Erciyes Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
Cilt 39, Sayı 1, 2023

Erciyes University
Journal of Institue Of Science and Technology
Volume 39, Issue 1, 2023

# Güçlü S-box Yapıları Üretmek İçin Yeni Bir Yaklaşım

**Fırat Artuğer**[*1]

[*1] Munzur Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği, TUNCELİ

(Alınış / Received: 20.02.2023, Kabul / Accepted: 25.04.2023, Online Yayınlanma / Published Online: 02.05.2023)

**Anahtar Kelimeler**
S-box
Lineer olmama
Simetrik şifreleme
Kaotik harita

**Öz:** S-box, kriptografik yapılar için hayati öneme sahiptir. Çünkü bir simetrik şifreleme algoritmasında karıştırma olarak adlandırdığımız gereksinimi yerine getirmektedir. Bu yüzden geliştirilecek olan simetrik şifreleme algoritmasının başarımı önemli ölçüde s-box yapısına bağlı olacaktır. Bir s-box yapısı olabildiğince lineer bir yapıya sahip olmamalıdır. Yani bir s-box yapısının bakılması gereken en önemli kriteri yüksek lineer olmama değeridir. Lineer olmama değeri ne kadar yüksek olursa algoritmanın kırılması o kadar zor olacaktır. Bir s-box elde etmek için genellikle kaotik yöntemler kullanılmaktadır. Ancak bu şekilde elde edilen s-box yapılarında lineer olmama değeri düşüktür. Bu çalışmada özellikle bu şekilde üretilen s-box yapılarının lineer olmama değerini hızlı bir şekilde arttıran bir yöntem önerilmektedir. Bu yöntemde rastgele elde edilmiş bir s-box yapısında ilk değer sırasıyla diğer tüm elemanlarla yer değiştirilir. Bu şekilde s-box yapısının lineer olmama değeri artar veya eşit kalırsa s-box güncellenir. Bu şekilde sadece 255 iterasyon ile lineer olmama değeri 102.25 'den 107.5 'e kadar arttırılmıştır. Bir diğer s-box 'da ise lineer olmama değeri 103.75 'den 107.25 'e çıkmıştır.

# A New Approach to Generation Strong S-box Structures

**Keywords**
S-box
Nonlinearity,
Symmetric encryption
Chaotic map

**Abstract:** The s-box is vital for cryptographic structures. Because it fulfills the requirement we call confusion in a symmetric encryption algorithm. Therefore, the performance of the symmetric encryption algorithm to be developed will depend significantly on the s-box structure. An s-box structure should not be as linear as possible. In other words, the most important criterion for an s-box structure is its high nonlinearity value. The higher the nonlinearity value, the more complex the algorithm will be to break. Chaotic methods are generally used to obtain an s-box. However, the nonlinearity value of the s-box structures obtained this way is low. In this study, a method that rapidly increases the nonlinearity value of s-box structures produced in this way is proposed. In this method, the first value in a randomly generated s-box structure is replaced with all other elements, respectively. In this way, if the nonlinearity of the s-box structure increases or remains equal, the s-box is updated. In this way, the nonlinearity value was increased from 102.25 to 107.5 with only 255 iterations. In another s-box, the nonlinearity value increased from 103.75 to 107.25.

*İlgili Yazar, email: firatartuger@munzur.edu.tr

## 1. Giriş

Bilimin hızlı bir şekilde gelişmesiyle birlikte birçok gereksinim ortaya çıkmaktadır. Bu gereksinimlerden bir tanesi verileri gizliliğinin sağlanmasıdır. Özellikle kablosuz ağlar üzerinden verilerin güvenli bir şekilde iletilmesi önemli bir gereksinimdir. Günümüzde verilerin gizliliği genellikle kriptografik yapılar ile sağlanmaktadır [1]. Özellikle verinin gizliliği söz konusu olduğunda şifreleme algoritmaları karşımıza çıkmaktadır. Yani özetle; verilerin gizliliğini sağlamak için günümüzde şifreleme algoritmaları kullanılmaktadır. Bu yapılar temel olarak iki mimariye sahiptirler. Bunlardan bir tanesi asimetrik şifrelemedir. Bu şifreleme mimarileri genellikle verinin gizliliğinden

