Araştırma Makalesi
Adıyaman Üniversitesi Mühendislik Bilimleri Dergisi
21 (2023) 242-251

KRİPTOGRAFİK YAPILAR İÇİN SEÇMELİ KAOTİK PERMÜTASYONLAR TABANLI YENİ BİR S-BOX ÜRETME ALGORİTMASI

Fırat ARTUĞER[1*]

[1]Munzur Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, Tunceli, 62000, Türkiye
Geliş Tarihi/Received Date: 28.07.2023 Kabul Tarihi/Accepted Date: 25.12.2023 DOI: 10.54365/adyumbd.1334213

ÖZET

Kriptografi, güvenli olmayan ağlar üzerinden iletilen verilerin korunması için algoritmalar tasarlamayı amaçlamaktadır. Bu algoritmalar, verileri şifreler ve üçüncü kişiler tarafından ele geçirilse bile, veriyi anlaşılmaz hale getirir. S-box, algoritmada karıştırma adı verilen temel gereksinimlerden birini sağlamaktadır. Lineer olmama değeri yüksek bir s-box yapısı, çeşitli saldırılarına karşı güvenliği oldukça arttırmaktadır. Bu nedenle, bir şifreleme algoritmasında s-box oldukça hayati bir önem taşımaktadır. Literatüre bakıldığında kaos tabanlı s-box yapıları sıklıkla kullanılmaktadır. Ancak kaos ile üretilen s-box 'ların lineer olmama değeri düşüktür. Bu makalede, bu problemin üstesinden gelmek için yeni bir algoritma önerilmiştir. Önerilen yöntemde öncelikle herhangi bir kaotik harita yardımıyla bir s-box üretilir. Daha sonra bu s-box 'da yine aynı kaotik harita ile seçilmiş iki elemanın yeri değiştirilerek lineer olmama değeri kontrol edilir. Bu değer arttığında s-box güncellenir. Bu şekilde sadece 100 yineleme sonucunda lineer olmama değeri 107.5 olan bir s-box üretilmiştir. Bu değer literatürdeki birçok çalışmayı geride bırakmaktadır.

Anahtar Kelimeler: *Yer değiştirme kutusu (s-box), Kaos, Kaotik haritalar*

A NEW S-BOX GENERATION ALGORİTHM BASED ON SELECTİVE CHAOTİC PERMUTATİONS FOR CRYPTOGRAPHİC STRUCTURES

ABSTRACT

Cryptography aims to design algorithms for the protection of data transmitted over unsecured networks. These algorithms encrypt the data and render it incomprehensible even if it is intercepted by third parties. S-box satisfies one of the basic requirements in the algorithm, called confusion. An s-box structure with a high nonlinearity value greatly increases the security against various attacks. Therefore, s-box is of vital importance in an encryption algorithm. When we look at the literature, chaos-based s-box structures are frequently used. However, the non-linearity value of s-boxes produced with chaos is low. In this article, a new algorithm is proposed to overcome this problem In the proposed method, an s-box is first generated with the help of any chaotic map. Then, in this s-box, the nonlinearity value is checked by changing the location of the two selected elements with the same chaotic map. When this value increases, the s-box is updated. In this way, an s-box with a nonlinearity value of 107.5 was produced after only 100 iterations. This value surpasses many studies in the literature.

Keywords: *Substitution box (s-box), Chaos, Chaotic maps*

1. Giriş

Kriptografi, geçmişten günümüze kadar çeşitli önemli verileri korumak için uygulanan yaklaşımların başında gelmektedir [1]. Bu bilimin alt dallarından biri olan şifreleme, gizliliği sağlayan en önemli yapıdır. Şifreleme algoritmaları, simetrik ve asimetrik olmak üzere iki şekilde ele

* e-posta[1] : firatartuger@munzur.edu.tr ORCID ID: https://orcid.org/0000-0002-4096-0458 (Sorumlu Yazar)

alınmaktadır. Asimetrik algoritmalar yavaş olduğu için genellikle anahtar değişimi ve sayısal imza gibi uygulamalarda kullanılmaktadır. Şifreleme aşaması için simetrik algoritmalar kullanılmaktadır. Simetrik algoritmalar ikiye ayrılır. İlki akış şifrelemedir. Akış şifrelemedeki temel felsefe bitleri tek tek şifrelemektir. Bu teknikte verinin boyutu arttıkça uygulaması olanaksız hale gelmektedir [1]. Bir diğer yaklaşım ise blok şifreleme yapısıdır. Burada veri bloklara bölünür ve her blok kendi içinde şifrelenir. Günümüzde kullanılan veri şifreleme standardı olan AES algoritması [2] ve hala sıklıkla kullanılan DES algoritması [3], blok şifreleme algoritmalarıdır. Günümüzün sürekli gelişen koşullarıyla birlikte özellikle uygulamaların boyutlarına göre yeni şifreleme algoritmalarına olan ihtiyaç kaçınılmazdır. Bu ihtiyacı karşılamak için yeni ve etkili blok şifreleme algoritmaları geliştirilmelidir. Bir blok şifreleme algoritmasının en önemli birimlerinden bir tanesi s-box yapılarıdır. Yani blok şifreleme algoritmalarının güvenliği çoğunlukla kullanılan s-box yapısının gücüne bağlıdır. Bundan dolayı, doğrusal kriptanaliz saldırılarına karşı dirençli bir şifreleme algoritması tasarlamak için yüksek lineer olmama özelliklerine sahip olan s-box yapılarına ihtiyaç duyulmaktadır [4].

