Araştırma Makalesi

Rasgele Seçim Tabanlı Yer Değiştirme Kutularının Performans İyileştirmesi için Son İşlem Algoritmaları

Yaşar Selim Bahceci [1], Fatih Özkaynak*[1]

[1]*Fırat Üniversitesi, Teknoloji Fakültesi, Yazılım Mühendisliği Bölümü, Elazığ, Türkiye*

Anahtar Kelimeler:
Kaos
Kriptoloji
Bilgi Güvenliği

ÖZ

Yer değiştirme kutuları (substitution-box / s-box) önemli bir kriptolojik yapı taşıdır. Bu kriptolojik yapıların tasarımında matematiksel dönüşümleri temel alan tasarım teknikleri özellikle Gelişkin Şifreleme Standardı (Advanced Encryption Standart / AES) olarak bilinen blok şifreleme algoritmasına damgasını vurmuştur. Çünkü AES s-box yapısı en iyi kriptolojik özelliklere sahiptir. Ancak uygulamaya yönelik saldırılar göz önüne alındığında çeşitli zafiyetler ortaya çıkmaktadır. Rasgele seçim tabanlı tasarım tekniklerini temel alan s-box yapışlarının ise kriptolojik özellikleri AES s-box yapısından kötü olmasına rağmen uygulama saldırıları özelinde daha başarılıdır. Bu çalışmanın amacı rasgele seçim tabanlı yer değiştirme kutularının performans iyileştirmesini sağlayacak yöntemleri araştırmaktır. Çalışmada önerilen son işlem algoritması ile rasgele seçim tabanlı tasarımların performans iyileştirmelerinin sağlanabileceği gösterilmiştir. Elde edilen bu sonuçların ileride özellikle uygulamaya yönelik saldırıların engellenmesi için bir karşı önlem olarak önemli katkılar sunacağı düşünülmektedir.

Post-processing Algorithms for Performance Improvement of Substitution Boxes Based on Random Selection

Keywords:
Chaos
Cryptology
Information Security

ABSTRACT

Substitution boxes are an important cryptographic primitive. Design techniques based on mathematical transformations, a design technique of these cryptographic primitives, have played a particularly important role in the block encryption algorithm known as the Advanced Encryption Standard (AES). Because AES substitution box structure has the best cryptographic properties. However, various weaknesses arise when the implementation attacks are considered. Although the cryptographic properties of substitution box structures based on random selection techniques are worse than the AES substitution box structure, they are more successful to prevent implementation attacks. The aim of this study is to investigate the performance improvement algorithms of substitution boxes based on random selection. In this study, it has been shown that performance improvements of substitution boxes based on random selection can be achieved with the proposed post-processing algorithms. These results are thought to make significant contributions in the future, especially as a countermeasure for the prevention of implementation attacks.

***Sorumlu Yazar**

*(ozkaynak@firat.edu.tr) ORCID ID 0000-0003-1292-8490
(yasarselimbahceci@gmail.com) ORCID ID 0000-0002-7567-4961

e-ISSN: XXXXXXXXXXXX
Geliş Tarihi: 21/03/2020; Kabul Tarihi: 05/05/2020

1. GİRİŞ

Bir kriptolojik protokolün sağlaması gereken temel gereksinimler karıştırma ve yayılma özellikleridir. Blok şifreleme algoritmaları özelinde karıştırma özelliğini sağlamak için yer değiştirme kutuları (substitution boxes/s-boxes) olarak adlandırılan doğrusal olmayan dönüşümler kullanılmaktadır (Cusick ve Stanica, 2009; Wu ve Feng, 2016). En basit anlamda s-box yapısı doğrusal olmayan bir fonksiyondur. Literatürde bu doğrusal olmayan fonksiyonların tasarımı için matematiksel, sezgisel ve rasgele seçim tabanlı tasarım teknikleri vardır. En yaygın bilinen tasarım tekniği matematiksel dönüşümleri temel alan tasarım teknikleridir. Matematiksel dönüşümleri temel alan tasarım teknikleri özellikle Advanced Encryption Standart olarak bilinen blok şifreleme algoritmasına damgasını vurmuştur. Çünkü AES s-box yapısı en iyi kriptolojik özelliklere sahiptir (Cusick ve Stanica, 2009; Wu ve Feng, 2016). Ancak bu tasarım tekniklerinin uygulamaya yönelik saldırılar için çeşitli problemlere sebep olabileceği gösterilmiştir. Bu yüzden rasgele seçimleri temel alan tasarım teknikleri giderek popüler olmaya başlamıştır (Açıkkapı ve ark., 2019).

