Kaos Tabanlı İkame Kutuları

Fırat ARTUĞER[1*]

[1]*Bilgisayar Mühendisliği / Mühendislik Fakültesi, Munzur Üniversitesi, TÜRKİYE*

[*]*(firatartuger@munzur.edu.tr) Başlıca yazarın mail adresi*

Özet – İkame kutusu(s-box), özellikle blok şifreleme algoritmaları için oldukça önemli bir yapıdır. S-box, lineer olmayan bir yapı olduğundan, şifreleme sürecinde karıştırma olarak adlandırılan gereksinimi yerine getirmektedir. Kriptografik gereksinimleri sağlayan bir s-box elde etmek için genellikle kaos kullanılmaktadır. Bu çalışmada s-box yapılarının kaos ile nasıl elde edildiği açıklanmıştır. Ayrıca kaotik lojistik ve sinüs haritalar ile iki farklı s-box yapısı elde edilmiştir. Elde edilen s-box yapılarının nasıl analiz edileceği de açıklanmıştır. Özellikle bu alana yeni başlayan araştırmacılar için çalışmanın faydalı olacağı düşünülmektedir.

Anahtar Kelimeler – İkame Kutusu, Kaos, Kaotik Harita, Lineer Olmama, Blok Şifreleme

I. GİRİŞ

Kriptografi, geçmişten günümüze kadar çeşitli verileri korumak için uygulanan yaklaşımların başında gelmektedir [1]. Bu bilimin alt dallarından biri olan şifreleme, gizliliği sağlayan en önemli yapıdır. Şifreleme algoritmaları genellikle simetrik ve asimetrik olmak üzere iki şekilde ele alınmaktadır. Asimetrik algoritmalar yavaş olduğu için genellikle anahtar değişimi için kullanılır. Şifreleme aşaması için simetrik algoritmalar kullanılmaktadır. Simetrik algoritmalar ikiye ayrılır. İlki akış şifrelemedir. Akış şifrelemedeki temel felsefe bitleri tek tek şifrelemektir. Bu yüzden verinin boyutu arttıkça uygulaması olanaksız hale gelmektedir. Bir diğer yaklaşım ise blok şifreleme yapısıdır. Burada veri bloklara bölünür ve her blok kendi içinde şifrelenir. Günümüzde kullanılan veri şifreleme standardı olan AES algoritması [2] ve hala sıklıkla kullanılan DES algoritması [3] blok şifreleme algoritmalarıdır. Günümüzün sürekli gelişen koşullarıyla birlikte, özellikle uygulamaların boyutlarına göre yeni şifreleme algoritmalarına olan ihtiyaç kaçınılmazdır. Bu ihtiyacı karşılamak için yeni ve etkili blok şifreleme algoritmaları geliştirilmelidir. Bir blok şifreleme algoritmasının en önemli birimlerinden bir tanesi ikame kutusudur. Yani blok şifreleme algoritmalarının güvenliği çoğunlukla kullanılan s-box yapısının gücüne bağlıdır. Bundan dolayı, doğrusal kriptanaliz saldırılarına karşı dirençli bir şifreleme algoritması tasarlamak için iyi kriptografik özelliklere sahip olan s-box yapılarına ihtiyaç duyulmaktadır [4].

S-box yapılarını matematiksel olarak ifade etmek gerekirse, $S: \{0,1\}^n \rightarrow \{0,1\}^m$ şeklinde bir lineer olmayan dönüşüm olarak tanımlanabilir [4]. Bu dönüşümün en etkileyici özelliği lineer olmamasıdır. Lineer olamama özelliğinin yanı sıra, bir s-box 'ın elemanlarının komşu değerlerine bit olarak bakıldığında, yarısı veya yarısına yakın bitin farklı olması istenmektedir. Yani bir verinin girişinde meydana gelen bir bitlik bir değişikliğin çıkıştaki bitlerin yarısını değiştirmesi beklenmektedir. Bu özellik kriptografi uygulamaları için oldukça önemlidir [5]. AES algoritmasında kullanılan s-box yapısı bu özellikleri mükemmel şekilde sağlamaktadır. AES s-box yapısı 8 bitlik girişleri 8 bitlik çıkışlara dönüştürebilen etkili bir dönüşümdür. Bu

çalışmada AES benzeri s-box yapıları oluşturmak için kaos kullanılmıştır. 8 bit s-box yapıları 256 değer içermektedir ve bijektif bir dönüşümdür. Yani buna benzer s-box yapılarında, 0 ile 256 aralığında her değer yalnızca bir kere kullanılmaktadır.

II. KAOS TABANLI İKAME KUTULARININ ELDE DİLMESİ

Kaos tabanlı bir s-box elde etmek için öncelikle bir kaotik harita seçilmektedir. Burada genellikle tek boyutlu haritalar kullanılmaktadır. Bu çalışmada lojistik ve sinüs haritalar seçilerek iki farklı s-box yapısı elde edilmiştir. Lojistik ve sinüs haritaların matematiksel yapıları denklem 1 ve denklem 2 ‘de sırasıyla verilmiştir.

