Kaos Tabanlı Yeni Bir Blok Şifreleme Algoritması

Fatih Özkaynak[1] Ahmet Bedri Özer[2] Sırma Yavuz[3]

[1]Yazılım Mühendisliği Bölümü, Fırat Üniversitesi, Elazığ
[2]Bilgisayar Mühendisliği Bölümü, Fırat Üniversitesi, Elazığ
[3]Bilgisayar Mühendisliği Bölümü, Yıldız Teknik Üniversitesi, İstanbul

[1]ozkaynak@firat.edu.tr [2] bedriozer@firat.edu.tr
[3] sirma@ce.yildiz.edu.tr

Özetçe

Bilimin birçok dalında uygulama alanı bulunan kaos teorisinin bilgisayar bilimlerindeki yaygın kullanım alanlarından biride kaotik sistemleri kullanarak yeni kriptolojik sistemlerin tasarlanmasıdır. Bu çalışmada kaos ve kriptoloji bilimleri arasındaki doğal ilişkiden yararlanılarak simetrik şifreleme algoritmalarının nasıl tasarlanabileceği açıklanmıştır. Çalışmada ilk olarak kaos tabanlı kriptolojik sistemlerin teorisi açıklanmış ardından kaos tabanlı blok şifreleme algoritması örneği verilmiştir. Teorik analizler ve bilgisayar simülasyonları önerilen algoritmaların blok şifreleme tasarımları için gerekli tüm performans gereksinimlerini karşıladığını, etkili ve uygulanabilir bir yapıda olduğunu göstermiştir.

1. Giriş

Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür. Kriptoloji biliminin kriptografi ve kriptanaliz olarak adlandırılan iki temel alt dalı bulunmaktadır. Kriptografi, belgelerin şifrelenmesi ve şifresinin çözülmesi için kullanılan yöntemleri araştırırken; kriptanaliz ise kriptolojik sistemlerin kurduğu mekanizmaları inceler ve kırmaya çalışır [1].

Bazı araştırmacılar kaotik sistemlerin gösterdikleri özel davranışlardan dolayı; kaos ve kriptoloji bilimleri arasında güçlü bir ilişki olduğunu vurgulamıştır [2]. 1990'lardan beri blok şifreler, akan şifreler, özet (hash) fonksiyonları, görüntü şifreleme algoritmaları gibi birçok şifreleme sisteminin tasarlanmasında da kaotik sistemleri kullanmışlardır.

Kaos doğrusal olmayan dinamik sistemlerde bulunan gerekirci (deterministik) ve rasgele benzeri bir süreçtir. Kaotik sistemlerin önemli karakteristiklerinden biri sistem parametreleri ve/veya başlangıç koşullarına duyarlı olmasıdır [3]. Sistem parametrelerinde ve/veya başlangıç koşullarında yapılan küçük bir değişiklik, sistem yörüngelerinde büyük değişimlere sebep olmaktadır. Kaosun bu temel karakteristiği; Shannon'un mükemmel gizlilik teorisi için vurguladığı ve modern şifreleme sistemleri için temel karakteristikler olan karıştırma (confusion) ve yayılma (diffusion) özellikleri ile örtüşmektedir [2–4].

Bu çalışmada kaos ve kriptoloji bilimleri arasındaki doğal ilişkiden yararlanılarak kaos tabanlı yeni kriptolojik sistemlerin nasıl tasarlanabileceğine ilişkin teorik temel açıklandıktan sonra kaotik sistemleri temel alan bir blok şifreleme algoritması örneği verilmiştir. İncelenen blok şifreleme mimarisi kaos tabanlı dinamik yer değiştirme kutularını temel almaktadır. Teorik analizler ve bilgisayar simülasyonları önerilen yeni kaos tabanlı dinamik yer değiştirme tablosunun blok şifreleme tasarımları için gerekli tüm performans gereksinimlerini karşıladığını, etkili ve uygulanabilir bir yapıda olduğunu göstermiştir.

