Kaos Tabanlı S-Box Üreteçlerinin Güçlendirilmesi için Yeni Bir Algoritma
A Novel Algorithm for Strengthening of Chaos Based S-Box Generators

Fatih ÖZKAYNAK[1], Ahmet Bedri ÖZER[2]

[1]Müühendislik Fakültesi Bilgisayar Mühendisliği Bölümü
Tunceli Üniversitesi
ozkaynak_fatih@hotmail.com

[2]Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü
Fırat Üniversitesi
bedriozer@firat.edu.tr

Özet

Kaos ve kriptoloji bilimleri arasındaki güçlü ilişkiden yararlanılarak birçok kaos tabanlı S-Box üreteç algoritması önerilmiştir. Ancak bu algoritmaların güçlü kriptografik özelliklere sahip olması seçilen kaotik sistemlere bağımlıdır. Bu çalışmada önerilen algoritma ile kaotik sistemlere olan bağımlılık ortadan kaldırılmıştır. Analiz sonuçları önerilen algoritmanın güvenli iletişim için oldukça güvenilir bir sistem olduğunu göstermiştir.

Abstract

Many chaos based S-Box generator algorithms have been proposed utilizing a strong relationship between the science of chaos and cryptography. However these algorithms have a strong cryptographic features are dependent on the selected chaotic system. The proposed algorithm in this study the dependence of chaotic systems is eliminated. The results of the analysis show that the proposed algorithm is a highly reliable system suitable for secure communication.

1. Giriş

Kaos teorisi oldukça basit matematiksel modellere sahip olmasına rağmen karmaşık bir davranış göstermektedir. 1980'lerden beri kaosun temel özelliklerinden yararlanılarak birçok güçlü kriptolojik sistem önerilmiştir. Kaosun modern kriptolojideki uygulama alanlarından biride S-Box üreteçleridir. Literatürde birçok kaos tabanlı S-Box üreteç algoritması bulunmaktadır [1–5]. Ancak bu algoritmalar incelendiğinde sistemin güçlü kriptolojik özelliklere sahip olması seçilen kaotik sisteme bağımlıdır. Yani kaotik sistem (önerilen algoritma) ne kadar düzgün bir rastgele dağılım gösteriyorsa kaos tabanlı S-Box o kadar güçlüdür [5]. Ayrıca son zamanlarda birçok kaos tabanlı şifreleme sisteminin kriptoanalizi yapılmış ve çeşitli saldırı teknikleri geliştirilmiştir [6–14]. Saldırıların temel dayanak noktası incelendiğinde kaotik sistemlerin sahip olduğu temel özelliklerin analizinden yola çıkıldığı görülmüştür [15, 16]. Buda kaotik sistemlere olan bağımlılığın ortadan kaldırılması problemini ortaya koymuştur.

Bu çalışmada literatürdeki bazı kaos tabanlı S-Box üreteçleri ele alınmıştır. Önerilen algoritma ile değiştirilen S-Box'ların kaotik sistemlere olan bağımlığı ortadan kaldırılmıştır. Çalışmada beş farklı kaos tabanlı S-Box üreteci incelenmiştir. Değiştirilmiş her bir S-Box'un performans analizleri karşılaştırmalı olarak yapılmıştır.

Çalışmanın geri kalan kısmı aşağıdaki gibi organize edilmiştir. İkinci bölümde çalışmada analiz edilen S-Box üreteçleri kısaca tanıtılmıştır. Üçüncü bölümde önerilen algoritma detaylı olarak açıklanmıştır. Dördüncü bölümde önerilen algoritma ile elde edilen S-Box'ların performans analizleri yapılmıştır. Son bölümde elde edilen sonuçlar verilerek gelecek çalışmalar için önerilerde bulunulmuştur.

2. Analiz Edilen Kaos Tabanlı S-Box Üreteçleri

Tang ve arkadaşları [1] S-box üreteci için iki aşamalı bir algoritma önermiştir. İlk aşamada kaotik bir haritanın iterasyonları sonucunda oluşan reel değerli yörüngeden 8-bit binary rastgele değişkenler elde edilmiş ve $0\text{-}2^n$ aralığındaki tamsayı değerlerine dönüştürülerek tablo oluşturulmuştur. İkinci adımda ise iki boyutlu Baker Map aracılığıyla tablonun karıştırılması sağlanmıştır.