ziyade anahtar değişimi sürecinde kullanılmaktadır. Çünkü bu algoritmalarda mantık, büyük asal sayıları çarpımına dayanmaktadır. Verinin boyutu arttıkça gizlilik için uygulanması imkânsız hale gelmektedir. Ancak bunlar çok güvenli algoritmalardır. Bu yüzden hibrit sistemlerde anahtar değişimini sorunsuz bir şekilde yerine getirebilmektedirler. Bir diğer şifreleme mimarisi simetrik şifreleme yapılarıdır. Bu yapılar verinin şifrelenmesi için kullanılmaktadır. Bu algoritmalar genellikle hızlı ve çoğu zaman güvenlidirler. Bu mimari de yine kendi içinde iki bölüme ayrılmaktadır. Bunlar akış ve blok şifreleme yapılarıdır. Akış şifreleme de bitler tek tek şifrelenir. Bu algoritmalar mantığı gereği oldukça hızlı ve güvenli yapılardır. Ancak daha az verinin olduğu alanlarda etkili bir şekilde çalışabilirler. Verinin uzunluğu arttıkça bu mimariyi uygulamak zor hale gelecektir. Bu yüzden bu algoritmalar daha hafif uygulamalar için kullanılmaktadırlar. Diğer simetrik şifreleme yapısı blok şifrelemedir. Günümüzde verinin şifrelenmesi için en çok bu algoritmalar kullanılmaktadır. Bu algoritmaların temel yapısı veriyi eşit uzunluktaki bloklara ayırmaktır. Bu şekilde veri ne kadar büyük olursa olsun eşit bloklara ayrılır ve bu şekilde her bir blok kendi içinde şifrelenir. Daha sonra bütün bloklar bir araya getirilerek şifreli veri elde edilir. Bu mimari, verinin aynı zamanda hem güvenli hem de hızlı bir şekilde şifrelenmesini sağlamaktadır. Günümüz simetrik blok şifreleme standardı AES [2] algoritmasıdır. Bunun yanında en çok DES [3] algoritması kullanılmaktadır. AES algoritması farklı anahtar uzunluklarına sahip esnek ve oldukça güvenilir bir algoritmadır.

Bir blok şifreleme algoritmasında güvenliğin sağlanabilmesi için temelde iki gereksinimin sağlanması istenir. Bunlar difüzyon ve konfüzyon olarak adlandırılır. Difüzyon özelliğinde verilerin etkili bir şekilde yayılması amaçlanmaktadır. Bu özellik bir nevi permütasyon sürecidir. Diğeri ise en önemli gereksinimlerden biri olan konfüzyon özelliği, veriyi etkili bir şekilde karıştırmayı amaçlamaktadır. Veri ne kadar etkili bir şekilde karıştırılırsa saldırganlar tarafından şifrenin çözülmesi o kadar zor olacaktır. Bu yüzden karıştırma sürecinde bu işlemin lineer olmayan bir yapıyla yapılması gerekir. Aksi taktirde bu yapı lineer olursa saldırganlar tarafından çıkarım yapılması kolaylaşacaktır [4]. Blok şifreleme algoritmalarında bu lineer olmayan yapı s-box yapısıdır. Yani algoritmadaki konfüzyon adımı genellikle lineer olmayan bir s-box yapısı ile gerçekleştirilir. S-box temel olarak bir tablodan oluşmaktadır. Veriyi bir formdan alır başka bir forma çevirir. Yani s-box tablosundaki değerlere göre veride bir değerin yerine başka bir değer yazılır [5]. Bu özelliklere bakıldığında; bir blok şifreleme algoritması tasarlanmak istenildiğinde güçlü bir s-box olmazsa olmaz yapılardan biri olarak karşımıza çıkmaktadır. Güçlü, yani yüksek lineer olmama değerine sahip bir s-box üretmek aslında bir optimizasyon problemidir. Çünkü AES benzeri bir s-box yapısı 256 değer içermektedir. Bu da güçlü bir s-box elde etmek için 256! durumun olduğunu ifade eder. Bu problemin belirli bir birim zamanda çözülmesi imkansızdır. Yani bu bir NP problemdir. Bu yüzden bu problem, geçmişten günümüze kadar araştırmacıların üzerinde çalıştığı sıcak bir konu olarak gelmiştir. Buda çalışmanın en önemli motivasyonlarından bir tanesidir. Bu problemin çözümü için literatürde onlarca yöntem önerilmiş olup çalışmalar devam etmektedir. Çünkü en iyi sonuçlar elde edilememektedir. Bazı çalışmalar optimum sonuçlara ulaşmış olsa da bu yapıların elde edilme şeklinde çeşitli zayıflıklar olabilmektedir. Güçlü bir s-box geliştirmek için günümüze kadar kaos, optimizasyon yöntemleri ve matematiksel dönüşümler en çok kullanılan yaklaşımların başında gelmektedir.