Bir s-box basitçe, matematiksel olarak bir değerin başka bir değerle değiştirildiği bir dönüşümdür [5]. Bu dönüşüm sayesinde algoritmalar oldukça güçlü hale gelmektedir. Ancak, algoritmanın güçlü olabilmesi için s-box yapısının da kriptografik olarak güçlü olması gerekmektedir. Bir s-box ‘ın güçlü olabilmesi için yüksek lineer olmama değerine sahip olması gerekmektedir. Çünkü, blok şifreleme algoritmalarında genellikle lineer olmayan tek yapı s-box ‘dır. Bu yüzden lineer olmama değeri yüksek olmalıdır. Bu tür s-box ‘lar üretmek oldukça zordur. Çünkü 8 bit bir s-box yapısında 256 değer bulunmaktadır. Bunun anlamı, optimum bir s-box elde etmek için arama uzayının 256! büyüklüğünde olmasıdır. Bu tür problemler NP-hard problem olarak adlandırılmaktadır. Bu problemi çözmek için geçmişten günümüze kadar farklı yaklaşımlar üzerinde durulmuştur. Bu yaklaşımlar temelde 3 sınıfta toplanmaktadır. Bunlar optimizasyon tabanlı, matematiksel dönüşüm tabanlı ve kaos tabanlı yaklaşımlardır. Bu yaklaşımların birbirlerine göre avantaj ve dezavantajları olduğu için yeni yöntemler geliştirilmeye devam etmektedir.

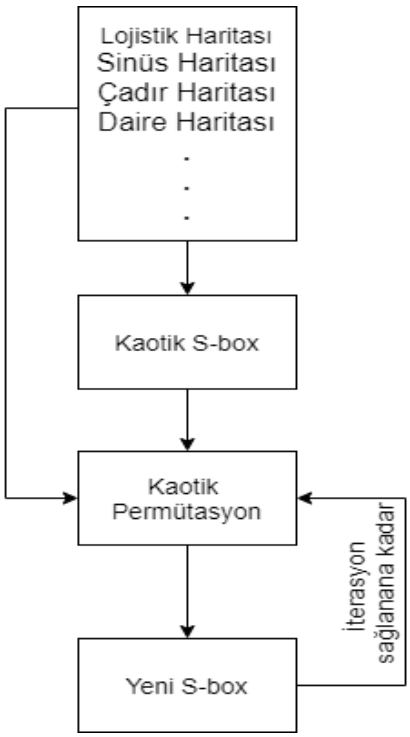
Optimizasyon temelli yaklaşımların avantajı, çoğu zaman kriptografik olarak güçlü s-box yapıları elde edilebilmesidir. Ancak, bu yaklaşımda hesaplama maliyeti oldukça fazladır. En önemli dezavantajının bu olduğu söylenebilir. Geçmişten günümüze kadar s-box üretiminde; parçacık sürüsü optimizasyonu [6], genetik algoritma [5], ateş böceği algoritması [7], kesirli sıralı hopfield sinir ağı algoritması [8], sinüs kosinüs optimizasyon algoritması [9], öğretme-öğrenme optimizasyonu [10], bakteriyel yiyecek arama optimizasyonu [11], karınca kolonisi optimizasyonu [12], tavlama algoritması [13], tiki-taka algoritması [14], uyarlanabilir ajan kahramanları ve korkaklar optimizasyonu [15], guguk kuşu arama algoritması [16] teknikleri kullanılmıştır. Bu optimizasyon teknikleri kullanılırken, genellikle bir kaotik harita yardımıyla başlangıç için bir s-box üretilir, daha sonra bu s-box optimizasyon algoritması ile daha güçlü hale getirilir. Bir diğer yaklaşım matematiksel dönüşüm tabanlı yaklaşımlardır. Bu yaklaşımlarda genellikle cebirsel dönüşümler kullanılmaktadır. Bu felsefe ile elde edilen s-box yapıları genellikle kriptografik olarak güçlü özelliklere sahiptirler. Ancak bu s-box ‘lar çeşitli cebirsel [17] ve uygulama [18] saldırılara karşı dayanıksız olabilmektedirler. Ayrıca hesaplama maliyetleri de oldukça yüksek ve karmaşık bir yapıya sahiptirler. Bu sebepler, bu yöntemlerle elde edilen s-box yapılarının en önemli dezavantajıdır. Son yıllarda; boole fonksiyonları tabanlı [19], dönme matrisleri tabanlı [20], mobius grubuna ve sonlu alana dayalı [21], grup teorik ve grafiksel tabanlı [22], karmaşık davranış ve cebirsel yapı tabanlı [23], simetrik bir grup kullanılarak [24], modüler bir grubun eylemi kullanılarak [25], bir grup teorisine dayalı [26] yöntemler kullanılarak matematiksel dönüşüm tabanlı s-box yapıları geliştirilmiştir. S-box üretmek için, son olarak kaos tabanlı yaklaşımlar kullanılmaktadır. Bu yaklaşımlarda genellikle kaotik haritalar kullanılır. Kaotik haritalar sayesinde s-box tablosu rastgele bir şekilde doldurulur. Sadece kaos ile elde edilen bu s-box yapılarının elde edilmesi oldukça hızlı ve kolaydır. En önemli avantajının bu olduğu söylenebilir. Ancak, bu s-box ‘lar kriptografik olarak genellikle kötü özelliklere sahiptirler. Özellikle lineer olmama değerleri çok düşük kalabilmektedir. En büyük dezavantajlarının bu olduğu söylenebilir. Çünkü düşük lineer olmama değeri çeşitli saldırılara karşı zafiyetler yaratmaktadır. Çok düşük lineer olmama değerine sahip s-box yapılarının performansını arttırmak için zig-zag tarama yöntemi [27] önerilmiştir. Bu yöntemde elde edilen kaotik s-box, zig-zag şekilde taranarak s-box ‘ların lineer olmama değeri arttırılmıştır. Bir diğer