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

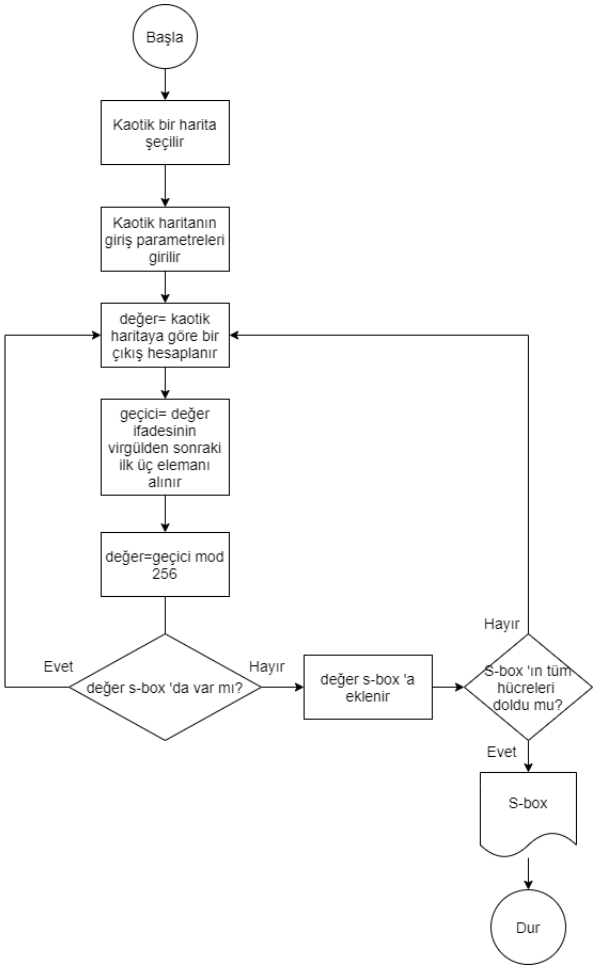
$$x_{n+1} = a \sin(\pi x_n)\,, \quad x_n \in [0,1]\,, \quad a \in [0.85,1] \quad (2)$$

Kaotik harita seçildikten sonra bu haritanın başlangıç parametreleri belirlenir. Bu parametreler genellikle sabittir. Ancak probleme göre optimizasyon teknikleriyle de seçilebilir. Başlangıç parametreleri girildikten sonra denklem başlatılır ve yeni bir x_{n+1} değeri üretilir. Bu değer eğer ikame kutusunda yoksa eklenir. Varsa yeni bir değer üretilerek akış devam eder. Bu şekilde 256 hücre dolana kadar bu işlem devam eder. 256 hücrenin tamamı dolduğunda kaotik s-box elde edilmiş olur. Kaotik bir harita yardımıyla s-box üretme algoritmasının akış diyagramı şekil 1 ‘de verilmiştir.

Şekil 1 ‘de verilen algoritma mantığı kullanılarak birçok s-box üretme algoritması önerilmiştir. Bu algoritmaların en önemli avantajları; hızlı, kodlaması kolay ve anlaşılır olmalarıdır. Ancak dezavantaj olarak da genellikle kriptografik olarak çok iyi özellikler gösteremezler. Özellikle lineer olmama değerleri düşük kalmaktadır. Bu yüzden bu algoritmaların lineer olmama değerlerini arttırmak için çalışmalar devam etmektedir [6]. Bunun için çeşitli yöntemler önerilmiş olmakla birlikte, en çok optimizasyon teknikleri kullanılmaktadır.

III. ANALİZ SONUÇLARI

Bu çalışmada şekil 1 ‘de verilen algoritma ile iki farklı s-box elde edilmiştir. Bunlardan ilki lojistik harita ile elde edilmiş olup tablo 1 ‘de verilmiştir. İkincisi ise sinüs harita ile elde edilmiş olup tablo 2 ‘de verilmiştir. Bu tarz s-box yapılarını analiz edebilmek için literatürde genellikle dört farklı metrik kullanılmaktadır. Bu metriklerden ilki katı çığ kriterleri (KÇK) olarak adlandırılmaktadır [7]. Bu kriterdeki temel felsefe, giriş verisindeki bir bit değiştiğinde, çıkış verisindeki bitlerin yarısının veya yarısına yakının değişmesidir. Yani KÇK değeri 0.5 değerine yakın bir değer olmalıdır.