Tang ve Liao [2] ise üç aşamalı bir algoritma önermişlerdir. İlk aşamada keyfi olarak oluşturulmuş anahtar gibi bir K başlangıç dizisi elde edilmiştir. $K=X_0=\{1,2,\ldots,2^n\}$. İkinci aşamada kaotik Skew Tent Map kullanılarak X_0 başlangıç dizisinin iterasyonları sonucunda $\{X\}$ tamsayı dizisi elde edilmiştir. Son olarak $\{X\}$ dönüştürülerek S-Box elde edilmiştir.

Chen ve arkadaşları [3] iki boyutlu Baker Map haritasını üç boyutlu olarak genelleştirerek yeni bir üreteç önermişlerdir. S-Box için üç aşamalı bir algoritma kullanmışlardır.

Chen [4] kaotik Baker ve Chebyshev haritalarını karıştırarak yeni bir yaklaşım önermiştir. Chen önerdiği üreteçte sadece kaotik haritaların karıştırılmasıyla yetinmemiş tasarım aşamasında simulated annealing algoritmasından da yararlanılmıştır.

Özkaynak ve Özer [5] kaotik Lorenz sistemini temel alan bir S-Box üreteci önermişlerdir. İki aşamalı bir algoritma kullanılmıştır. İlk aşamada Lorenz sistem yörüngesinden örnekleme yapılarak bir tablo oluşturulmuştur. İkinci aşamada ise kullanılan algoritma ile karıştırma işlemi sağlanmıştır.

3. Önerilen Algoritma

Kaosun ergodiklik, rastgele benzeri davranış göstermesi ve başlangıç şartlarına bağımlılık gibi özelliklerinden faydalanılarak kriptolojik sistemlerin geliştirilmesi ne kadar mantıklı ise sistemin güvenilirliğinin sadece kaotik sisteme bağımlı olması o kadar problemlidir. Bu problemi ortadan kaldırabilmek için kaos başlangıçta rastgelelik kaynağı olarak düşünülmeli ama belirli kriptolojik özellikleri garanti edebilmek için daha sonra çeşitli algoritmalar uygulanmalıdır.

Aslında bu bakış açısıyla incelenen problem kaosla elde edilmiş veriler üzerinde güçlü kriptolojik özellikleri garanti edecek dizilimlerin araştırıldığı bir problemidir [17–19]. En uygun dizilimi elde edebilmek için aşağıda detaylı olarak açıklanan algoritma kullanılmıştır.

Çalışmada *N x N* boyutunda S-Box üreteçleri üzerinde değişiklik yapacak algoritma aşağıda detaylı olarak verilmiştir.

- İşlem yapılan hücre binary olarak kodlanır. (bit sayısı = *N*)
- Her bir hücrenin kaç hücreyle komşu olduğu belirlenir. *A* komşu hücre sayısını göstersin.
- Komşuların sırası saat yönünde ilerlenerek belirlenir.
- Hücrenin *i*. komşusu *(N-i)* biti farklı olacak şekilde değiştirilir. Bu işlem *A* defa tekrarlanır.
- Değiştirmeye en anlamsız bitten başlanır. Bit değeri 1 ise 0; 0 ise 1 yapılır.
- Tüm hücreler için işlem yapılıncaya kadar devam edilir.

Algoritmanın rahat anlaşılabilmesi için *4 x 4* boyutumda küçük bir S-Box üzerinde algoritmanın çalışması gösterilmiştir. Örnek S-Box tablo 1'de verilmiştir. 0. satır 0. sütun hücresinin değeri 8'dir. Bu hücrenin değerleri 1 ve 11 olan iki komşusu bulunmaktadır. Benzer şekilde 2. satır 2. sütun hücresinin değeri 14'dür. Dört komşusu bulunmaktadır. Koşularının değerleri sırasıyla (saat yönünde) 0, 15, 5 ve 6'dir. S-Box 4 x 4 boyutunda olduğu için her bir hücrenin binary karşılığı 4 bit şeklinde kodlanır.

İlk hücre için algoritma çalıştırılırsa yapılan işlemler aşağıda gösterilmiştir. İlk hücre için iterasyon tamamlandıktan sonra oluşan yeni durum tablo 2'de verilmiştir.

- 8=*1000 (ilk hücrenin binary karşılığı)*
- *Komşularının sayısı A=2*
- *Birinci komşu 4–1=3 bit yer değiştirilir. Hücrenin yeni değeri 15=1111 olacaktır. İçeriği 15 olan hücre ile yer değiştirir.*
- İkinci komşu 4–2=2 bit yer değiştirir. Hücrenin yeni değeri 11=1011 olacaktır. Hücrenin mevcut değeri 11 olduğundan yer değiştirme olmaz.