Rasgele seçim tabanlı tasarım teknikleri arasında kaos tabanlı s-box yapıları giderek popüler olmuştur. Bu popülerliğin en önemli sebeplerinden biri kaosun doğrusal olmayan ve tahmin edilemez yapısı olarak gösterilebilir (Kocarey ve Lioan, 2011; Sprott, 2010). Ancak kaos tabanlı tasarımların performans karakteristiklerinin matematiksel tabanlı tekniklere göre kötü olması ciddi bir problemdir (Özkaynak, 2017). Bu çalışmanın amacı bu problemin etkisi azaltacak son işlem algoritmalarını araştırmaktır. Çalışmada önerilen son işlem algoritmasının s-box performans ölçütlerinden biri olan doğrusal olmama özelliğini iyileştirebileceği gösterilmiştir.

Çalışmanın geri kalan kısmı aşağıdaki gibi organize edilmiştir. İkinci bölümde kaos tabanlı s-box literatürü için kısa bir tanıtım verilmiştir. Üçüncü bölümde performans iyileştirmesi için önerilen yöntemin detayları açıklanmıştır. Dördüncü bölümde analiz sonuçları verilmiştir. Son bölümde çalışma özetlenmiş ve ileride yapılabilecek çalışmalar için önerilerde bulunulmuştur.

2. KAOS TABANLI S-BOX YAPILARI

En genel ifade ile bir kriptolojik s-box yapısının tasarımı Denklem 1'de verildiği gibi doğrusal olmayan bire bir ve örten bir fonksiyon tasarımı ile ilişkilidir. Denklem 1'de ifade edildiği gibi s-box büyüklüğüne bağlı olarak 0 ile n arasındaki sayılar yine 0 ile n arasındaki sayılara dönüştürülerek karıştırma özelliğinin sağlanması garanti edilmeye çalışılmaktadır. S-box yapılarının kriptolojik özelliklerini değerlendirmek için fonksiyonun bijektive olmasının yanı sıra doğrusal olmama, giriş çıkış bağımsızlığı, katı çığ kriteri ve diferansiyel kriptanalizle ilişkili olan XOR dağılım tablosu gibi kriterler bulunmaktadır (Cusick ve Stanica, 2009; Wu ve Feng, 2016; Özkaynak, 2019).

Denklem 1: S-Box yapısı tasarımı

$$S(n): [0:n] \rightarrow [0:n]$$

S-box tasarımı blok şifreleme algoritmalarının tarihsel gelişiminde önemli bir rol oynamıştır. Data Encryption Standart (DES) algoritmasında kullanılan s-box yapısının tasarım prensiplerinin açıklanmamış olması, diferansiyel saldırılara karşı dirençli olmadığının gösterilmesi araştırmacıları yeni bir blok şifreleme algoritması tasarım sürecine yönlendirmiş ve 2000'li yılların başında AES algoritması ortaya çıkmıştır. AES algoritmasında kullanılan s-box yapısı Nyberg tarafından indirgenemez polinomlarda ters haritalama yöntemi kullanılarak tasarlanmıştır. DES s-box yapısının problemlerini gideren bu tasarım güçlü matematiksel fonksiyonlara dayandığı için kriptolojik özellikler bakımından herhangi bir zayıflık içermediği görülmüştür. AES s-box yapısının kriptolojik özellikleri Tablo 1'de verilmiştir (Cusick ve Stanica, 2009; Wu ve Feng, 2016).