Çalışmanın geri kalan kısmı aşağıdaki gibi düzenlenmiştir. Kaos ve kriptoloji bilimleri arasındaki ilişkinin teorik temelleri bölüm 2'de açıklanmıştır. Blok şifreleme algoritmaları hakkında özet bilgiler bölüm 3'de verilmiştir. Çalışmada önerilen algoritmanın detaylı mimarisi bölüm 4'de açıklanmıştır. Önerilen algoritmanın performans ve güvenlik analizleri bölüm 5'de yapılmıştır. Son bölümde ise sonuçlar tartışılarak çalışma özetlenmiş ve önerilerde bulunulmuştur.

2. Kaos Tabanlı Kriptoloji

Daha önce belirtildiği gibi kaos ve kriptoloji bilimleri arasında doğal bir ilişki bulunmaktadır. Bu ilişki Shannon'un herhangi bir şifreleme sisteminin güvenilir olması için sahip olması gereken özellikler olan karıştırma ve yayılma özellikleri ile kaotik sistemlerin başlangıç koşullarına duyarlı olması ve doğrusal olmaması özellikleriyle örtüşmesinden ortaya çıkmaktadır [2–4].

Karıştırma özelliğine sahip şifreleme sistemlerinde; her anahtar için şifreleme algoritması öyle olmalıdır ki, açık metin ve şifreli metin arasındaki yapılar arasında istatistiksel bağlılık olmamalıdır. Bu özelliğin olabilmesi için anahtar ve açık metinin her bitinin şifreli metini etkilemesi gerekmektedir [1].

Yayılma özelliğine sahip bir şifreleme sistemi için ise; şifreli metin ile anahtar arasındaki ilişkiyi mümkün olduğunca karmaşık olmalıdır. Diğer bir deyiş ile yayılma, anahtarın açık ve şifreli metine bağlılığının kriptanaliz için faydalı olmayacak kadar karmaşık olması demektir. Yani şifreleme sistemini tanımlayan eşitliklerin doğrusal olmaması ve karışık olması sağlanmalı böylece şifreleme algoritmasından anahtarı bulmanın imkânsız olması gerekir [1].

Karıştırma ve yayılma özellikleri dinamik sistemlerin sahip olduğu özelliklerdir. Kaotik sistemlerin başlangıç koşulları ve/veya kontrol parametrelerine bağımlılığı bir kaotik sistemden üretilen yörüngeler boyunca yayılma özelliğini sağlar. Başka bir ifade ile herhangi bir yörünge üzerinde alınan her bir değer başlangıç koşulları veya kontrol parametrelerine bağımlıdır. Başlangıç koşulları ve/veya kontrol parametrelerindeki en ufak bir değişiklik ile tamamen farklı yörüngeler oluşacağından bu bağımlılık çok güçlüdür. Sonuç olarak kaotik sistemler başlangıç koşulları ve/veya kontrol parametrelerine bağımlılığı yayılma özelliğine sahiptir [5].

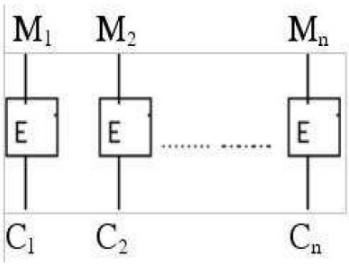
Kaotik sistemlerin ergodiklik özelliği kaotik yörüngenin uzun vadeli davranışının başlangıç koşulları veya kontrol parametrelerine bağımlılığını ortaya koymaktadır. Buradan bir kaotik sistemden üretilen yörüngelerin bir kümesi ile istatistikî olarak başlangıç koşulları ve/veya kontrol parametrelerinin tam değerlerinin çıkarılmasının mümkün olmadığı görülebilinir. Sonuç olarak kaotik sistemler karıştırma özelliğini göstermedir [5].