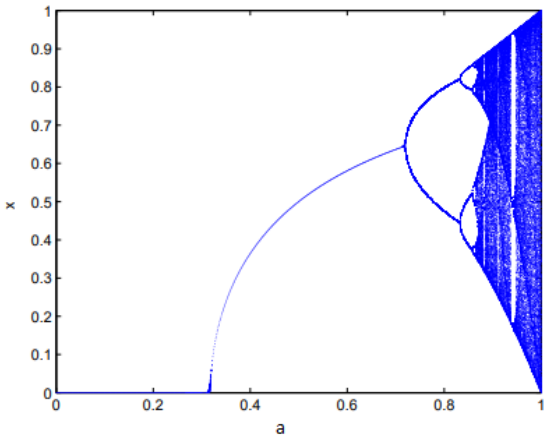
Sadece kaos kullanarak geliştirilen yöntemler genellikle düşük lineer olmama değerlerine sahip s-box yapılarıdır. Bu nokta çalışmanın bir diğer motivasyon kaynağıdır. Bu yapıları hızlı bir şekilde iyileştiren yöntemlerin geliştirilmesi araştırmacıların her zaman ilgisini çekmiştir. Bu şekilde elde edilen s-box yapılarında genellikle bir kaotik harita kullanılmaktadır. Kaotik haritanın parametrelerine göre bir değer elde edilir ve s-box tablosunda bu değer yoksa tabloya eklenir. Bu şekilde bir s-box elde etmek oldukça kolay ve hızlı olacaktır. Ancak lineer olmama değerlerinin düşük olması büyük bir dezavantaj oluşturmaktadır. Günümüze kadar kaos ile elde edilen s-box yapılarında kesirli sıralı kaotik Chen sistemi [6], kaotik kısmi diferansiyel denklem [7], lojistik harita [8], yeni bir ayrık zamanlı kaotik harita [9], tek boyutlu ayrık bir kaotik harita [10], baker harita [11], çadır harita [12], kaotik Lorenz sistemi [13], kaotik labirent rene Thomas sistemi [14], kesirli Lorenz-Duffing sistemi [15], kaotik ölçekli Zhongtang sistemi [16], kaotik sinüs harita [17] ve daha birçok farklı kaotik harita kullanılmıştır.

Bir diğer çok kullanılan yaklaşım optimizasyondur. Optimizasyon yöntemleri özellikle çözülmesi zor problemlerin çözümünde uzun yıllardır kullanılmaktadır. S-box üretme problemi içinde kullanımları oldukça uygundur. Bu yöntemlerde hesaplama maliyetleri genellikle yüksek olsa da lineer olmama değerleri yüksek s-box yapıları elde edilmektedir. Bu yöntemlerin bir diğer avantajı ise gün geçtikçe yeni optimizasyon algoritmalarının tasarlanmasıdır. Bu yeni algoritmalar da kullanılarak güçlü s-box yapıları elde edilebilir. Özellikle son yıllarda s-box üretme probleminde parçacık sürüsü optimizasyonu [18], bakteriyel yiyecek arama optimizasyonu [19], genetik algoritma [20, 21], tavlama algoritması [22], öğretme-öğrenme optimizasyonu [23], ateş böceği optimizasyonu [24], karınca kolonisi optimizasyonu [25], çıplak köstebek faresi algoritması [26], gri kurt optimizasyonu [27] ve daha birçok optimizasyon algoritması kullanılmıştır. Bir diğer yaklaşım olan matematiksel dönüşümler ile farklı s-box yapıları elde edilmektedir. Bu yaklaşım ile genellikle güçlü s-box yapıları üretilmektedir. Ancak bu s-box yapıları çeşitli durumlarda uygulama saldırılarına karşı çeşitli zayıflıklar göstermektedir [28]. Bunun yanı sıra karmaşık matematiksel denklemlere dayandıkları için hesaplama maliyetleri yüksektir. Bu yaklaşımla son yıllarda mobius grubu ve sonlu alan ile [29], dönme matrisleri ile [30], modüler bir grup eylemi ile [31], simetrik bir grup ile [32], boole fonksiyonları ile [33, 34] ve daha birçok dönüşüm yardımıyla güçlü s-box yapıları elde edilmiştir.

Bu çalışmada bu yöntemlerden farklı olarak hızlı, basit ama etkili bir yöntem önerilmiştir. Önerilen yöntemde herhangi bir şekilde elde edilen bir s-box yapısında ilk eleman sırasıyla diğer elemanlarla yer değiştirilir. Yer değiştirme sonrasında lineer olmama değeri artar veya eşit kalırsa s-box güncellenmektedir. Bu şekilde sadece 256 yineleme sonucunda etkili sonuçların elde edilebildiği yapılan analizler sonucunda gösterilmiştir. Esasen önerilen yöntem yukarıda bahsedilen tüm mantıklarla elde edilen s-box yapılarını da iyileştirebilecek bir yapıya sahiptir. Bu çalışma, özellikle kaos tabanlı s-box yapılarının iyileştirilmesi için düşünülmüştür. Ancak diğer felsefelerle üretilen s-box yapılarına da kolaylıkla uygulanabilir. Çalışmanın geri kalan kısmında ikinci bölümde önerilen yaklaşım sözde kodu ile verilmiştir. Üçüncü bölümde analiz sonuçları değerlendirilmiş olup diğer yöntemlerle performans karşılaştırması yapılmıştır. Dördüncü bölümde ise sonuçlar tartışılmıştır.