yaklaşımda [28] kaotik bir s-box yapısının satır ve sütunları yer değiştirilerek performansı arttırılmıştır. Buradaki yer değiştirme işleminde DES algoritmasında kullanılan s-box yapıları kullanılmıştır. DES s-box tabloları birleştirilerek yer değiştirecek olan satır ve sütunlar bu tablodan seçilmiştir. Bu sayede lineer olmama değeri arttırılmıştır. Kaos tabanlı yaklaşımlarla s-box üretmek için çadır harita [29], baker harita [30], geliştirilmiş tek boyutlu ayrık bir kaotik harita [31], tam sayıların çarpımını temel alan yeni bir ayrık zamanlı kaotik harita [32], kaotik labirent rene Thomas sistemi [33], kaotik sinüs harita [34], kesirli Lorenz-Duffing sistemi [35], lojistik harita [36], kaotik kısmi diferansiyel denklem [37], kaotik ölçekli Zhongtang sistemi [38], hiperkaotik sistem [39], kaotik Lorenz sistemi [40], kesirli kaotik sistem [41], kesirli sıralı kaotik Chen sistemi [42] ve daha birçok kaotik sistem kullanılmıştır.

2. Önerilen Yöntem

Önerilen yöntemde öncelikle kaotik bir harita yardımıyla giriş için kullanılacak lineer olmama değeri genellikle düşük olan bir s-box üretilir. Bu giriş s-box 'ını elde etmek için kullanılan algoritmanın sözde kodu tablo 1 'de verilmektedir. Bunun için öncelikle kaotik bir haritanın başlangıç ve durum parametreleri belirlenir. Daha sonra bir çıkış değeri hesaplanır ve mod256 işlemi ile [0,256] aralığında bir değere dönüştürülür. Bu değer s-box 'da yoksa tabloya eklenir, varsa eklenmez. Çünkü s-box yapısının bijektif olması gerekmektedir. Yani 0 'dan 256 'ya kadar her değerin bir kez kullanılması gerekmektedir. Bu şekilde tablo dolana kadar devam edilmektedir. Sadece bu yaklaşım ile oluşturulan s-box yapılarında lineer olmama değeri en fazla 106.75 olarak hesaplanmıştır [43]. Böylece çeşitli güvenlik zafiyetleri ortaya çıkabilmektedir. Daha sonra, elde edilen bu zayıf s-box yapısında kaotik bir harita ile seçilmiş iki eleman yer değiştirilmektedir. Bu yer değiştirme sonucunda lineer olmama değeri artarsa s-box güncellenmektedir. Bu şekilde s-box 'ın lineer olmama değeri arttırılmaktadır. Önerilen yöntemin sistem modeli şekil 1 'de verilmiştir. Şekil 1 'de verilmiş kaotik haritalar arttırılabilir. Bu çalışmada s-box oluşturmak ve yer değiştirecek elemanları elde etmek için lojistik harita kullanılmıştır. Lojistik haritanın matematiksel modeli denklem 1 'de verilmiştir.