Özetleyecek olursak kaotik sistemlerin başlangıç koşullarına ve/veya kontrol parametrelerine duyarlılığı yeni kriptolojik sistemlerin tasarlanmasında kullanılabilir.

3. Blok Şifreleme Algoritmaları

Blok şifreleme algoritmaları birçok uygulamada kullanılan simetrik şifreleme algoritmaları için temel birleşenlerden biridir. Blok şifreleme algoritmaları açık metinleri ardışık bloklara böler ardından her bloğu şifreleyerek şifreli metin bloklarına dönüştürmektedir. Şekil 1'de bir blok şifreleme sistemi şematik olarak gösterilmiştir. Şekilden görülebileceği gibi $M_1, M_2, \ldots, M_n$ her biri k bitten oluşan açık metinlerin bloklarını göstermektedir. Benzer şekilde $C_1, C_2, \ldots, C_n$ ise açık metin bloklarına karşılık gelen şifrelenmiş metin bloklarını göstermektedir. Şekilde E şifreleme algoritmasını temsil etmektedir. Çoğu blok şifre sistemlerinde blok uzunluğu 64 bittir. İşlemcilerin hızı arttıkça blok uzunluğu da artabilmektedir. Son yıllarda üretilen şifreleme sistemlerinde 128 bit blok uzunluğu kullanılmaktadır [1].

Bir blok şifreleme sisteminde, şifreli metin bloklarından birinin kaybolması, diğer blokların deşifre işleminde bir yanlışlığa neden olmaz. Bu blok şifreleme sistemlerinin en büyük avantajıdır. Blok şifre sistemlerinin en büyük dezavantajı ise şifreli metindeki birbirinin aynısı olan blokların, açık metinde de birbirinin aynı olmasıdır.



Şekil 1: Blok şifreleme sisteminin genel görünümü.

4. Önerilen Algoritma

Çalışmada önerilen yeni blok şifreleme algoritmasında kaotik sistemler kullanılarak oluşturulmuş dinamik yer değiştirme kutularını (Substitution Box, S-Box) temel alan bir tasarım mimarisi benimsenmiştir. Bu yüzden öncelikle S-Box oluşturmak için kullanılan algoritma açıklanmış ardından oluşturulan dinamik S-Box'lar kullanılarak blok şifreleme algoritmasının nasıl tasarlanacağı açıklanmıştır.

4.1. S-Box Tasarım Algoritması

S-Box DES, IDEA, AES gibi geleneksel blok şifreleme sistemlerindeki karıştırma özelliğini sağlayan doğrusal olmayan tek birleşendir. Bu yüzden güçlü şifreleme sistemlerinin tasarlanması için kriptolojik özellikleri iyi olan S-Box'ların tasarlanması gerekmektedir [6].

Literatürde S-box tasarımları için cebirsel teknikleri temel alan, sözde rasgele tabanlı veya sezgisel tabanlı yöntemler gibi birçok yöntem önerilmiştir. Bu yöntemlerden en popüleri AES şifreleme algoritmasında da kullanılan ters dönüşüm yöntemidir [7, 8]. Ancak son zamanlarda geliştirilen kriptanaliz yöntemlerinden cebirsel saldırı teknikleri bu tasarımlar için önemli bir tehdit oluşturmaktadır [9–14]. Bu yüzden cebirsel saldırılara karşı alternatif olabilecek yeni yöntemler araştırılmalıdır. Kaos tabanlı tasarımlar da modern şifreleme sistemlerinde kullanılan katı cebirsel teknikleri temel alan tasarımlara alternatif olmaya aday tasarımlardır.