## 2. Önerilen Yöntem

Önerilen yaklaşımda öncelikle kaotik bir harita kullanılarak lineer olmama değeri düşük bir s-box elde edilir. Bu çalışmada kaotik sinüs harita ile başlangıç parametreleri ayarlanarak s-box yapıları elde edilmiştir. Kaotik sinüs haritasının matematiksel modeli denklem 1 'de verilmiştir. Ayrıca sinüs haritasının çatallanma diyagramı şekil 1 'de gösterilmiştir. Çatallanma diyagramı sayesinde sistemin kaotikliği, kararlılığı vb. davranışsal özellikleri hakkında yorum yapılabilmektedir. Kullanılan sinüs haritanın verilen parametrelerle kaotik davranış gösterdiği görülmektedir.




Şekil 1. Sinüs haritasının çatallanma diyagramı

$$x_{n+1} = a\sin(\pi x_n)\,, \quad x_n \in [0,1]\,, \quad a \in [0.85,1] \tag{1}$$

Denklem 1 'de verildiği gibi kaotik bir harita kullanılarak aşağıdaki adımlara göre kolaylıkla bir s-box elde edilebilir.

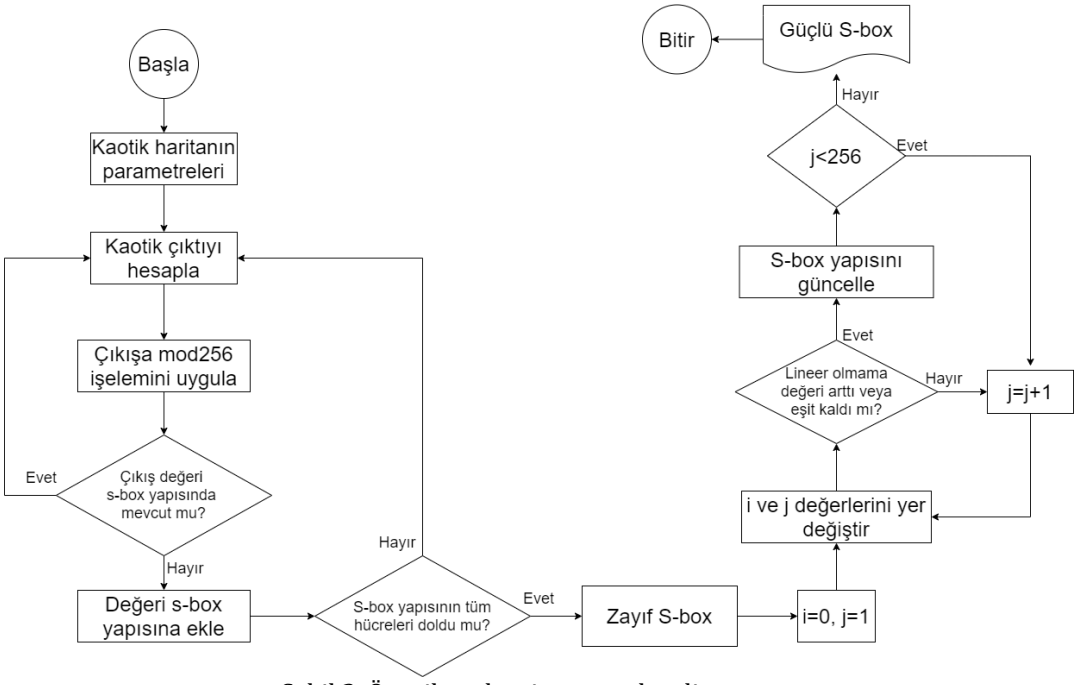
Adım 1. Kaotik haritanın başlangıç parametreleri girilir.
Adım 2. Bu başlangıç değerlerine göre rastgele bir sayı ($x_{n+1}$) üretilir.
Adım 3. Üretilen bu değerin 3 veya daha fazla basamaklı bir tamsayıya dönüşmesi için 1000000 ile çarpılır.
Adım 4. Bu değerin 0 ile 256 arasındaki bir değere dönüşmesi için mod256 işlemi uygulanır.
Adım 5. Elde edilen bu değer, s-box yapısında yoksa eklenir, varsa yeni bir değer üretilir. Bu şekilde s-box dolana kadar bu adımlar devam eder.

