S-kutularının Kriptografik Özellikleri
Cryptographic Properties of S-boxes

Bora ASLAN[1], *M.Tolga SAKALLI*[2]

[1] Lüleburgaz Meslek Yüksekokulu
Kırklareli Üniversitesi
boraaslan@trakya.edu.tr
[2] Bilgisayar Mühendisliği, Müh. Mim. Fakültesi
Trakya Üniversitesi
tolga@trakya.edu.tr

Özet

Günümüzde bilgi güvenliği internetin de gelişimi ile birlikte bilginin güvenliğinin sağlanması gerekliliği açısından önemli hale gelmiştir. Kriptografi, verinin güvenli bir şekilde iletilmesi ile ilgilidir. Dolayısıyla güvenli şifreleme algoritması tasarımı kriptografide çok önemli bir yer tutar. Buna ek olarak Türkiye'de kriptografi ile ilgili çalışmaların daha da genişlemesi ve gelecekte ülkenin kendi simetrik şifreleme algoritması tasarlamasının da gerekliliği düşünüldüğünde şifrenin içyapısında güvenli doğrusal olmayan ve AES S-kutusunda olduğu gibi cebirsel S-kutuları kullanılabilir.

Abstract

Nowadays, with increasing use of the Internet, information security has become more important than before. That has brought the need of information security. On the other hand, cryptography is the science of information security and presents various methods for taking legible, readable data, and transforming it into unreadable data for the purpose of secure transmission, and then using a key to transform it back into readable data when it reaches its destination. For that reason, the design of strong and secure encryption algoritm is very important concept in cryptography. Moreover, if the need of expansion of cryptographic studies in Turkey and the design of a new symmetric encryption algorithm for Turkey are concerned, to design algebraically improved AES S-box like S-boxes for probable ciphers in the next is important matter.

1. Giriş

2001 yılında AES [1] (Advanced Encryption Standard) şifreleme algoritması, DES [1] (Data Encryption Standard) şifreleme algoritmasının yerine seçilmiştir. Bunun nedenleri arasında AES'in güvenlik, maliyet, algoritma ve uygulama özellikleri açısından daha iyi olması vardır. AES şifreleme algoritması bilinen bütün kriptanaliz yöntemlerine karşı güvenilirdir. AES ve DES gibi blok şifreleme algoritmalarının gücünü berirleyen bazı özellikler aşağıdaki gibidir [3]:

- Anahtar: Blok şifrelerde anahtarın uzunluğu saldırılara karşı güçlü olacak şekilde seçilmelidir. DES algoritması 56-bit anahtar uzunluğu kullanırken, AES algoritması 128, 192, 256 bit anahtar uzunluklarını seçenekli olarak sunmaktadır. Bunun sayesinde şifrenin kaba kuvvet (brute-force) saldırısına karşı kırılabilirliği zorlaşmaktadır.
- Döngü sayısı: Blok şifreleme algoritmalarında döngü sayısı iyi seçilmelidir. Böylelikle doğrusal dönüşüm ve yerdeğiştirme işlemleri ile şifreleme algoritması daha da güçlenmektedir. Ayrıca şifrenin karmaşıklığının arttırılmasında çok önemli bir etkendir. Böylelikle saldırılara karşı açık metin iyi derecede korunabilir.
- S-kutuları(Yerdeğiştirme kutuları):Blok şifreleme algoritmalarının en önemli elemanı S-kutularıdır. Algoritmanın tek doğrusal olmayan elemanıdır. Bu yüzden iyi bir S-kutusu seçimi şifrenin karmaşıklığını doğrudan etkiler.

Şifreleme algoritmasına yapılan saldırılardan, doğrusal ve diferansiyel saldırılara karşı blok şifreleme algoritmasını güvenli kılmak için kriptografik özellikleri iyi olan S-kutuları seçilmelidir. Bijektif S kutuları birçok modern şifrelerin güvenliğinin sağlanmasında çok önemli rol oynarlar ve diğer S-kutularına göre iyi kriptografik özelliklere sahiptirler. S-kutuları tasarlanırken aşağıdaki çeşitli yöntemler kullanılmaktadır[4]:

- pseudo-random üretim,
- sonlu cisimde ters alma,
- sonlu cisimde üs alma,
- heuristic teknikler.