Matematiksel olarak *n x n* boyutunda bir S-Box GF(2) üzerinde $S:\{0,1\}^n \rightarrow \{0,1\}^n$ şeklinde doğrusal olmayan bir dönüşümdür. n x n boyutunda S-Box'lar oluşturmak için kullanılan algoritma kaotik sistemin çıkışını 0 ile 2^n arasındaki sayılara dönüştürerek S-Box tasarımını gerçekleştirmektedir. Algoritmanın çalışması adım adım aşağıda açıklanmıştır. Ayrıca sözde kodu tablo 1'de verilmiştir.

Adım 1. Belirlenen başlangıç koşulları ve kontrol parametreleri için kaotik sistemin çıkışı hesaplanır.

Adım 2. Hesaplanan çıkış değeri $A,y_0y_1y_2y_3y_4y_5$ biçimindedir ve S-Box tablosunun hücreleri virgülden sonraki 6 dijit kullanılarak hesaplanmaktadır.

Adım 3. Her adımda kaotik sistemin çıkışından belirlenen 6 dijit içerisinden 3 dijit seçilerek işleme devam edilir bu seçim aşağıdaki şekilde yapılır.

$$y_0y_1y_2 \rightarrow y_1y_2y_3 \rightarrow y_2y_3y_4 \rightarrow y_3y_4y_5 \rightarrow y_4y_5y_0 \rightarrow y_5y_0y_1 \rightarrow y_0y_1y_2$$

Adım 4. $y_py_qy_r$ şeklinde 3 dijit seçildikten sonra bu üç dijitin oluşturduğu decimal değerin 2^n'e göre kalanı (modu) hesaplanarak 0 ile 2^n arasındaki sayılara dönüştürülür.

Adım 5. Elde edilen sayı tabloda mevcut değilse tabloya eklenir. Aksi takdirde adım 1'e gidilerek yeni bir değer hesaplanır ve işleme devam edilir.

Adım 6. Tablodaki tüm hücrelerin değerleri hesaplanıncaya kadar adım 1'den işleme devam edilir.

4.2. Şifreleme ve Şifre Çözme Algoritması

Önerilen şifreleme algoritmasının detayları aşağıda adım adım açıklanmıştır. Detaylı mimari için [15] incelenebilir.

Adım 1. Şifrelenecek *m* mesajı *l* byte (burada *l*=32 seçilmiştir) uzunluğunda bloklara (B_j) bölünür. Eğer blok uzunluğu *l*'den küçük ise bloğun sonuna 0 eklenir.

Adım 2. Bölüm 4.1'de açıklanan algoritma kullanılarak 32 tane 8 x 8 boyutunda S-Box üretilir. Farklı S-Box'lar üretmek için seçilen kaotik haritanın başlangıç koşulu veya kontrol parametreleri değiştirilebilinir.

Adım 3. Her bir bloğun S-Box'lar kullanılarak karıştırılması sağlanır. Ardından sola kaydırma işlemi gerçekleştirilir. Bu işlem *l*-1 defa tekrarlanır. Şifreleme mimarisi görsel olarak şekil 2'de gösterilmiştir.

Adım 4. $C_j = c_0 \oplus c_1 \oplus \ldots \oplus c_{l-1}$ hesaplanarak bloğun şifrelenmesi işlemi tamamlanır.

Şifre çözme işlemi de şifreleme sürecine benzer şekilde yapılır. Tek fark sola kaydırma işlemleri yerine sağa kaydırma yapılır. Yer değiştirme işlemleri için ise S-Box'ların tersi alınır.

5. Performans ve Güvenlik Analizleri

Güvenli blok şifreleme sistemleri geliştirmek için kriptolojik olarak güçlü S-Box tasarımlarının yapılması gerektiği daha önce belirtilmişti. Buradan hareketle şifreleme algoritmasının performans ve güvenlik analizleri için S-Box tasarım kriterleri göz önüne alınmıştır.

5.1. S-Box Tasarım Kriterleri

Kriptolojik olarak güçlü S-box'lar tasarlamak için genellikle beş kriter seçilmektedir [16–21]. Bunlar bijektif olma özelliği, doğrusal olmama kriteri, katı çığ kriteri, çıkış bitlerinin bağımsızlık kriteri ve olası giriş/çıkış XOR dağılımıdır.

