1 5 8
257 8 A F 5 D 3 6 9 0 7 1 C B 4 E 2
258 7 9 2 D 8 E B 0 4 1 A 6 F 3 5 C
259 B 4 A D 1 8 C 7 5 E 2 0 6 3 9 F
260 0 D C B F 6 5 A 8 E 7 3 2 1 9 4
261 7 C 4 A 2 B D 0 8 9 3 5 1 6 F E
262 0 C 2 5 A 3 D E F B 4 9 1 6 7 8
263 0 C 2 9 F 7 8 5 6 3 D E 1 A B 4
264 0 F 2 4 3 8 D E 5 B C 9 A 6 7 1
265 0 F 2 4 3 9 D A B 5 7 8 E 6 C 1
266 C 5 2 E F 1 6 9 B 7 D 8 0 A 3 4
267 9 6 C 7 F 8 1 3 5 0 A D 2 B E 4
268 5 B 6 E F 0 2 9 8 7 D 1 C A 3 4
269 0 1 F 4 3 E 8 D 6 C B A 9 7 5 2
270 0 1 F 4 3 E A 9 B 7 6 8 D C 5 2
271 E 5 2 F 9 1 6 C B 4 D 8 7 A 0 3
272 7 C 3 2 A F D 0 8 9 4 E 1 6 B 5
273 B 9 5 E 4 2 8 D 6 1 F 0 C 7 3 A
274 B 4 2 E 1 F 6 9 C 7 D 0 8 A 3 5
275 C A F 4 3 7 8 5 6 9 1 B 0 E D 2
276 C 9 2 E 7 B D 4 F 1 A 5 0 6 3 8
277 E 8 6 5 9 3 2 C 1 4 D B 7 A 0 F
278 7 8 9 E 6 B 4 0 1 2 C 5 A D 3 F
279 D 6 7 8 A F 1 2 3 B 4 9 C 0 E 5
280 4 7 C A 0 E B 1 F 9 3 6 2 D 5 8
281 7 C 3 2 8 B D 0 4 A 9 5 1 6 E F
282 4 F 9 6 0 8 3 D 5 2 A C B 7 E 1
283 D 6 E 8 4 B 1 F 3 A 9 5 C 0 2 7
284 E 4 2 3 1 F B C 9 8 D 6 7 A 0 5
285 C A F 4 3 D 6 9 B 7 1 8 0 5 E 2
286 0 1 C A F 8 7 6 5 E 3 D 2 B 9 4
287 6 A B D 9 7 0 5 F 4 1 2 C 3 E 8
288 1 0 C 6 F 8 3 D 5 E A B 2 7 9 4
289 6 F 5 8 9 2 0 E 3 4 A B D C 7 1
290 B 1 6 E 8 5 2 9 4 7 D 0 F A 3 C
291 0 F B 5 9 3 E C 8 4 D 2 7 A 6 1
292 0 F 2 8 7 9 B 4 3 5 D 6 E A C 1
293 A C 5 B F 2 6 9 D 7 0 3 1 8 E 4
294 A 9 7 D 4 E B 2 F 1 0 6 C 3 5 8
295 9 7 F 4 3 E 8 1 6 0 A B D C 5 2
296 B 5 4 E 2 1 F 9 8 7 D 0 C A 3 6
297 B 6 C F 7 8 1 4 5 D A 0 2 9 E 3
298 C F 9 4 3 5 E A B 2 7 8 0 D 6 1
299 4 6 F 9 0 B 1 C D 3 A 5 7 8 E 2

300 4 F 5 8 0 2 B D 3 C A 6 9 7 E 1
301 2 F 0 4 3 C D A E 9 7 B 5 6 8 1
302 6 C 9 7 D B 0 3 F 2 A 5 1 4 E 8
303 E D 9 4 3 8 6 7 5 2 B A F 1 0 C
304 E 2 1 4 3 9 D A C 5 7 B 8 6 0 F
305 3 C 9 0 A D 6 B F 2 4 7 1 5 E 8
306 D 9 2 4 3 E 8 B 6 1 A 7 F 0 5 C
307 D 1 6 F A 5 2 C B E 4 8 7 0 9 3
308 B 1 C 3 6 F 4 A D E 7 0 2 8 9 5
309 D A 3 2 4 5 F 9 E 7 1 C B 0 8 6
310 D A 7 9 4 5 8 2 6 3 1 C B 0 F E
311 D 1 A F 7 E 8 4 6 9 2 C B 0 5 3
312 7 1 A E 8 B D 0 4 9 2 5 F 6 3 C
313 E B 9 4 3 8 7 6 5 2 F 1 C D 0 A
314 B C 3 2 8 6 5 9 4 7 D 0 1 A E F
315 2 6 0 D F 8 1 E 5 9 C B A 3 7 4
316 7 D 9 E A 6 5 0 C 2 4 B 8 1 3 F
317 3 F E 0 4 5 B C 9 8 D 6 7 A 2 1
318 E 9 2 F 7 8 D 4 5 1 A C B 6 0 3
319 0 6 F 8 4 B 1 D 3 C E 5 9 7 A 2
320 5 B 9 E A 0 7 6 F 2 4 1 C D 3 8
321 8 F 9 4 3 C 6 A 0 2 7 D 5 B E 1
322 0 C 5 A F 2 E 9 8 7 3 D 1 B 6 4
323 0 C E B F 6 5 9 8 7 D 3 1 A 2 4
324 0 1 9 E A 6 5 B F 2 4 7 D C 3 8
325 E 1 8 6 9 5 3 C 2 4 D F 7 A 0 B
326 A 4 F 7 1 E 8 3 6 9 0 C B D 5 2
327 4 C 9 3 0 B A 7 F 2 6 5 1 E D 8
328 3 F E 0 5 4 D A 8 9 7 C B 6 2 1
329 4 F E 3 0 8 D 7 5 A 9 C B 6 2 1
330 D 3 4 1 2 E F 9 8 7 A C B 0 5 6
331 E 7 5 8 9 2 F 1 3 4 B A C D 0 6
332 4 C 7 9 0 B D 2 F 3 A 5 1 6 E 8
333 D 6 E 8 A 7 1 5 3 9 4 B F 0 2 C
334 C 6 F 8 A 5 1 7 3 B 4 9 0 E D 2
335 7 A 4 D 2 C B 0 8 9 1 6 5 3 F E
336 4 A F 5 0 3 8 E 6 9 1 C B D 7 2
337 E B 5 6 9 2 3 C 8 4 A 1 7 F 0 D
338 9 7 2 D C E B 1 F 0 A 6 4 3 5 8
339 0 6 F A 4 B 1 C E D 3 5 7 9 8 2
340 9 F 4 8 2 7 B 5 3 0 D 6 C A E 1
341 B 6 C 7 E 8 1 3 5 9 F 0 2 D 4 A
342 7 C B 5 A 3 D 0 9 8 4 2 1 6 E F
343 A F 5 8 9 2 7 6 3 4 0 E C D B 1
344 5 6 8 D F 0 1 A 2 9 7 B E 3 C 4
345 D 2 1 F 6 B 4 C 8 E A 5 7 0 9 3