Yukarıdaki adımlar ile elde edilen s-box yapılarında lineer olmama değeri neredeyse her zaman düşük kalmaktadır. Bunun için bu s-box yapılarının sadece ilk değerini diğer değerlerle karşılaştırılıp lineer olmama değerini kontrol edilmektedir. Bu değer arttığında ya da eşit kaldığında s-box yapısını güncellenir. Bu sayede lineer olmama değeri hızlı bir şekilde arttırılmış olur. Ayrıca önerilen yöntem Python programlama dili ile uygulanmıştır. Ancak, kullanıcıların tercihine göre diğer dillerde de kolayca uygulanabilecek bir yapıya sahiptir. Önerilen yöntemin araştırmacılar için daha iyi anlaşılması ve uygulanabilmesi için sözde kodu tablo 1 'de, akış diyagramı ise şekil 2 'de verilmiştir.

Tablo 1. Önerilen algoritmanın akış sözde kodu

```
1.  Başla
2.  SboxUretme ()
3.  KaotikSbox= []
4.  YeniSbox = []
5.  EskiLineerOlmama= KaotikSbox yapısının lineer olmama değeri
6.  for(int i=1; i<256; i++)
7.  YerDeğiştir (KaotikSbox[0], KaotikSbox[i]
8.  YeniLineerOlmama =YeniSbox yapısının lineer olmama değeri
9.  if (YeniLineerOlmama >= EskiLineerOlmama)
10. Sbox yapısını güncelle
11. end if
12. else
13. KaotikSbox = YeniSbox
14. end else
15. end for
16. Bitir
```

Tablo 1 'de gösterildiği gibi önerilen algoritma oldukça basit ve uygulanabilir bir yapıdadır. Satır 6 'da görüldüğü üzere sadece 256 iterasyon ile etkili sonuçlar alınabilmektedir.




Şekil 2. Önerilen algoritmanın akış diyagramı

### 3. Analiz Sonuçları

Önerilen yöntem ile iki farklı s-box yapısı iyileştirilmiştir. Bu sayede algoritmanın başarımı daha iyi değerlendirilebilir. Başlangıçta kaotik sinüs harita ile elde edilen güçsüz s- box yapıları sırasıyla tablo 2 ve tablo 3 'de verilmiştir. Bu s-box yapılarının önerilen algoritma ile iyileştirildikten sonraki halleri ise tablo 4 ve tablo 5 'de verilmiştir. Elde edilen s-box yapılarında önerilen algoritma neredeyse aynı başarıyı sergilemiştir. Önerilen bu s-box yapılarını test etmek için literatürde en çok kullanılan metrikler kullanılmıştır. Bunların ilki lineer olmama metriğidir. Bu metrik aynı zamanda uygunluk değeri olarak kullanılmıştır. Çünkü s-box yapıları lineer olmayan yapılardır ve en önemli özellikleri budur [35]. Bu yüzden bu değerin yüksek olması, algoritmanın performansını önemli ölçüde etkileyecektir. Önerilen s-box yapılarında lineer olmama değerleri sırasıyla 107.25, 107.5 olarak hesaplanmıştır. Bu değerler yüksek olarak kabul edilebilir. Bu sayede önerilen s-box yapıları lineer olmama özelliğini sağlamaktadır. Ayrıca bu değerler literatürdeki çoğu çalışmayı geride bırakmaktadır. Bir diğer önemli s-box değerlendirme kriteri SAC değeridir. Bu değer giriş bitlerinde yapılan bir değişikliğe göre çıkıştaki bitlerin değişimini hesaplamaktadır [36]. Şöyle ki; bir şifreleme algoritmasında girişteki bir bitte değişiklik yapıldığında çıkıştaki bitlerin yarısına yakınının değişmesi istenmektedir. Bu durum, saldırganların bir çıkarımda bulunmalarını engellemektedir. Bu yüzden SAC değerinin 0.5 değerine yakın bir değerde olması istenir. Önerilen s-box yapılarının ikisinde de bu değer 0.5 değerine oldukça yakındır. Yani önerilen s-box yapıları bu metriği de

sağlamaktadır. Bir diğer değerlendirme metriği BIC değeridir. Bu değerde yine literatürde sıklıkla kullanılmaktadır. Bu değer bitlerin birbirinden bağımsız olması gerektiğini ifade eder [36]. Yani bir bitte yapılacak olan değişikliklerle diğer bitler hakkında çıkarım yapılamamalı. Bu metrikte hem lineer olmama değeri hem de SAC değeri hesaplanmaktadır. Lineer olmama değerinin yüksek, SAC değerinin ise yine 0.5 'e yakın bir değer olması beklenmektedir. Önerilen s-box yapıları bu metriği de sağlamaktadır. Bir diğer değerlendirme kriteri s-box yapısının XOR değerlerinin hesaplanmasıdır. Bu metrik, bir s-box yapısının giriş ve çıkış değerlerinde olasılık dağılımlarına izin verilmemesini sağlar [37]. Bu değerin tüm s-box yapısı için düşük değerlerde olması istenir. Önerilen s-box yapıları bu metriği de sağlamaktadır. Bir diğer istenilen metrik ise s-box yapısının bijektif olmasıdır. Yani her bir değerin sadece bir kez kullanılması gerekmektedir. 8 bit bir s-box yapısında 256 değer olduğundan 0 ile 256 arasındaki sayılarla s-box elde edilir. Önerilen s-box yapılarında değerler sadece bir kere kullanıldığı için ikisi de bijektiftir.