Tablo 1. AES blok şifreleme algoritması kriptolojik özellikleri

Kriptolojik Özellik	Değer
Doğrusal Olmama (Nonlinearity)	112
Katı Çığ Kriteri (SAC)	0.5
Giriş/Çıkış Bitleri- Nonlinearity	112
Giriş/Çıkış Bitleri- SAC	0.5
XOR Dağılım Tablosu	4

Her ne kadar AES s-box yapısı kriptolojik özellikler bakımından zayıflıklar içermese de kriptanaliz tekniklerinin gelişmesi ve çeşitlenmesi ile çeşitli zayıflıkların olabileceği ortaya koyulmuştur. Bu saldırı tekniklerinden biri uygulamaya yönelik saldırılardır. Bir uygulamaya yönelik saldırı tekniği olan yan kanal saldırıları bu zafiyeti ve rasgele seçim tabanlı s-box tasarımlarının bu zafiyete karşı bir alternatif olabileceğini göstermiştir (Tanyıldızı ve Özkaynak, 2019; Solami ve ark., 2018). Literatürde en etkili rasgele seçim tabanlı s-box yaklaşımlarından biri entropi kaynağı olarak kaotik sistemleri temel alan tasarımlar olmuştur (Yi ve ark., 2019; Naseer ve ark., 2019; Özkaynak, 2020). Çok farklı kaotik sistemler kullanılarak birçok s-box tasarımı önerilmiştir. Her ne kadar kaos tabanlı tasarımlar bir alternatif olma niteliği taşımasına rağmen kriptolojik özelliklerinin matematiksel tabanlı s-box

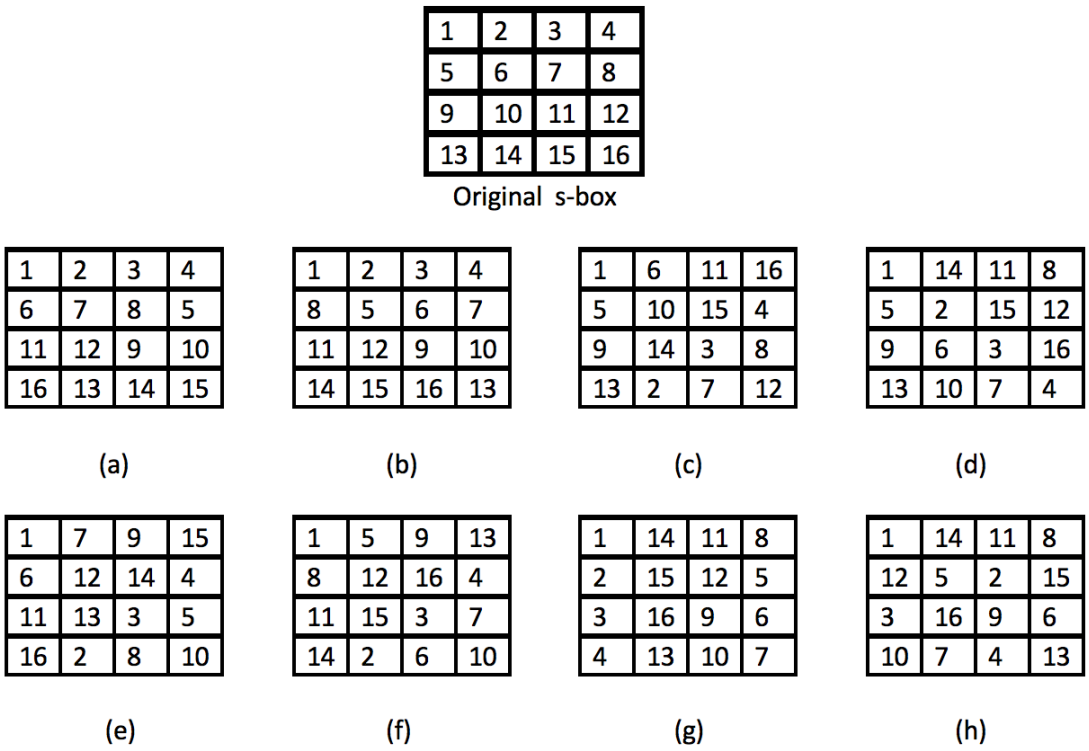
yapılarına göre daha kötü olması bir problem olarak bu konuda çalışan araştırmacıların bir problemi olarak ortaya çıkmıştır (Özkaynak, 2017). Üçüncü bölümde bu problemi gidermek için yeni bir son işlem algoritması önerilmiştir. İleride bu son işlem algoritmalarının özellikle rasgele sayı üreteçlerinin (Avaroğlu ve ark., 2015; Koyuncu ve ark., 2017) performans iyileştirmesi içinde bir alternatif olarak değerlendirilebileceği düşünülmektedir.