$$x_{n+1} = ax_n(1 - x_n)\ , x_n\ \in [0,1]\ , a \in [3.5, 4] \quad (1)$$



Şekil 1. Önerilen yöntemin sistem modeli

Tablo 1 ‘de, bu kaotik s-box ‘ların lineer olmama değerini hızlı bir şekilde arttırmak için önerilen algoritma verilmektedir. Önerilen yaklaşımda, herhangi bir kaotik harita ile iki değer üretilmektedir. Bu değerler mod256 işlemi ile [0,256] aralığındaki değerlere dönüştürülmektedir. Daha sonra elde edilen bu iki değer yer değiştirilir ve yeni lineer olmama değeri hesaplanır. Yeni lineer olmama değeri eski lineer olmama değerinden büyük ise s-box güncellenir. Bu şekilde yineleme sayısı tamamlanana kadar devam edilir. Bu sayede lineer olmama değeri hızlı bir şekilde arttırılmış olur. Bu çalışmada sadece 100 yinelemede lineer olmama değeri 107.5 olan bir s-box elde edilmiştir.

Tablo 1. Önerilen yaklaşımın sözde kodu

```
SboxÜretme ()
Kaotik bir harita seçilir ve haritanın giriş
parametreleri girilir
begin
KaotikSbox= []
i=0
while (i < 256)
çıktı= kaotik haritanın matematiksel modeline göre
bir çıktı değeri hesaplanır
değer= (çıktı*10000000) mod 256
if ( !içeriyor (KaotikSbox, değer) )
KaotikSbox[i]= değer
i++
end if
end while
```

```
KaotikSboxİyileştirme ()
İyileştirilmişKaotikSbox = []
Eski_LineerOlmama= Kaotik s-box yapısının lineer
olmama değeri
for (int i=0; i<100; i++)
a= Kaotik harita ile seçilmiş değer
b= Kaotik harita ile seçilmiş değer
Yer_Değiştir (KaotikSbox[a], KaotikSbox[b]
Yeni_LineerOlmama = Hesapla_LineerOlmama
(İyileştirilmişKaotikSbox)
if (Yeni_LineerOlmama > Eski_LineerOlmama)
Güncelle Sbox
end if
else
KaotikSbox= İyileştirilmişKaotikSbox
end else
end for
end
```

3. Analiz Sonuçları

Bir s-box ‘ı analiz etmek için kullanılan çeşitli değerlendirme kriterleri mevcuttur. Bu çalışmada elde edilen s-box yapısının performansını değerlendirmek için, eşit olası giriş-çıkış XOR dağılımı, katı çığ kriteri (SAC), çıkış bitlerinden bağımsızlık kriteri (BIC) ve lineer olmama metrikleri kullanılmıştır. Bu metrikler aşağıda kısaca açıklanmıştır.

3.1. Giriş-Çıkış XOR Dağılımı

XOR dağılımında, çıkışta elde edilen XOR değerleriyle, girişteki XOR değerlerinin aynı olasılığa sahip olması istenmektedir [44]. Diferansiyel saldırılara karşı direnci ölçmek için kullanılan bir kriterdir. Saldırı başarısını istatistiksel olarak değerlendirdiği için tabloda hesaplanan en yüksek değerin olabildiğince küçük olması istenmektedir. Burada ideal değer AES algoritmasında olduğu gibi 4 olmalıdır. Önerilen algoritma ile elde edilen s-box yapısının XOR dağılım değerleri Tablo 2 'de verilmektedir. Bu değerlere bakıldığında en yüksek değer 12 olarak görülmektedir. Bu değer iyileştirilebilecek bir değerdir. Literatürdeki birçok çalışmanın bu noktada eksik olduğu söylenebilir. Çünkü bu çalışmada olduğu gibi çoğu çalışma lineer olmama değerini arttırmak için algoritmalar geliştirmektedir. Ayrıca bu noktadaki eksiklik gelecek çalışmalar için bir motivasyon olabilir.

Tablo 2. Önerilen s-box yapısı için XOR dağılımı değerleri

8	6	10	6	8	6	6	10	10	8	6	6	8	6	6	8
8	12	8	6	6	6	6	6	8	10	10	8	8	6	8	6
6	6	6	6	6	6	8	6	6	8	6	6	6	8	10	6
6	6	6	6	6	8	6	6	8	6	6	6	6	6	8	6
8	10	6	6	6	6	6	6	8	6	6	10	8	6	6	8
8	8	6	6	8	6	6	8	6	4	8	8	6	6	6	6
8	6	8	8	6	6	6	8	8	8	8	6	8	8	6	6
6	6	6	8	8	6	8	10	8	8	8	6	8	8	6	6
6	8	6	8	8	6	6	8	8	8	6	6	8	6	6	8
6	6	10	8	6	8	8	6	10	6	8	8	10	6	6	8
6	6	6	6	8	6	10	6	8	8	8	6	6	6	8	6
6	6	8	6	6	10	8	6	8	8	6	6	8	8	6	10
6	8	10	6	6	6	6	6	6	6	6	6	4	8	6	8
6	8	6	6	6	6	8	6	6	6	8	6	6	6	6	6
6	6	6	6	6	10	6	6	6	6	8	8	6	8	8	6
6	6	6	6	6	6	6	8	6	8	8	6	8	8	8	0