Tablo 1: 4 x 4'lük örnek S-Box

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

Tablo 2: Algoritmanın bir iterasyon çalıştırılması sonucunda oluşan yeni S-Box

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

4. S-Box Performans Ölçütleri

Kriptolojik olarak güçlü S-Box'lar tasarlamak için genellikle beş özellik seçilmektedir. Bunlar birebir özelliği, doğrusal olmama, katı çığ kriteri (SAC), çıkış bitlerinin bağımsızlık kriteri (BIC) ve olası giriş/çıkış XOR dağılımıdır.

4.1. Birebir Özelliği

Birebir özelliğini kontrol etmek için [20]'de bir metot geliştirilmiştir. Eğer f_i boolean fonksiyonu $wt(\sum_{i=1}^{n} a_i f_i) = 2^{n-1}$ şartını sağlıyorsa birebirdir. Burada $a_i \in \{0,1\}$ $(a_1, a_2, ..., a_n) \neq (0,0,...,0)$ ve $wt()$ hamming ağırlığıdır. Önerilen algoritma kullanılarak değiştirilmiş bütün S-Box'lar birebir özelliğini sağlamaktadır.

4.2. Doğrusal Olmama Özelliği

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

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

Walsh spektrumu aşağıdaki gibi tanımlanabilir.

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

Burada $\omega \in GF(2^n)$ ve $x \cdot \omega$ ifadesi aşağıda verildiği gibi x ve ω'nin nokta çarpımını göstermektedir.

$$x \cdot \omega = x_1 \cdot \omega_1 \oplus \ldots \oplus x_n \omega_n \quad (3)$$

Önerilen algoritma kullanılarak değiştirilmiş S-Box'ların doğrusal olmama ölçütleri tablo 3'de verilmiştir. Tablodan görüleceği gibi [1] numaralı çalışmada önerilen S-Box haricinde değiştirilmiş S-Box'ların doğrusal olmama ölçütü daha iyidir.

Tablo 3: Doğrusal olmama ölçütlerinin karşılaştırılması

S-Box	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**Ortalama**
Ref. [1]	103	109	104	105	105	106	104	103	104.875
Önerilen Ref. [1]	103	104	103	104	101	105	108	109	104.625
Ref. [2]	104	99	105	101	102	100	106	105	102.75
Önerilen Ref. [2]	104	107	102	105	103	105	97	104	103.375
Ref. [3]	106	102	106	106	100	104	100	100	103
Önerilen Ref. [3]	105	106	104	102	103	107	101	108	104.5
Ref. [4]	104	106	106	104	102	104	102	104	104
Önerilen Ref. [4]	104	104	101	105	104	104	105	106	104.125
Ref. [5]	104	100	106	102	104	102	104	104	103.25
Önerilen Ref. [5]	102	105	99	103	105	106	103	104	103.375

4.3. Katı Çığ Kriteri

Katı çığ kriteri ilk olarak Webster ve Tavares tarafından yayınlanmıştır [21]. Fonksiyon katı çığ kriterini sağlıyorsa tek bir giriş bitinde değişiklik olduğunda çıkış bitlerinin her birinin yarısının değişmesi olasılığı anlamına gelmektedir. Verilen S-Box'ın tamamının katı çığ kriterini sağlayıp sağlamadığını tespit etmek için etkili bir metot [22]'de gösterilmiştir. Bu metot kullanılarak önerilen S-Box ve diğer S-Box'lar için bağımlılık matrisi ve ortalama değerler hesaplanmıştır.

Bağımlılık matrisi için hesaplanan minimum, maksimum ve ortalama değerler tablo 4'de gösterilmiştir. [1, 4, 5] numaralı çalışmalardan daha iyi değerler elde edilmiştir. Diğer çalışmalar içinse çok yakın sonuçlar elde edilmiştir.

4.4. Çıkış Bitlerinin Bağımsızlık Kriteri

Bu kriter de ilk olarak Webster ve Tavares tarafından gösterilmiştir [21]. 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.

Önerilen algoritma ile değiştirilen S-Box'lar için elde edilen sonuçlar Tablo 5'de gösterilmiştir. Bu kriter için minimum değerlerin yüksek olması istenmektedir. Önerilen algoritma ile değiştirilen S-Box'lar için hesaplanan değerlerde [2] numaralı çalışma dışındakilerde daha düşük değerler hesaplanmıştır. Maksimum değerler ise incelenen S-Box'lara çok yakın değerler elde edilmiştir.