Tablo 2. Kaotik s-box-1

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

Tablo 3. Kaotik s-box-2

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

Tablo 4. Kaotik s-box-1 yapısının iyileştirilmiş hali

| | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** | **13** | **14** | **15** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

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

Tablo 5. Kaotik s-box-2 yapısının iyileştirilmiş hali

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

Başlangıçta kaotik sinüs harita ile elde edilen zayıf s-box yapıları ve bu yapıların önerilen algoritma ile iyileştirildikten sonraki performans değerleri tablo 6 'da verilmiştir. Bu tablo incelendiğinde s-box-1 yapısının lineer olmama değerinin 103.75 'den 107.25 'e, s-box-2 yapısının lineer olmama değerinin ise 102.25 'den 107.5 'e yükseldiği görülmektedir. Bu değerlere sadece 255 yineleme ile hızlı bir şekilde ulaşılmıştır.

Tablo 6. Giriş olarak alınan ve iyileştirildikten sonraki s-box yapılarının performans değerleri

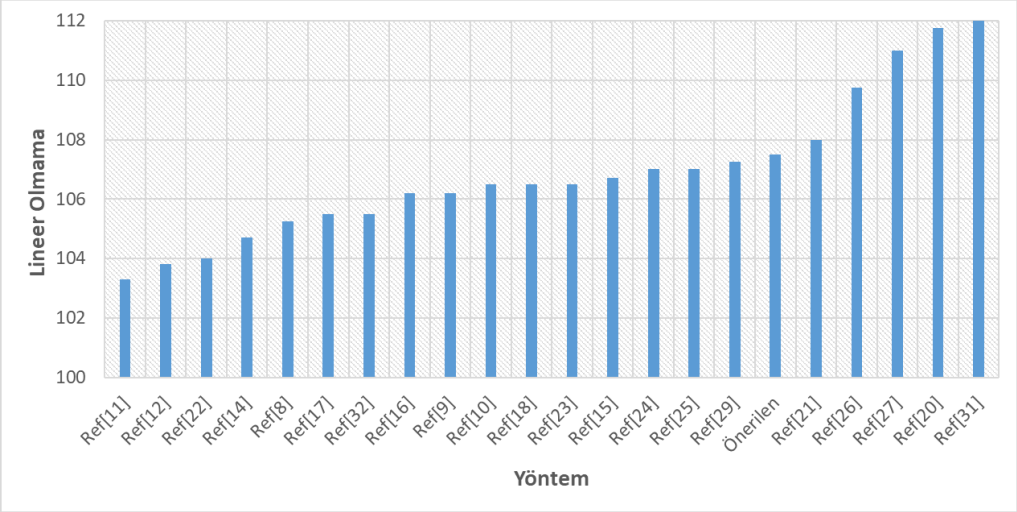
| **S-BOX** | **Lineer Olmama** | | | **SAC** | **BIC** | | **En Yüksek XOR** |
|---|---|---|---|---|---|---|---|
| | **ort** | **min** | **max** | **ort** | **SAC** | **Lineer Olmama** | |
| **S-box-1** | 103.75 | 100 | 106 | 0.5081 | 0.4954 | 103.5 | 10 |
| **S-box-2** | 102.25 | 98 | 106 | 0.5022 | 0.4996 | 103.5 | 10 |
| **İyileştirilmiş S-box-1** | 107.25 | 106 | 110 | 0.5078 | 0.4954 | 103.14 | 10 |
| **İyileştirilmiş S-box-2** | 107.5 | 104 | 110 | 0.5073 | 0.5048 | 103.43 | 12 |

Önerilen s-box yapıları literatürdeki birçok s-box ile karşılaştırılmış olup karşılaştırma sonuçları tablo 7 'de verilmiştir. Bu tablodan da anlaşılacağı gibi önerilen yöntem literatürdeki birçok yöntemi geride bırakmıştır. Ancak özellikle optimizasyon ve matematiksel dönüşüm tabanlı yöntemlerin gerisinde kalmıştır. Bunun temel sebebi, önerilen yöntemin bu yöntemlere göre çok daha hızlı bir sonuç elde etmesidir. Ayrıca önerilen yöntemin karmaşıklığı diğer algoritmalarla karşılaştırıldığında oldukça düşüktür. Bu da algoritmanın bir diğer avantajı olarak kabul edilebilir.