Tablo 3. Önerilen s-box yapısı için SAC değerleri

0,5469	0,4531	0,5	0,5	0,4688	0,4531	0,5	0,4688
0,4688	0,4844	0,5	0,5156	0,4844	0,4531	0,4531	0,5469
0,5156	0,5469	0,5	0,4531	0,5625	0,5	0,5938	0,5
0,5312	0,5156	0,5	0,5312	0,4219	0,4844	0,5156	0,5312
0,4688	0,5625	0,5	0,5312	0,5781	0,4844	0,4375	0,5
0,4531	0,4844	0,5938	0,5	0,5469	0,5469	0,5312	0,5781
0,5469	0,4688	0,4844	0,5312	0,5156	0,4844	0,4531	0,4375
0,5	0,5	0,5469	0,5156	0,5	0,5156	0,4844	0,5469

3.2. Katı Çığ Kriteri (SAC - Strict Avalanche Criterion)

SAC, girişte meydana gelebilecek bir değişikliğin, çıkışta meydana getireceği olasılığı hesaplamaktadır [45]. Kriptografi, girişte meydana gelen bir bitlik bir değişikliğin, çıkıştaki bitlerin yarısın değişmesi gerektiğini söylemektedir. Yani girişteki bir bitlik değişiklik çıkıştaki çok sayıda ya da az sayıda biti etkilerse, bu durum saldırganlar için ipuçları sağlar. Bu yüzden SAC oldukça önemli bir metriktir. Yani SAC değerinin 0,5 veya buna yakın bir değer olması istenmektedir. Önerilen

algoritma ile elde edilen kaotik s-box yapısının SAC değerleri Tablo 3 ‘de verilmektedir. Bu değerlerin ortalamasına bakıldığında 0,5051 değeri ile bu kriterin sağlandığı görülmektedir.

3.3. Bitlerinden Bağımsızlık Kriteri (BIC - Bits Independence Criterion)

BIC, bitlerin birbirlerinden bağımsız olarak değişmesi gerektiğini belirtmektedir [45]. Bu kriterde hem lineer olmama değeri hesaplanmaktadır. Bu değerin olabildiğince yüksek olması istenir. Hem de SAC değerini sağlaması gerekmektedir. BIC metriği için önerilen s-box yapısında SAC değerleri tablo 4 ‘de, lineer olmama değerleri ise tablo 5 ‘de verilmektedir. Burada SAC değerinin ortalama 0.4988 değeri ile 0.5 ‘e çok yakın olduğu için bu kriterin sağlandığı söylenebilir. Lineer olmama değerinin ise ortalama 103.57 olduğu hesaplanmıştır. Bu değer de yine XOR dağılımında olduğu gibi geliştirilebilecek bir sonuçtur. Burada ideal değer 112 ‘dir. Ancak çok az çalışma bu değere ulaşabilmiştir. Bu değerin geliştirilmesi de yine gelecek çalışmalar için önemli bir motivasyon kaynağıdır.

Tablo 4. Önerilen s-box yapısı için BIC-SAC değerleri

0	0,5117	0,4688	0,5078	0,5098	0,5215	0,498	0,5059
0,5117	0	0,4746	0,5039	0,4961	0,4844	0,5	0,4941
0,4688	0,4746	0	0,4961	0,4844	0,5215	0,4922	0,5156
0,5078	0,5039	0,4961	0	0,5137	0,5059	0,5176	0,4707
0,5098	0,4961	0,4844	0,5137	0	0,4766	0,4961	0,5195
0,5215	0,4844	0,5215	0,5059	0,4766	0	0,5195	0,4922
0,498	0,5	0,4922	0,5176	0,4961	0,5195	0	0,4688
0,5059	0,4941	0,5156	0,4707	0,5195	0,4922	0,4688	0

Tablo 5. Önerilen s-box yapısı için BIC-Lineer olmama değerleri

0	106	102	106	100	106	106	106
106	0	106	102	104	108	106	98
102	106	0	106	100	104	106	92
106	102	106	0	108	100	110	104
100	104	100	108	0	100	104	104
106	108	104	100	100	0	102	104
106	106	106	110	104	102	0	100
106	98	92	104	104	104	100	0

3.4. Lineer Olmama

Blok şifreleme algoritmalarında genellikle lineer olmayan tek birim s-box yapısıdır. Bir s-box yapısının saldırılara karşı dirençli olabilmesi için bu değerin olabildiğince yüksek olması gerekmektedir. AES algoritmasında kullanılan s-box yapısı en yüksek değer olan 112 lineer olmama değerine sahiptir. Önerilen s-box yapısının lineer olmama değerleri tablo 6 ‘da verilmiştir. Bu tablo incelendiğinde önerilen yöntem ile elde edilen s-box ‘da bu değerin ortalama 107.5 olduğu görülmektedir. Bu değer 112 değerinden uzak olsa da literatürdeki özellikle kaos tabanlı çalışmaların çoğunu geride bırakmaktadır. Ancak bu değer de geliştirilebilecek bir değerdir.