3. ÖNERİLEN YÖNTEM

Bu çalışmada önerilen son işlem algoritmasının s-box performans ölçütleri üzerindeki etkisini en iyi şekilde analiz edebilmek için AES s-box yapısına benzer olarak 16x16 boyutunda s-box yapıları temel alınmıştır. Önerilen son işlem algoritmasının temel prensibi kaotik sistem çıkışlarını s-box değerlerine dönüştürülmesinin ardından elde edilen tablonun satır ve sütun pozisyonlarının karıştırılması prensibine dayanmaktadır. Bu süreçte sekiz farklı olasılık incelenerek s-box performans ölçütlerine olan etkileri analiz edilmiştir. Bu olasılıklar Tablo 2'de verilmiştir.

Tablo 2. Önerilen Son İşlem Teknikleri

İşlem No	Açıklama
1	i numaralı satır (i-1) defa dairesel olarak sola kaydırılır.
2	i numaralı satır (i-1) defa dairesel olarak sağa kaydırılır.
3	i numaralı sütun (i-1) defa dairesel olarak yukarı kaydırılır.
4	i numaralı sütun (i-1) defa dairesel olarak aşağı kaydırılır.
5	i numaralı satır (i-1) defa dairesel olarak sola kaydırılır. Ardından i numaralı sütun (i-1) defa dairesel olarak yukarı kaydırılır.
6	i numaralı satır (i-1) defa dairesel olarak sağa kaydırılır. Ardından i numaralı sütun (i-1) defa dairesel olarak yukarı kaydırılır.
7	i numaralı sütun (i-1) defa dairesel olarak aşağı kaydırılır. Ardından i numaralı satır (i-1) defa dairesel olarak sola kaydırılır.
8	i numaralı sütun (i-1) defa dairesel olarak aşağı kaydırılır. Ardından i numaralı satır (i-1) defa dairesel olarak sağa kaydırılır.



Şekil 1. Çalışmada önerilen detayları Tablo 2'de verilen sekiz son işlem algoritmasının çıktıları

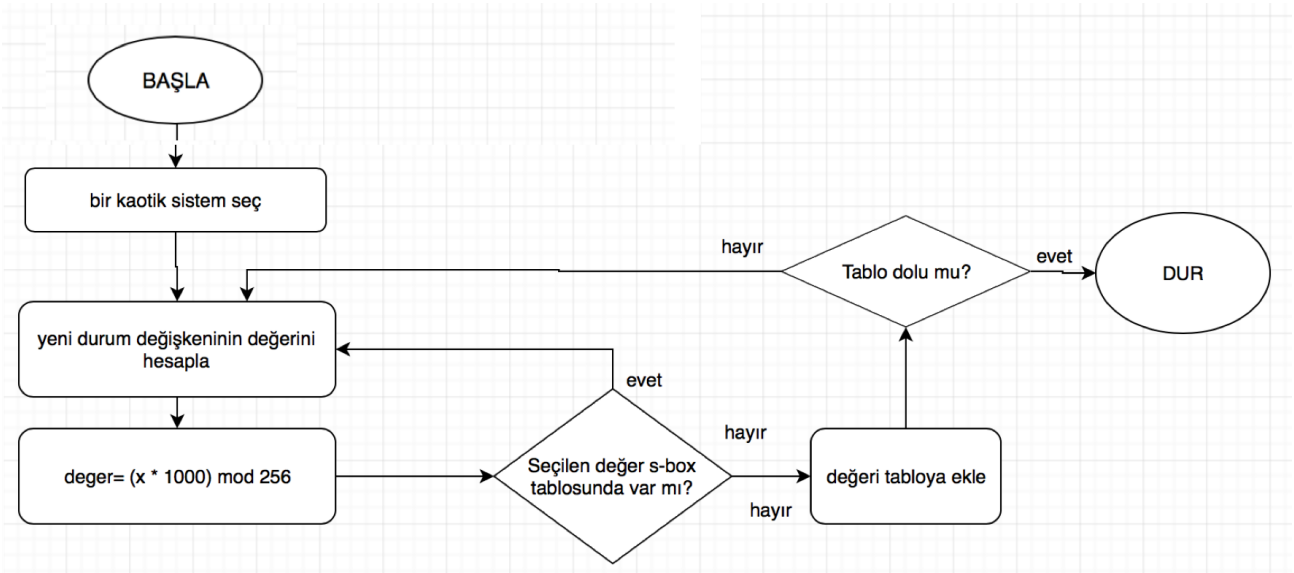
Tablo 2'de listelenen bu son işlemlerin mantığını etkili bir şekilde ifade edebilmek için 4x4 boyutunda küçük bir s-box yapısı için sonuçlar grafiksel olarak Şekil 1'de gösterilmiştir.