S-kutuları vektörel fonksiyonlar olarak ifade edilebilir ve $f_1, f_2, f_3, ..., f_m$ ile temsil edilebilir. f_i boole fonksiyonları F_2^n'den F_2'ye tanımlanır ve S-kutusunun çıkış fonksiyonları olarak isimlendirilir.

AES şifresinde kullanılan S-kutuları Nyberg'in [5] önerdiği sonlu cisimde ters alma tabanlıdır ve cebirsel ifadesi aşağıdaki gibidir.

$$f(x) = x^{-1},\ x \in GF(2^8),\ f(0) = 0 \qquad (1)$$

2. S-kutularının Kriptografik Özellikleri

Blok şifrelerdeki bu kadar önemli bir elemanın güçlü olması istenir. Bunun için üretilen S-kutularının kriptografik özelliklerinin iyi olması önemlidir. Çalışmanın devamında S-kutularının önemli bazı kriptografik özellikleri belirtilmektedir.

2.1. Bütünlük Kriteri

Kam ve Davida'nın tarafından belirlenmiştir [6]. S-kutuları vektörel bir fonksiyondur ve bir fonksiyonun bütünlük özelliği taşıması için gerekli olan kurallar aşağıdaki gibi olmalıdır.

$f : \{0,1\}^n \rightarrow \{0,1\}^n$ olsun. i ve $j \in \{1,2,...,n\}$ olmak üzere f fonksiyonun en az bir tane $x \in \{0,1\}^n$ olmalı ki $f(x)$ ve $f(x \oplus \Delta x_i)$ bir j'de farklılaşıyorsa bütünlük özelliği sağlanmış olur. Kısacası her çıkış biti giriş bitlerinin tümüne bağlıdır.

Bir S-kutusunun çığ (avalanche) vektörü (2) denkleminde verilmiştir[7][8][9].

$$\begin{aligned} \Delta Y^{\Delta x_i} &= f(x) \oplus f(x \oplus \Delta x_i) \\ &= [a_1^{\Delta x_i} a_2^{\Delta x_i} \dots a_n^{\Delta x_i}] \end{aligned} \quad (2)$$

$\Delta Y^{\Delta x_i}$, çığ vektörü giriş şeridinden sadece bir biti değiştirerek oluşturulmuş çıkış şeridir. O zaman toplam değişim (3) gibi olacaktır.

$$wt(a_j^{\Delta x_i}) = \sum_{\forall x} a_j^{\Delta x_i} \quad (3)$$

Eğer $wt(a_j^{\Delta x_i}) = 0$ ise çıkış bitleri giriş bitlerinden etkilenmemiştir ve dolayısı ile bütünlük yoktur. Bunun yanında eğer $wt(a_j^{\Delta x_i}) = 2^n$ ise giriş bitinin değili alındığında çıkış biti doğrudan etkilenecektir ve buda istenmeyen bir durumdur. Dolayısı ile bütünlük kriterinin sağlanabilmesi için (4) denklemi sağlanmalıdır.

$$0 < wt(a_j^{\Delta x_i}) < 1 \quad (4)$$

2.2. Çığ (Avalanche) Kriteri

Çığ ölçütü (avalance criterion) (AVAL) Feistel [10] tarafından S-kutuları ve SPN tabanlı blok şifreler için tanımlanmıştır. Buna göre bir $f : \{0,1\}^n \rightarrow \{0,1\}^n$ fonksiyonu için giriş bitinin bir biti değiştiğinde çıkış bitlerinin yarısı değişecektir. Yani (3) deki toplam değişme, i giriş ve j çıkış bitleri için (5) sağlanır ise çığ kriteri [7][8][9] sağlanmış olur.

$$\frac{1}{2^n} \sum_{j=1}^{n} wt(a_j^{\Delta x_i}) = \frac{1}{2} \quad (5)$$

Eğer (5) ifadesi bir çığ kriter parametresi oluşturulmak için tekrar düzenlenerek yazılır ise (6) ifadesine ulaşılır.

$$k_{cig}(i) = \frac{1}{n.2^n} \sum_{j=1}^{n} wt(a_j^{\Delta x_i}) = \frac{1}{2} \quad (6)$$

(6) ifadesine göre herhangi bir i değeri için $k_{cig}(i)$ değeri $\frac{1}{2}$ değerinden farklı bir değer alırsa S-kutusu için çığ kriteri sağlanmayacaktır.