Tablo 7. Önerlin yöntemin diğer yöntemlerle performans karşılaştırması

| S-BOX | Ortalama Lineer Olmama | BIC | | SAC | En Yüksek XOR |
|---|---|---|---|---|---|
| | | SAC | Lineer Olmama | | |
| **Ref[11]** | **103.3** | 0.4995 | 103.3 | 0.4987 | 10 |
| **Ref[12]** | **103.8** | 0.4958 | 102.6 | 0.5058 | 14 |
| **Ref[22]** | **104** | 0.4971 | 103.2 | 0.4980 | 10 |
| **Ref[14]** | **104.7** | 0.4972 | 103.3 | 0.5034 | 10 |
| **Ref[8]** | **105.25** | 0.4994 | 102.6 | 0.5037 | 10 |
| **Ref[17]** | **105.5** | 0.4988 | 104.3 | 0.5010 | 12 |
| **Ref[32]** | **105.5** | 0.4994 | 105.7 | 0.4926 | 32 |
| **Ref[16]** | **106.2** | 0.5023 | 102.3 | 0.5039 | 10 |
| **Ref[9]** | **106.2** | 0.5288 | 100 | 0.501 | 10 |
| **Ref[10]** | **106.5** | 0.5003 | 104.2 | 0.4978 | 10 |
| **Ref[18]** | **106.5** | 0.4995 | 105.85 | 0.5036 | 10 |
| **Ref[23]** | **106.5** | 0.4984 | 105.2 | 0.5120 | 10 |
| **Ref[15]** | **106.7** | 0.504 | 103.5 | 0.4976 | 10 |
| **Ref[24]** | **107** | 0.4974 | 104.6 | 0.496 | 10 |
| **Ref[25]** | **107** | 0.5010 | 105.5 | 0.5015 | 10 |
| **Ref[29]** | **107.25** | - | 107 | 0.501 | 6 |
| **Önerilen** | **107.5** | 0.5048 | 103.43 | 0.5073 | 12 |
| **Ref[21]** | **108** | - | - | - | - |
| **Ref[26]** | **109.75** | 0.5041 | 104.14 | 0.4998 | 10 |
| **Ref[27]** | **111** | 0.4994 | 113.35 | 0.5 | - |
| **Ref[20]** | **111.75** | 0.5033 | 104 | 0.4968 | 12 |
| **Ref[31]** | **112** | - | 112 | 0.4951 | - |

Performans sonuçlarının daha iyi değerlendirilebilmesi için lineer olmama değerlerinin karşılaştırıldığı grafik şekil 3 'de verilmiştir.




Şekil 3. Performans karşılaştırma grafiği

## 4. Sonuçlar

Geçmişten günümüze güçlü s-box yapıları elde etmek oldukça zor bir problem olarak gelmiştir. Bu problemi çözmek için kaos, matematiksel dönüşümler ve optimizasyon algoritmaları başta olmak üzere pek çok yöntem

geliştirilmiştir. Ancak halen optimum çözümler elde edilememiştir. Çünkü tüm bu yöntemlerin avantaj ve dezavantajları vardır. Bu çalışmada bu problemin çözümü için yeni bir yöntem önerilmiştir. Önerilen yöntemde öncelikle kaotik bir harita yardımıyla zayıf bir s-box elde edilmektedir. Daha sonra bu s-box yapısında ilk eleman diğer 255 elemanla sırasıyla yer değiştirilerek lineer olmama değeri kontrol edilir. Bu değer artar ya da eşit kalırsa s-box güncellenir. Bu şekilde sadece 255 iterasyon sonunda lineer olmama değeri önemli ölçüde arttırılabilmektedir. Bu çalışmada bu felsefe ile iki farklı s-box üretilmiştir. Bu s-box yapıları 107.25 ve 107.5 lineer olmama değerleri ile literatürdeki birçok çalışmayı geride bırakmıştır. Bu sonuçların özellikle gelecekte inşa edilecek olan simetrik şifreleme algoritmaları için faydalı olacağı düşünülmektedir. Önerilen yöntemin hızlı ve basit olmasının yanı sıra en önemli avantajlarından bir tanesi ise; diğer yöntemler ile elde edilen nispeten zayıf s-box yapılarının tamamını iyileştirebilecek etkinlikte olmasıdır. Bu algoritmanın lineer olmama değerini belli bir seviyeye kadar arttırabilmesi bir dezavantaj olarak görülebilir. Ancak kullanıcılar daha fazla elemanın yerini değiştirip daha yüksek lineer olmama değerlerine ulaşabilirler.

## Çıkar Çatışması Beyanı

Makale yazarları herhangi bir kurum, kuruluş, kişi ile kişisel ve finansal çıkar çatışması olmadığını beyan etmektedirler.