Tablo 6. Önerilen s-box yapısı için lineer olmama değerleri

1	2	3	4	5	6	7	8
108	108	108	108	106	104	110	108

Önerilen algoritma ile elde edilen s-box yapısı tablo 7 ‘de verilmektedir. Bu s-box sadece 100 yineleme ve O(n) notasyonunda elde edilmiştir. Bu durum, algoritmanın hızlı çalıştığını göstermektedir. Yani önerilen algoritma hızlı bir şekilde lineer olmama değerini arttırmaktadır. Önerilen s-box yapısının üstünlük sağladığı diğer s-box yapılarıyla performans karşılaştırması tablo 8 ‘de verilmiştir. Buradaki karşılaştırma sonuçları, 8-bit bir S-box 'ın lineer olmama, XOR dağılımı, SAC ve BIC özelliklerini göstermektedir. Önerilen yöntem, lineer olmama değeri bakımından bu çalışmalara üstünlük sağlamıştır. Diğer kriterler için çalışmaların çoğunda birbirine yakın sonuçlar elde edilmiştir.

Tablo 7. Önerilen s-box yapısı

	0	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**
0	136	138	39	55	243	145	46	74	3	179	36	73	58	156	15	41
1	89	210	247	115	111	126	198	30	171	214	185	199	14	186	42	96
2	140	71	114	90	7	226	155	116	35	117	148	225	22	13	178	59
3	130	240	92	106	235	84	190	91	215	43	194	113	49	183	78	137
4	69	158	139	180	132	110	141	101	134	231	208	249	182	250	27	102
5	95	238	200	224	52	252	123	0	227	149	165	79	127	244	31	40
6	216	57	203	1	230	67	2	63	105	120	229	160	56	242	174	170
7	197	61	175	251	37	254	146	223	32	143	228	233	220	29	162	108
8	218	47	142	153	133	128	150	65	19	206	24	70	221	81	204	177
9	201	222	60	191	248	82	6	25	87	112	236	48	144	166	93	159
10	62	213	98	253	125	104	205	195	168	245	184	20	100	103	8	207
11	241	176	121	68	16	86	107	33	255	38	239	34	135	17	51	26
12	234	187	189	5	77	4	9	237	129	209	54	217	192	99	147	28
13	169	75	80	88	94	181	164	124	161	122	12	172	212	193	72	131
14	83	163	157	188	152	232	53	45	211	151	196	85	64	246	66	18
15	11	21	50	109	219	119	76	23	97	44	202	10	173	118	154	167

Tablo 8. Diğer s-box üretme yaklaşımlarıyla performans karşılaştırması

Yöntem	**Lineer Olmama**			**SAC**	**BIC**		**max XOR**
	ort	**min**	**max**	**ort**	**SAC**	**Lineer O.**	
Önerilen	**107.5**	104	110	0.5051	0.4988	103.57	12
[21]	**107.25**	106	110	0.501	-	107	6
[7]	**107**	106	108	0.496	0.4974	104.6	10
[12]	**107**	106	110	0.5015	0.5010	105.5	10
[35]	**106.7**	108	104	0.4976	0.504	103.5	10
[31]	**106.5**	108	106	0.4978	0.5003	104.2	10

[10]	**106.5**	104	110	0.5120	0.4984	105.2	10
[6]	**106.5**	104	108	0.5036	0.4995	105.85	10
[32]	**106.2**	108	106	0.501	0.5288	100	10
[38]	**106.2**	110	104	0.5039	0.5023	102.3	10
[34]	**105.5**	110	102	0.5010	0.4988	104.3	12
[36]	**105.25**	108	102	0.5037	0.4994	102.6	10
[33]	**104.7**	108	102	0.5034	0.4972	103.3	10
[13]	**104**	102	106	0.4980	0.4971	103.2	10
[29]	**103.8**	108	101	0.5058	0.4958	102.6	14
[30]	**103.3**	99	110	0.4987	0.4995	103.3	10

Tablo 8. Devamı.