5.1.1. Bijektif Olma Özelliği

Bir fonksiyon hem bire bir özelliğini hem de örten özelliğini sağlıyorsa bijectif bir fonksiyon olarak adlandırılmaktadır. Önerilen S-Box tasarım algoritmasıyla oluşturulan yapılar bu özelliği sağlamaktadır.

5.1.2. Doğrusal Olmama Kriteri

f(x) boolean fonksiyonun doğrusal olmaması Walsh spektrumuyla gösterilmektedir.

$$N_f = 2^{n-1}\left(1 - 2^{-n} \max_{\omega \in GF(2^n)} \left|S_{(f)}(\omega)\right|\right) \quad (1)$$

Walsh spektrumu aşağıdaki gibi tanımlanabilir.

$$S_{(f)}(\omega) = \sum_{\omega \in GF(2^n)} (-1)^{f(x) \oplus x \cdot \omega} \quad (2)$$

5.1.3. Katı Çığ Kriteri

Katı çığ kriteri ilk olarak Webster ve Tavares tarafından yayınlanmıştır [18]. Fonksiyon katı çığ kriterini sağlıyorsa tek bir giriş bitinde değişiklik olduğunda çıkış bitlerinin her birinin yarısının değişmesi olasılığı anlamına gelmektedir. Verilen S-kutusunun tamamının katı çığ kriterini sağlayıp sağlamadığını tespit etmek için etkili bir metot [14]'da gösterilmiştir.

Tablo 1: S-Box tasarım algoritması sözde kodu

```
// S-Box'ın tüm elemanlarına başlangıçta -1 atanır
tablo[2n][2n]=-1
i=0, j=0, p=0, q=1, r=2;
while(i<2n)
{
      while(j<2n)
      {
            data=-1
            while(data tabloda mevcutsa)
            {
                  y=f(x)    //y=A.y0y1y2y3y4y5
                  x=y
                  data=ypyqyr mod (2n)
                  p=p+1(mod 6)
                  q=q+1(mod 6)
                  r=r+1(mod 6)
            }
            tablo[i][j]=data
            j=j+1
      }
      i=i+1;        j=0;
}
```

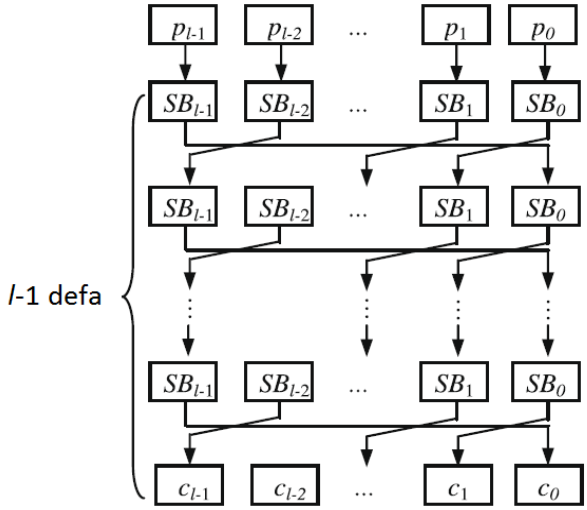
5.1.4. Çıkış Bitlerinin Bağımsızlık Kriteri

Bu kriter de ilk olarak Webster ve Tavares tarafından gösterilmiştir [18]. Şifreleme sisteminin güvenliği için gerekli olan diğer bir özelliktir. Tekbir açık metin bitlerinin tersiyle üretilen çığ vektörlerinin kümesi için tüm çığ değişkenleri çiftlerinin bağımsız olması anlamına gelmektedir. Çığ değişken çiftleri arasındaki bağımsızlığın derecesini ölçmek için çiftler arasındaki korelasyon katsayı hesaplanmaktadır. Webster ve Tavares çalışmalarında S-Box'un iki çıkış bitlerinin boolean fonksiyonları olan f_j ve f_k BIC kriterini sağlıyorsa $f_j \oplus f_k$ ($j \neq k$, $1 \leq j, k \leq n$) nında doğrusal olmama ve katı çığ kriterlerini sağlamalıdır.