4. ANALİZ SONUÇLARI

S-box yapısı oluşturulurken son işlem tekniğinin başarısını ön plana çıkarmak için mümkün olduğunca basit bir yaklaşım kullanılmaya

çalışılmıştır bu yüzden çok güçlü bir tek yönlü fonksiyon olan mod fonksiyonu kullanılarak kaotik sistem çıkışları 0 ile 255 arasındaki değerlere dönüştürülmüştür. Kaotik sistemleri temel alarak s-box oluşturan algoritmanın akış şeması şekil 2'de verilmiştir. Bu algoritma ve s-box değerlendirme kriteri olarak kullanılabilecek ölçümler hakkında daha detaylı bilgiler için Kaynak (Özkaynak, 2019) incelenebilir. Kaynak (Özkaynak, 2017)'deki algoritma kullanılarak elde edilen biri ayrık zamanlı diğeri sürekli zamanlı kaotik sistem için üretilen iki farklı s-box yapısı sırasıyla Tablo 3 ve Tablo 4'de verilmiştir.

Her iki s-box yapısı için bölüm 3'de çalışma mantığı açıklanan sekiz farklı son işlem algoritması için 16 farklı s-box elde edilmiştir. Son işlemler sonucunda üretilen s-box yapılarının performans üzerinde olumlu etkileri olduğu görülmüştür. Önerilen yöntemin başarısını genelleştirmek için her bir son işlem algoritması için beş farklı s-box yapısı kullanılarak toplam 40 s-box yapısı elde edilmiştir. Bu yeni s-box yapılarının 34'ünde performans iyileşmesi gözlemlenmiştir. Başka bir iade ile %85 oranında bir başarı elde edilmiştir. İlerideki çalışmalarda daha fazla deneme yapılarak yöntemin başarı yüzdesinin artabileceği düşünülmektedir. Yakın zamanda yayınlanan çalışmalar bu görüşü desteklemektedir (Artuğer ve Özkaynak, 2020).



Şekil 2. S-box oluşturmak için kullanılan algoritma

Tablo 3. Örnek s-box yapısı 1

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

Tablo 4. Örnek s-box yapısı 2

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

5. SONUÇLAR

Bu çalışmada kaotik s-box yapıların performans kriterlerinin işlem sonrası algoritma kullanılarak daha da iyileştirilip iyileştirilemeyeceği araştırılmıştır. Sekiz farklı son işlem algoritması önerilmiştir. Analiz sonuçlarının sonunda aşağıdaki çıkarımlar yapılabilir.

- Analiz sonuçları, önerilen son işlem algoritmalarının s-box yapılarının kriptolojik özelliklerine olumlu katkıda bulunabileceğini göstermiştir.
- Satır tabanlı son işlem algoritmalarının s-box performans ölçütlerinde sütun tabanlı son işlem algoritmasından daha etkili olabileceğini göstermiştir.
- Çoklu son işlem tekniklerinin kombinasyonlarının birlikte uygulanmasının performans üzerinde her zaman olumlu bir etkisi olmayabilir.
- Katı çığ kriteri için ideal değer olan 0,5'e çok yakın sonuçların elde edilebileceği gösterilmiştir.
- Katı çığ kriteri ile XOR dağılımı arasında genellikle doğrusal bir ilişki gözlemlenmiştir.
- Bazı son işlem teknikleri doğrusal olmama özelliğini etkilerken, bazıları XOR dağıtım özelliğini geliştirmiştir.