4. Sonuçlar

Bu çalışmada, yüksek lineer olmama değerine sahip s-box yapıları üretmek için yeni ve hızlı bir yöntem önerilmiştir. Önerilen yöntem özellikle kaos tabanlı s-box yapılarının lineer olmama değerini arttırmak için geliştirilmiştir. Çünkü kaos tabanlı s-box yapılarının lineer olmama değeri düşüktür ve bu durum çeşitli güvenlik zafiyetleri doğurmaktadır. Önerilen yöntem ile başlangıçta kaotik bir harita yardımıyla bir s-box üretilir. Daha sonra yine kaotik harita ile elde edilen iki değerin yeri değiştirilerek lineer olmama değeri kontrol edilir. Bu değer arttığında s-box güncellenir. Bu sayede lineer olmama değeri hızlı bir şekilde arttırılır ve s-box daha güçlü hale gelir. Bu çalışmada sadece 100 yineleme sonucunda lineer olmama değeri 107.5 olan bir s-box elde edilmiştir. Bu değer bile literatürdeki birçok çalışmayı geride bırakmaktadır. Yineleme sayısı arttırıldığında daha yüksek değerlere ulaşılabilmektedir. Ayrıca önerilen yöntem ile elde edilen s-box yapısının diğer kriptografik gereksinimleri sağladığı da yapılan analizler sonucunda belirlenmiştir. Önerilen yöntemin en önemli avantajlarından bir tanesi, çok sayıda kaotik harita olmasıdır. Farklı kaotik haritalarla hem başlangıç s-box yapısı oluşturulabilir hem de yer değiştirilecek elemanlar farklı kaotik haritalarla seçilebilir.

Kaynaklar

[1] Van Oorschot, P. C., Menezes, A. J., Vanstone, S. A. Handbook of applied cryptography. CRC press, 1996.
[2] J. Daemen and V. Rijmen, AES proposal: Rijndael, in Proc. 1st Adv. Encryption Conf., CA, USA, pp. 1–45, 1998.
[3] Standard, D. E. Data encryption standard. Federal Information Processing Standards Publication, 112, 1999.
[4] Artuğer, F., Özkaynak, F. SBOX-CGA: substitution box generator based on chaos and genetic algorithm. Neural Computing and Applications, 1-9, 2022.
[5] Artuğer, F., Özkaynak, F. An effective method to improve lineer olmama değer of substitution boxes based on random selection. Information Sciences, 576, 577-588, 2021.
[6] Ahmad, M., Khaja, I. A., Baz, A., Alhakami, H. Alhakami, W. Particle swarm optimization based highly nonlinear substitution-boxes generation for security applications. IEEE Access, 8, 116132-116147, 2020.
[7] Alhadawi, H. S., Lambić, D., Zolkipli, M. F., Ahmad, M. Globalized firefly algorithm and chaos for designing substitution box. Journal of Information Security and Applications, 55, 102671, 2020.
[8] Ahmad, M., Al-Solami, E. Evolving dynamic S-boxes using fractional-order hopfield neural network based scheme. Entropy, 22(7), 717, 2020.
[9] Alzaidi, A. A., Ahmad, M., Ahmed, H. S., Solami, E. A. Sine-cosine optimization-based bijective substitution-boxes construction using enhanced dynamics of chaotic map. Complexity, 2018, 2018.

[10] Farah, T., Rhouma, R., Belghith, S. A novel method for designing S-box based on chaotic map and teaching–learning-based optimization. Nonlinear dynamics, 88(2), 1059-1074, 2017.

[11] Tian, Y., Lu, Z. Chaotic S-box: Intertwining logistic map and bacterial foraging optimization. Mathematical Problems in Engineering, 2017, 2017.

[12] Ahmad, M., Bhatia, D., Hassan, Y. A novel ant colony optimization based scheme for substitution box design. Procedia Computer Science, 57, 572-580, 2015.

[13] Chen, G. A novel heuristic method for obtaining S-boxes. Chaos, Solitons & Fractals, 36(4), 1028-1036, 2008.

[14] Zamli, K. Z., Kader, A., Din, F., Alhadawi, H. S. Selective chaotic maps Tiki-Taka algorithm for the S-box generation and optimization. Neural Computing and Applications, 1-18, 2021.

[15] Zamli, K. Z. Optimizing S-box Generation based on the Adaptive Agent Heroes and Cowards Algorithm. Expert Systems with Applications, 115305, 2021.

[16] Alhadawi, H. S., Majid, M. A., Lambić, D., Ahmad, M. A novel method of S-box design based on discrete chaotic maps and cuckoo search algorithm. Multimedia Tools and Applications, 80(5), 7333-7350, 2021.

[17] Wei, Y., Pasalic, E., Zhang, F., Hodžić, S. Efficient probabilistic algorithm for estimating the algebraic properties of Boolean functions for large n. Information Sciences, 402, 91-104, 2017.

[18] Örs, S. B., Preneel, B., Verbauwhede, I. Side-channel analysis attacks on hardware implementations of cryptographic algorithms. Wireless Security and Cryptography-Specifications and Implementations, 213-247, 2007.