Tablo 4: Katı çığ kriteri için hesaplanan değerler

S-Box	**Min**	**Mak.**	**Ort.**
Ref. [1]	0.398438	0.570313	0.496582
Önerilen Ref. [1]	0.414063	0.585938	0.500488
Ref. [2]	0.398438	0.578125	0.506592
Önerilen Ref. [2]	0.429688	0.601563	0.510986
Ref. [3]	0.421875	0.609375	0.5
Önerilen Ref. [3]	0.429688	0.59375	0.500488
Ref. [4]	0.375	0.609375	0.498047
Önerilen Ref. [4]	0.40625	0.609375	0.499756
Ref. [5]	0.421875	0.59375	0.504883
Önerilen Ref. [5]	0.414063	0.601563	0.5

Tablo 5: Çıkış bitleri bağımsızlık kriteri için hesaplanan değerler

S-Box	Min	Mak	Karesel Sapma
Ref. [1]	95	102.964	3.38571
Önerilen Ref. [1]	93	102.25	3.9154
Ref. [2]	96	102.786	3.26625
Önerilen Ref. [2]	96	103.536	2.78365
Ref. [3]	98	103.143	2.89968
Önerilen Ref. [3]	95	103	3.29502
Ref. [4]	100	103.286	2.21774
Önerilen Ref. [4]	90	103.75	3.7093
Ref. [5]	100	103.714	2.11891
Önerilen Ref. [5]	94	103.107	3.78285

4.5. Olası Giriş/Çıkış XOR Dağılımı

Biham ve Shamir bir S-Box için giriş/çıkış XOR dağılım tablosundaki dengesizlikleri temel alan diferansiyel kriptoanalizi göstermişlerdir [23]. 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.

$$DP_f = \max_{\Delta x \neq 0, \Delta y} \left(\frac{\#\{x \in X \mid f(x) \oplus f(x \oplus \Delta x) = \Delta y\}}{2^m} \right) \qquad (4)$$

Burada X olası tüm giriş değerlerinin kümesidir. 2^m ise elamanların sayısıdır. Önerilen algoritma ile değiştirilen S-Box'lar için diferansiyel yaklaşım tabloları hesaplanmıştır. Her bir S-Box için hesaplanan değerler verilmemiştir. Tablolardaki maksimum değerler karşılaştırmalı olarak tablo 6'da gösterilmiştir. Tablo 6'dan görülebileceği gibi [2] numaralı çalışmayla aynı diğerlerine ise yakın değerler elde edilmiştir.

5. Sonuçlar

Bu çalışmada kaos tabanlı S-Box üreteçlerinin kriptolojik özelliklerinin geliştirilmesi için yeni bir yöntem önerilmiştir. Önerilen yöntem literatürdeki kaos tabanlı S-Box üreteçleri kullanılarak kriptografik olarak güçlü olup olmadığı test edilmiştir. S-Box performans analiz ölçütleri önerilen yöntemle başarılı üreteçler elde edildiğini göstermiştir.

Literatürde birçok kaos tabanlı şifreleme algoritması mevcuttur. Ancak önerilen sistemlerin çoğunun kriptoanalizi noktasında eksiklikler bulunmaktadır. Analizi yapılan sistemlerin ise kriptolojik olarak zayıflıkları görünmektedir. Birçok kriptoanalizin çıkış noktası ise kaotik sistemlerin analizidir.

Tablo 6: Diferansiyel yaklaşım tablosu maksimum değerlerinin karşılaştırılması

S-Box	Maksimum
Ref. [1]	10
Önerilen Ref. [1]	14
Ref. [2]	14
Önerilen Ref. [2]	14
Ref. [3]	14
Önerilen Ref. [3]	16
Ref. [4]	10
Önerilen Ref. [4]	14
Ref. [5]	10
Önerilen Ref. [5]	14

Bu çalışmanın katkısı şifreleme sisteminin sadece kaotik sistemlere olan bağımlılığını ortadan kaldırmasıdır. Önerilen algoritma ile kaosu rastgelelik kaynağı olarak kullanan hibrit bir yöntem önerilmiştir. İleride yapılacak çalışmalarda farklı algoritmalar kullanılarak farklı tasarımlar yapılabilir.