5.1.5. Olası Giriş/Çıkış XOR Dağılımı

Biham ve Shamir bir S-Box için giriş/çıkış XOR dağılım tablosundaki dengesizlikleri temel alan diferansiyel kriptoanalizi göstermişlerdir [22]. Çıkış değişimleri giriş değişimlerin bilgisinden elde edilebilir ve her bir çıkışın XOR değeri her giriş XOR için eşit olasılıklı olmalıdır. Yani eğer S-Box giriş/çıkış olasılık dağılımında kapalı ise S-Box'ın diferansiyel kriptoanalize karşı dirençlidir. Verilen bir f haritası için diferansiyel yaklaşım olasılığı diferansiyel dayanıklılık ölçülerek aşağıdaki gibi hesaplanır.

$$DP_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\#\{x \in X \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^m} \right) \quad (5)$$



Şekil 2: Blok şifreleme mimarisi.

5.2. Performans Karşılaştırmaları

Son zamanlarda Wang ve diğerleri [15] kaotik Tent haritasını temel alarak oluşturdukları dinamik S-Box'ları kullanan bir blok şifreleme algoritması önermişlerdir. Karşılaştırma yapabilmek için bu çalışmada önerilen S-Box tasarımı içinde kaotik Tent harita temel alınarak dinamik S-Box'lar üretilmiştir.

Doğrusal olmama ölçütü bakımından Wang ve diğerlerinin çalışmasında ortalama değer 104 civarında iken bizim çalışmamızda ise bu değer 105 civarındadır.

Katı çığ kriteri için ise Wang ve diğerleri değerlerin 0.485 ile 0.515 arasında değiştiğini göstermişlerdir. Bizim çalışmamızda ise minimum ve maksimum değerler 0.375 ile 0.601 arasında değişmektedir. Ancak ortalama değere bakıldığında 0.5002 ile ideal değer olan 0.5 değerine çok yakın olduğu görülmektedir.

Olası giriş/çıkış XOR dağılımı ölçütü bakımından karşılaştırıldığında ise Wang ve arkadaşlarının çalışmasında maksimum değerlerin 10 ile 12 arasında değiştiği görülmektedir. Bizim çalışmamızda ise maksimum değerler 8 ile 10 arasında değişmektedir.

6. Sonuçlar

Bu çalışmada dinamik S-Box'ları kullanan yeni bir blok şifreleme algoritması önerilmiştir. Literatürdeki benzer çalışmalarla kıyaslandığında kaotik S-Box üreteç algoritması kriptolojik olarak daha güçlüdür. Ayrıca önceki çalışmalarda önerilen algoritmaların kriptolojik olarak güçlü olması önemli ölçüde seçilen kaotik sisteme bağımlı iken bu çalışmada önerilen dinamik S-Box tasarım algoritmasında ise farklı kaotik sistemler için bile başarılı sonuçların elde edildiği gözlenmiştir.

Literatürdeki birçok kaos tabanlı S-Box tasarım algoritması incelendiğinde kaotik yörüngenin kullanılarak tablonun oluşturulmasının yanı sıra satır ve sütün bazında döndürme, başka bir kaotik sistem yardımıyla karıştırma, optimizasyon süreçlerinden faydalanma gibi çeşitli yöntemlerinde kullanıldığı görülmektedir. Bu tip ek işlemler kriptolojik özelliklerin artırılması bakımından olumlu sonuçlar doğurmasına rağmen pratik uygulanabilirlik bakımından şifreleme süresinin artmasına sebep olduğu için önemli bir kısıt olarak ortaya koyulmaktadır. Bu çalışmada önerilen algoritmanın bu tip ek işlemlere ihtiyaç duymaması geliştirilen yöntemin önemli avantajlarından biridir.