## Kaynakça


[1] Van Oorschot, P. C., Menezes, A. J., & Vanstone, S. A. (1996). Handbook of applied cryptography. CRC press.

[2] J. Daemen and V. Rijmen, ‘‘AES proposal: Rijndael,’’ in Proc. 1st Adv. Encryption Conf., CA, USA, 1998, pp. 1–45.

[3] Standard, D. E. (1999). Data encryption standard. Federal Information Processing Standards Publication, 112.

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

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

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

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

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

[9] Lambić, D. (2020). 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.

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

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

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

[13] Khan, M., Shah, T., Mahmood, H., Gondal, M. A., & Hussain, I. (2012). A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. Nonlinear Dynamics, 70(3), 2303-2311.

[14] Özkaynak, F. (2020). 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.

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

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

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

[18] Hematpour, N., & Ahadpour, S. (2021). Execution examination of chaotic S-box dependent on improved PSO algorithm. Neural Computing and Applications, 33(10), 5111-5133.

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

[20] Artuğer, F., & Özkaynak, F. (2022). SBOX-CGA: substitution box generator based on chaos and genetic algorithm. Neural Computing and Applications, 34(22), 20203-20211.
[21] Kang, M., & Wang, M. (2022). New Genetic Operators for Developing S-Boxes With Low Boomerang Uniformity. IEEE Access, 10, 10898-10906.
[22] Chen, G. (2008). A novel heuristic method for obtaining S-boxes. Chaos, Solitons & Fractals, 36(4), 1028-1036.
[23] Farah, T., Rhouma, R., & Belghith, S. (2017). A novel method for designing S-box based on chaotic map and teaching–learning-based optimization. Nonlinear dynamics, 88(2), 1059-1074.
[24] Alhadawi, H. S., Lambić, D., Zolkipli, M. F., & Ahmad, M. (2020). Globalized firefly algorithm and chaos for designing substitution box. Journal of Information Security and Applications, 55, 102671.
[25] Ahmad, M., Bhatia, D., & Hassan, Y. (2015). A novel ant colony optimization based scheme for substitution box design. Procedia Computer Science, 57, 572-580.
[26] Zamli, K. Z., Din, F., & Alhadawi, H. S. (2023). Exploring a Q-learning-based chaotic naked mole rat algorithm for S-box construction and optimization. Neural Computing and Applications, 1-23.
[27] Khan, H., Hazzazi, M. M., Jamal, S. S., Hussain, I., & Khan, M. (2023). New color image encryption technique based on three-dimensional logistic map and Grey wolf optimization based generated substitution boxes. Multimedia Tools and Applications, 82(5), 6943-6964.
[28] Örs, S. B., Preneel, B., & Verbauwhede, I. (2007). Side-channel analysis attacks on hardware implementations of cryptographic algorithms. Wireless Security and Cryptography-Specifications and Implementations, 213-247.
[29] Arshad, B., Siddiqui, N., Hussain, Z., & Ehatisham-ul-Haq, M. (2022). A Novel Scheme for Designing Secure Substitution Boxes (S-Boxes) Based on Mobius Group and Finite Field. Wireless Personal Communications, 1-22.
[30] Malik, M. S. M., Ali, M. A., Khan, M. A., Ehatisham-Ul-Haq, M., Shah, S. N. M., Rehman, M., & Ahmad, W. (2020). Generation of highly nonlinear and dynamic AES substitution-boxes (S-boxes) using chaos-based rotational matrices. IEEE Access, 8, 35682-35695.
[31] Siddiqui, N., Yousaf, F., Murtaza, F., Ehatisham-ul-Haq, M., Ashraf, M. U., Alghamdi, A. M., & Alfakeeh, A. S. (2020). 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.
[32] Khan, M., & Shah, T. (2014). A novel image encryption technique based on Hénon chaotic map and S8 symmetric group. Neural Computing and Applications, 25(7), 1717-1722.
[33] Bakunina, E. V., & Dykyi, O. V. (2022). Synthesis method for S-boxes satisfying the criterion of correlation immunity of Boolean and 4-functions. Journal of Discrete Mathematical Sciences and Cryptography, 1-13.
[34] Sokolov, A. V., & Radush, V. V. (2022). A method for synthesis of S-boxes with good avalanche characteristics of component Boolean and quaternary functions. Journal of Discrete Mathematical Sciences and Cryptography, 1-12.
[35] Artuğer, F., & Özkaynak, F. (2021). An effective method to improve lineer olmama value of substitution boxes based on random selection. Information Sciences, 576, 577-588.
[36] Webster, A. F., & Tavares, S. E. (1985, August). On the design of S-boxes. In Conference on the theory and application of cryptographic techniques (pp. 523-534). Springer, Berlin, Heidelberg.
[37] Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY, 4(1), 3-72.