6. Kaynaklar

[1] Guoping Tang, Xiaofeng Liao, Yong Chen, A novel method for designing S-boxes based on chaotic maps, Chaos, Solitons and Fractals 23 (2005) 413–419

[2] Guoping Tang, Xiaofeng Liao, A method for designing dynamical S-boxes based on discretized chaotic map, Chaos, Solitons and Fractals 23 (2005) 1901–1909

[3] Guo Chen, Yong Chen, Xiaofeng Liao, An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps, Chaos, Solitons and Fractals 31 (2007) 571–579

[4] Guo Chen, A novel heuristic method for obtaining S-boxes, Chaos, Solitons and Fractals 36 (2008) 1028–1036

[5] Fatih Özkaynak, Ahmet Bedri Özer, A method for designing strong S-Boxes based on chaotic Lorenz system, Physics Letters A 374 (2010) 3733–3738

[6] Rhouma Rhouma, Safya Belghith, Cryptanalysis of a spatiotemporal chaotic cryptosystem, Chaos, Solitons and Fractals 41 (2009) 1718–1722

[7] Ercan Solak, Cahit Çokal, Cryptanalysis of a cryptosystem based on discretized two-dimensional chaotic maps, Physics Letters A 372 (2008) 6922–6924

[8] Ercan Solak, Cahit Cokal, Cryptanalysis of a cryptosystem based on discretized two-dimensional chaotic maps, Physics Letters A 372 (2008) 6922–6924

[9] Rhouma Rhouma, Safya Belghith, Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem, Physics Letters A 372 (2008) 5790–5794

[10] G. Álvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a discrete chaotic cryptosystem using external key, Physics Letters A 319 (2003) 334–339
[11] G. Alvarez, F. Montoya, M. Romera, G. Pastor, Cryptanalysis of a chaotic secure communication system, Physics Letters A 306 (2003) 200–205
[12] Yong Wang, Xiaofeng Liao, Tao Xiang, Kwok-Wo Wong, Degang Yang, Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map, Physics Letters A 363 (2007) 277–281
[13] Chengqing Li, Shujun Li, Gonzalo Alvarez, Guanrong Chen, Kwok-Tung Lo, Cryptanalysis of two chaotic encryption schemes based on circular bit shift and XOR operations, Physics Letters A 369 (2007) 23–30
[14] Ercan Solak, Cahit Cokal, Algebraic break of a cryptosystem based on discretized two-dimensional chaotic maps, Physics Letters A 373 (2009) 1352–1356
[15] Gonzalo Alvarez, Shujun Li, Some Basic Cryptographic Requirements for Chaos-Based Cryptosystems, International Journal of Bifurcation and Chaos 2006,16, 2129-2151
[16] David Arroyo, Gonzalo Alvarez, Veronica Fernandez, Basic Framework for the Cryptanalysis of Digital Chaos-Based Cryptography, Systems, Signals and Devices, 2009. SSD '09. 6th International Multi-Conference
[17] Guden, H., Vakvak, B., Ozkan, B. E., Altıparmak, F., Dengiz, B., 2005, Genel Amaçlı Arama Algoritmaları ile Benzetim Eniyilemesi: En İyi Kanban Sayısının Bulunması, Endüstri Mühendisliği Dergisi, Cilt: 16 Sayı: 1, 2-15.
[18] Simha, R., Carnahan, J., 2001, Nature's Algorithms: Natural and Social Metaphors in Algorithm Design, IEEE Potentials, Vol. 20, No. 2, 21-24.
[19] Holland, J. H., 1975, Adaptation in Natural and Artificial Systems, University of Michigan Press, Ann Arbor.
[20] Jakimoski G, Kocarev L. Chaos and cryptography: block encryption ciphers. IEEE Trans Circuits Syst-I 2001;48(2):163–70.
[21] Webster A, Tavares S. On the design of S-boxes. In: Advances in cryptology proc. Of CRYPTO85. Lecture notes in computer science. 1986. p. 523–4.
[22] Dawson M, Tavares S. An expanded set of S-box design criteria based on information theory and its relation to differential-like attacks. Adv Cryptol Proc Eurocrypt_91. Lecture Notes Computer Sci 1991:352–67.
[23] Biham E, Shamir A. A differential cryptanalysis of DES-like cryptosystems. J Cryptol 1991;4(1):3–72.
[24] Yong Wang, Qing Xie, Yuntao Wu, Bing Du, A Software for S-box Performance Analysis and Test, 2009 International Conference on Electronic Commerce and Business Intelligence