İlerideki çalışmalarda hem dinamik S-Box oluşturma algoritmasının hem de blok şifreleme mimarisinin daha fazla nasıl geliştirileceği araştırılacaktır.

7. Kaynakça

[1] Paar, C. Pelzl, J., Understanding Cryptography: A Textbook for Students and Practitioners, Springer, 2010.

[2] Amigo J. M., Kocarev L., Szczapanski J., Theory and practice of chaotic cryptography, Physics Letters A, 366:211-216, 2007.

[3] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers. IEEE Trans Circ Syst—I, 48(2):163–169, 2001

[4] Alvarez, G. Li, S., Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, International Journal of Bifurcation and Chaos,16: 2129-2151, 2006

[5] Arroyo D., Framework for the analysis and design of encryption strategies based on discrete time chaotic dynamical system, Instituto de Fı´sica Aplicada, 2009

[6] T. Cusick, P. Stanica, Cryptographic Boolean Functions and Applications, Academic Press, 2008.

[7] K. Nyberg, Differentially uniform mappings for cryptography, Proceedings of Eurocrypt'93 Lecture Notes in Computer Science Springer Berlin 765 (1994) 55-64.

[8] J. Daemen, V. Rijmen, AES Proposal: Rijndael, First Advanced Encryption Conference, California, 1998.

[9] G. Bard, Algebraic Cryptanalysis. Springer-Verlag, 2009.

[10] N. Courtois, G. Bard, Algebraic Cryptanalysis of the Data Encryption Standard. Lecture Notes in Computer Science 4887 (2007) 152-169.

[11] M. Youssef, S. E. Tavares, G. Gong, On Some probabilistic approximations for AESlike s-boxes. Discrete Mathematics 306 (2006) 2016-2020.

[12] L. Jing-mei, W. Bao-dian, C. Xiang-guo, W. Xin-mei, Cryptanalysis of Rijndael S-box and improvement, Applied Mathematics and Computation 170 (2005) 958-975.

[13] M. Youssef, S. E. Tavares, Affine equivalence in the AES round function, Discrete Applied Mathematics 148 (2005) 161-170.

[14] Y. Nawaz, K. C. Gupta, G. Gong, Algebraic Immunity of S-Boxes Based on Power Mappings: Analysis and Construction. IEEE Transactions on Information Theory, 55-9 (2009) 4263-4273.

[15] Wang Y, Wong K, Liao X, Xiang T. A block cipher with dynamic S-boxes based on tent map. Commun Nonlinear Sci Numer Simulat, 14:3089–3099, 2009

[16] M. Dawson, S. Tavares, Adv Cryptol Proc Eurocrypt_91. Lecture Notes Computer Sci, 352–367, 1991

[17] Detombe J, Tavares S. Constructing large cryptographically strong S-boxes. In: Advances in cryptology: Proc. of crypto'92. Lecture notes in computer science, 1992.

[18] Webster, S. Tavares, On the design of S-boxes, In: Advances in cryptology: Proc. of crypto'85. Lecture notes in computer science, 1986 pp. 523–534.

[19] C. Adams, S. Tavares, Good S-boxes are easy to find, In: Advances in cryptology: Proc. of crypto'89. Lecture notes in computer science, 1989. p. 612–615.

[20] J. Detombe, S. Tavares, Constructing large cryptographically strong S-boxes, In: Advances in cryptology: Proc. of crypto'92. Lecture notes in computer science, 1992.

[21] M. Dawson, S. Tavares, An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks, In: Advances in cryptology: Proc. of eurocrypt'91. Lecture notes in computer science, 1991. pp. 352–367.

[22] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology, 4 (1991) 3-72.