346 6 8 F B A 5 0 C 1 E 4 3 7 D 9 2
347 0 F 7 9 4 8 D 2 5 3 E C B 6 A 1
348 0 1 F 8 A C 7 6 3 E 4 D 5 B 9 2
349 B 6 C F 4 5 1 A 9 8 7 0 2 E D 3
350 B C 8 6 4 5 3 9 2 7 D 0 1 A F E
351 0 7 F A 4 E 8 1 6 D 3 C B 9 5 2
352 D 1 4 3 2 B F C A E 8 5 7 0 9 6
353 B 7 C A 6 8 4 1 5 E 3 0 2 D 9 F
354 2 C 0 5 F 3 8 E 6 9 D B 1 A 7 4
355 D 6 B 8 A 5 1 7 3 F 4 2 E 0 C 9
356 E 2 1 F 4 5 D A 9 8 7 C B 6 0 3
357 B 7 2 D C 8 F 1 5 E A 0 4 3 9 6
358 7 4 C 9 1 E B 0 8 3 A 6 2 F 5 D
359 E B 2 4 3 8 D F 5 C A 1 9 6 0 7
360 E 1 5 8 C 2 B D 3 9 F 6 4 7 0 A
361 0 1 5 E F 2 8 B 6 A 9 7 D C 3 4
362 7 A 6 D 9 F 2 0 8 4 1 E C 3 B 5
363 E 4 A 9 1 8 D 7 5 3 2 C B 6 0 F
364 B 3 C 1 8 6 5 A 4 E 7 0 2 D 9 F
365 B 4 5 E 1 2 C 9 A 7 8 0 6 D 3 F
366 B C 5 6 E 2 3 9 8 7 A 0 1 F 4 D
367 A F 5 3 9 2 E C D 4 0 B 7 8 6 1
368 D B A 4 3 E 8 7 6 C 2 1 9 0 5 F
369 E 1 9 3 8 6 5 A 4 2 7 C B F 0 D
370 D 3 8 1 4 B 6 C 2 E F 5 7 0 9 A
371 9 C 5 3 F 2 8 7 6 0 E D 1 B A 4
372 7 C 9 F A 5 E 0 B 2 4 8 1 D 6 3
373 B 6 A D 4 8 1 E 5 F 2 0 C 3 7 9
374 8 C 5 3 F 2 A 9 0 7 6 B 1 E D 4
375 0 1 9 E D B 7 6 F 2 C 5 A 4 3 8
376 7 3 C 1 8 E B 0 4 A 9 6 2 D 5 F
377 C 2 1 E F 7 8 5 6 9 D B 0 A 3 4
378 7 A C 5 D 3 B 0 9 8 1 6 2 4 E F
379 E 8 3 2 4 5 B C 1 F D 6 7 A 0 9
380 0 6 2 D F 8 1 B 5 A 9 7 E 3 C 4
381 5 A C B 9 0 6 D F 4 1 3 2 7 E 8
382 9 A 4 D 2 5 B 7 F 0 1 6 E 3 C 8
383 7 D 9 E 4 B 6 0 A 2 8 5 F 1 3 C
384 B 6 C 3 D 8 1 7 5 F E 0 2 4 A 9

ÖZGEÇMİŞ

Pınar SAVAŞTÜRK, Lise öğrenimini Kırklareli Remzi Yapıcı Anadolu Öğretmen Lisesi'nde tamamladıktan sonra 2015 yılında Dokuz Eylül Üniversitesi Bilgisayar Mühendisliği (İngilizce) Bölümü'nü kazandı. Hazırlık sınıfını ve lisans öğrenimini tamamladıktan sonra 2020 yılında mezun oldu. 2022 yılında Kırklareli Üniversitesi Yazılım Mühendisliği Bölümü'nde Araştırma Görevlisi olarak çalışmaya başladı. Aynı yıl Trakya Üniversitesi Bilgisayar Mühendisliği Bölümü'nde Yüksek Lisans çalışmalarına başladı. Halihazırda Kırklareli Üniversitesi Yazılım Mühendisliği Bölümü'nde Araştırma Görevlisi olarak görevine devam etmektedir.