Şekil 1. Kaos tabanlı ikame kutusu oluşturmak için kullanılan algoritmanın akış diyagramı

İkinci değerlendirme kriteri lineer olmama olarak adlandırılmaktadır. Bu kriterin diğerlerine göre daha önemli olduğu söylenebilir. Çünkü ikame kutuları lineer olmayan yapılardır. Lineer olmama değerleri ne kadar yüksek olursa o kadar güçlü olacaklardır. Üçüncü değerlendirme kriteri bit bağımsızlık kriteri (BBK) olarak adlandırılmaktadır [7]. Bu kriterde, herhangi bir giriş biti ters çevrildiğinde, çıkış bitlerinin tüm çığ vektörü çiftleri için bağımsız olarak değişmesi gerektiğini ifade eder. Daha sonra, çıkış bitlerinin çift yönlü bağımsız olması gerektiğini ifade eder.

Yani bir f düzleminde bijektif bir ikame kutusunun hem olabildiğince doğrusal olmaması, hem de KÇK değerini sağlaması gerekmektedir. Son olarak olasılığa sahip olmasıdır. Yani, bir s-box ‘ın özellikle diferansiyel kriptoanalize karşı dirençli olabilmesi için XOR dağılımına olabildiğince izin vermemesi gerekmektedir [8]. Bu değerin en yükseği AES algoritmasında 4 ‘tür. Daha yüksek değerler çıkması istenmemektedir.

giriş/çıkış XOR dağılımı olarak adlandırılan kriter bulunmaktadır. Bu kriterde temel felsefe, girişteki XOR değerlerinin çıkıştaki XOR değerleri ile aynı Ancak çoğu yaklaşım bu değerin oldukça üstüne çıkmaktadır. Bu çalışmada elde edilen s-box yapılarının performans değerleri tablo 3 ‘de verilmiştir. Ayrıca kıyaslama için literatürdeki diğer bazı yöntemlerin performans değerleri de yine bu tabloda verilmiştir.

Tablo 1. Lojistik harita ile elde edilen ikame kutusu

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

Tablo 2. Sinüs harita ile elde edilen ikame kutusu

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

IV. SONUÇLAR

İkame kutuları kriptografik uygulamalar için oldukça önemli yapılardır. Gelişen teknolojilerle birlikte şifreleme algoritmalarına yapılan saldırılar her geçen gün artmaktadır. Bu yüzden, güvenli blok şifreleme algoritmaları için güçlü ikame kutularına ihtiyaç duyulmaktadır. Bu yöntemlerden bir tanesi kaostur. Bu çalışmada kaos tabanlı ikame kutularının nasıl üretilip analiz edildiği açıklanmıştır. Kaos tabanlı ikame kutularını üretmek kolay ve hızlıdır. Ancak çoğu zaman kriptografik olarak kötü özellikler göstermektedirler. Özellikle lineer olmama değerleri oldukça düşüktür. Gelecekteki çalışmalarda bu kutuların lineer olmama değerlerinin arttırılması için yeni algoritmalar üzerine çalışılacaktır. Bu çalışmanın, bu alana yeni başlayacak olan araştırmacılara bir yol haritası olacağı düşünülmektedir.

Tablo 3. İkame kutularının performans değerleri

İkame Kutusu	Lineer Olmama			BBK		KÇK	Max. XOR
	min	max	ort	Lineer O.	KÇK	ort	
Tablo 1	102	106	104	104	0.4993	0.5002	10
Tablo 2	100	108	103	104.5	0.4971	0.5005	10
[9]	98	110	105.5	105.7	0.4994	0.4926	32
[10]	104	108	106.5	105.85	0.4995	0.5036	10
[11]	101	108	103.8	102.6	0.4958	0.5058	14
[12]	99	106	103.3	103.3	0.4995	0.4987	10
[13]	102	108	105.2	102.6	0.4994	0.5037	10
[14]	104	110	106.2	102.3	0.5023	0.5039	10
[15]	102	106	104	103.2	0.4971	0.4980	10
[16]	110	112	111.2	111.5	0.4950	0.5068	10
[17]	112	112	112	112	0.504	0.4998	4

KAYNAKLAR

[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. (2021). An effective method to improve nonlinearity value of substitution boxes based on random selection. Information Sciences, 576, 577-588.

[5] Wu, C. K., & Feng, D. (2016). Boolean functions and their applications in cryptography. Springer Berlin Heidelberg.

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

[7] 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.

[8] Biham, E., & Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY, 4(1), 3-72.

[9] 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.

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

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

[12] 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.

[13] 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.

[14] 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.

[15] Chen, G. (2008). A novel heuristic method for obtaining S-boxes. Chaos, Solitons & Fractals, 36(4), 1028-1036.
[16] Razaq, A., Ullah, A., Alolaiyan, H., & Yousaf, A. (2021). A novel group theoretic and graphical approach for designing cryptographically strong nonlinear components of block ciphers. Wireless Personal Communications, 116(4), 3165-3190.
[17] Anees, A., & Chen, Y. P. P. (2020). Designing secure substitution boxes based on permutation of symmetric group. Neural Computing and Applications, 32(11), 7045-7056.