Analizde kullanılan her iki s-box yapısı, ortalama şifreleme özelliklerine sahip s-box'lardır. İşlem sonrası algoritmaların s-box performans kriterleri üzerinde olumlu bir etkiye sahip olmasına rağmen, ileri çalışmalar, sonraki işlemlerde post-processing algoritmaların daha büyük bir s-box seti üzerindeki etkilerini genelleştirebilecektir. Ayrıca, bu etkinin uygulama (yan kanal) saldırılarına karşı saldırıları önlemek için yapacağı olumlu katkılarla analiz edilmesi planlanmaktadır.

BİLGİLENDİRME/TEŞEKKÜR

Bu makale TEKF 19.18 numaralı proje kapsamında Fırat Üniversitesi Bilimsel Araştırma Projeleri Birimi tarafında desteklenmiştir.

KAYNAKÇA

Açikkapi M. S., Özkaynak F., & Özer A. B., (2019). Side-channel analy- sis of chaos-based substitution box structures, IEEE Access, vol. 7, pp. 79030–79043, 2019. doi: 10.1109/ACCESS.2019.2921708.

Artuğer F. & Özkaynak F., (2020). A Novel Method for Performance Improvement of Chaos-Based Substitution Boxes, Symmetry 12 (4), 571.

Avaroğlu E., Koyuncu I., Özer A.B. & Türk M., (2015). Hybrid pseudo-random number generator for cryptographic systems. Nonlinear Dyn 82, 239–248. https://doi.org/10.1007/s11071-015-2152-8.

Cusick T. & Stanica P. (2009). Cryptographic Boolean Functions and Applications. Amsterdam, The Netherlands: Elsevier.

Kocarev L. & Lian S. (2011). Chaos Based Cryptography Theory Algorithms and Applications. Berlin, Germany: Springer-Verlag.

Koyuncu İ. & Özcerit A. T. (2017). The design and realization of a new high speed FPGA-based chaotic true random number generator, Computers & Electrical Engineering, Volume 58, February 2017, Pages 203-214.

Naseer Y., Shah T., Shah D., & Hussain S. (2019). A novel algorithm of constructing highly nonlinear s-p-boxes, Cryptography, vol. 3, no. 1, p. 6. doi: 10.3390/cryptography3010006.

Özkaynak F. (2019). An analysis and generation toolbox for chaotic substitu- tion boxes: A case study based on chaotic labyrinth rene thomas sys- tem, Iranian J. Sci. Technol.-Trans. Elect. Eng., pp. 1–10. doi: 10.1007/s40998-019-00230-6.

Özkaynak F. (2017). Construction of robust substitution boxes based on chaotic systems, Neural Comput. Appl., pp. 1–10. doi: 10.1007/s00521- 017-3287-y.

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, 124072.

Özkaynak F. (2017). Role of NPCR and UACI tests in security problems of chaos based image encryption algorithms and possible solution proposals, 2017 International Conference on Computer Science and Engineering (UBMK) DOI10.1109/UBMK.2017.8093481.

Solami E. A., Ahmad M., Volos C., Doja M. N., & Beg M. M. S. (2018). "A new hyperchaotic system-based design for efficient bijective substitution boxes," Entropy, vol. 20, no. 7, p. 525. doi: 10.3390/e20070525.

Sprott J. (2010). Elegant Chaos Algebraically Simple Chaotic Flows. World Scientific.

Tanyıldızı E. & Özkaynak F. (2019). A New Chaotic S-Box Generation Method Using Parameter Optimization of One Dimensional Chaotic Maps, VOLUME 7. DOI 10.1109/ACCESS.2019.2936447.

Tuna M., Alçın M., Koyuncu İ., Fidan C. B. & Pehlivan İ. (2019). High speed FPGA-based chaotic oscillator design, Microprocessors and Microsystems, Volume 66, April 2019, Pages 72-80.

Wu C. & Feng D. (2016). Boolean Functions and Their Applications in Cryptography. Berlin, Germany: Springer.

Yi L., Tong X., Wang Z., Zhang M., Zhu H., & Liu J. (2019). "A novel block encryption algorithm based on chaotic s-box for wireless sen- sor network," IEEE Access, vol. 7, pp. 53079–53090. doi: 10.1109/ACCESS.2019.2911395.