[19] Hussain, I. True-chaotic substitution box based on Boolean functions. The European Physical Journal Plus, 135(8), 1-17, 2020.

[20] Malik, M. S. M., Ali, M. A., Khan, M. A., Ehatisham-Ul-Haq, M., Shah, S. N. M., Rehman, M., Ahmad, W. Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. IEEE Access, 8, 35682-35695, 2020.

[21] Arshad, B., Siddiqui, N., Hussain, Z., Ehatisham-ul-Haq, M. A Novel Scheme for Designing Secure Substitution Boxes (S-Boxes) Based on Mobius Group and Finite Field. Wireless Personal Communications, 1-22, 2022.

[22] Razaq, A., Ullah, A., Alolaiyan, H., Yousaf, A. A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers. Wireless Personal Communications, 116(4), 3165-3190, 2021.

[23] Ahmad, M., Al-Solami, E. Improved 2D Discrete Hyperchaos Mapping with Complex Behaviour and Algebraic Structure for Strong S-Boxes Generation. Complexity, 2020.

[24] Khan, M., Shah, T. A novel image encryption technique based on Hénon chaotic map and S8 symmetric group. Neural Computing and Applications, 25(7), 1717-1722, 2014.

[25] Siddiqui, N., Yousaf, F., Murtaza, F., Ehatisham-ul-Haq, M., Ashraf, M. U., Alghamdi, A. M., Alfakeeh, A. S. A highly nonlinear substitution-box (S-box) design using action of modular group on a projective line over a finite field. Plos one, 15(11), e0241890, 2020.

[26] Razaq, A., Ahmad, M., Yousaf, A., Alawida, M., Ullah, A., Shuaib, U. A group theoretic construction of large number of AES-like substitution-boxes. Wireless Personal Communications, 122(3), 2057-2080, 2022.

[27] Artuğer, F., Özkaynak, F. A novel method for performance improvement of chaos-based substitution boxes. Symmetry, 12(4), 571, 2020.

[28] Artuğer, F., Özkaynak, F. A method for generation of substitution box based on random selection. Egyptian Informatics Journal, 23(1), 127-135, 2022.

[29] Tang, G., Liao, X. A method for designing dynamical S-boxes based on discretized chaotic map. Chaos, solitons & fractals, 23(5), 1901-1909, 2005.

[30] Tang, G., Liao, X., Chen, Y. A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons & Fractals, 23(2), 413-419, 2005.

[31] Lambić, D. S-box design method based on improved one-dimensional discrete chaotic map. Journal of Information and Telecommunication, 2(2), 181-191, 2018.

[32] Lambić, D. A new discrete-space chaotic map based on the multiplication of integer numbers and its application in S-box design. Nonlinear Dynamics, 100(1), 699-711, 2020.

[33] Özkaynak, F. An analysis and generation toolbox for chaotic substitution boxes: A case study based on chaotic labyrinth rene thomas system. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 44(1), 89-98, 2020.

[34] Belazi, A., Abd El-Latif, A. A. A simple yet efficient S-box method based on chaotic sine map. Optik, 130, 1438-1444, 2017.

[35] Ye, T., Zhimao, L. Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. Nonlinear Dynamics, 94(3), 2115-2126, 2018.

[36] Özkaynak, F. On the effect of chaotic system in performance characteristics of chaos based s-box designs. Physica A: Statistical Mechanics and its Applications, 550, 124072, 2020.

[37] Khan, M., Shah, T., Gondal, M. A. An efficient technique for the construction of substitution box with chaotic partial differential equation. Nonlinear Dynamics, 73(3), 1795-1801, 2013.

[38] Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., Kaçar, S. A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear dynamics, 87(2), 1081-1094, 2017.

[39] Liu, G. Designing S-box based on 4D-4wing hyperchaotic system. 3D Research, 8(1), 1-9, 2017.

[40] Özkaynak, F., Özer, A. B. A method for designing strong S-Boxes based on chaotic Lorenz system. Physics Letters A, 374(36), 3733-3738, 2010.

[41] Khan, M., Shah, T. An efficient construction of substitution box with fractional chaotic system. Signal, Image and Video Processing, 9(6), 1335-1338, 2015.

[42] Özkaynak, F., Çelik, V., Özer, A. B. A new S-box construction method based on the fractional-order chaotic Chen system. Signal, Image and Video Processing, 11(4), 659-664, 2017.

[43] Tanyildizi, E., Özkaynak, F. A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps. IEEE Access, 7, 117829-117838, 2019.

[44] Biham, E., Shamir, ADifferential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4(1), 3-72, 1991.

[45] Webster, A. F., Tavares, S. E. On the design of S-boxes. In Conference on the theory and application of cryptographic techniques (pp. 523-534). Springer, Berlin, Heidelberg, 1985.