2.3. Katı Çığ Kriteri (Strict Avalanche Criterion)

Webster ve Tavares [11] bütünlük ve çığ özelliklerini bileştirerek katı çığ özelliğini (Strict Avalanche Criterion) (SAC) tanımlamışlardır. $f : \{0,1\}^n \rightarrow \{0,1\}^n$ fonksiyonu için giriş biti i'yi değiştirmek için j'nin kesinlikle $\frac{1}{2}$ olasılıkla değişiyor ise SAC özelliği sağlanmaktadır denir. Tüm giriş ve çıkış bitleri için (7) ifadesi doğrulanır ise o S-kutusu için katı çığ kriteri sağlanmıştır [7][8][9].

$$\frac{1}{2^n} wt(a_j^{\Delta x_i}) = \frac{1}{2} \quad (7)$$

(7) ifadesi üzerinden bir katı çığ parametresi (8) deki gibi yazılabilir.

$$k_S AC(i,j) = \frac{1}{2^n} wt(a_j^{\Delta x_i}) \quad (8)$$

(8) ifadesi herhangi bir giriş i ve çıkış j kombinasyonu için $\frac{1}{2}$ değerinden farklı bir değer üretir ise S-kutusu için SAC kriteri sağlanmaz. Yukarıdaki ifadeler incelenir ise S-kutusu çığ ve bütünlük kriterlerinin ikisinide sağlıyor ise SAC kriterinide sağlar demek mümkündür.

2.4. Bit Bağımsızlık Kriteri (Bit Independence Criterion)

Bit bağımsızlık ölçütü (Bit Independence Criterion - BIC) yine Webster ve Tavares [11] tarafından tanımlanmıştır. $f : \{0,1\}^n \rightarrow \{0,1\}^n$ fonksiyonu için $i,j,k \in \{1,2,...,n\}$ ve $j \neq k$ olmak üzere tüm i,j,k değerleri için giriş biti i'nin tersini almak j ve k çıkış bitlerinin bağımsız olarak değişebiliyor ise BIC özelliği sağlanmıştır.

BIC değerini ölçmek için çığ verktörü ile j ve k bitleri arasındaki korelasyon katsayısını incelemek gerekmektedir. İki değişken (v,w) arasındaki korelasyon (9) ifadesi gibi hesaplanabilir

$$corr(v,w) = \frac{E(vw) - E(v)E(w)}{\sqrt{(E(v^2) - E(v)^2)(E(w^2) - E(w)^2)}} \quad (9)$$

(9) ifadesindeki $E(v)$ ya da $E(w)$, çığ vektörü v ya da w'nın ortalama değerini verecektir.

$$E(v) = \frac{1}{2^n} \sum_{\forall x} v(x) \quad (10)$$

Bir S-kutusunun çığ vektöründeki bitler $\left[a_1^{\Delta x_i} a_2^{\Delta x_i} \dots a_n^{\Delta x_i}\right]$ olmak üzere $i.$ giriş bitinin çığ vektörünün $j.$ ve $k.$ bitlerindeki etkisi ile ilgili BIC parametresi (11) ile verilebilir.

$$BIC(a_j, a_k) = \left| corr(a_j^{\Delta x_i}, a_k^{\Delta x_i}) \right| \quad (11)$$

bütün bu ifadeler düşünülerek bir f fonksiyonu için BIC kriteri tüm $1 \leq i,j,k \leq n$ için (12) ile ifade edilebilir.

$$\begin{aligned} BIC(f) &= maxBIC(a_j, a_k) \\ &= max \left| corr(a_j^{\Delta x_i}, a_k^{\Delta x_i}) \right| \end{aligned} \quad (12)$$

BIC(f), [0,1] aralığında olan bir değerdir. Mümkün olabildiğince 0'a yakın olması gereklidir. Böylelikle $\Delta Y^{\Delta x_i}$ çığ

vektörünün iki biti arasındaki korelasyon küçük olabilir. En kötü BIC değeri 1 dir ve bu da i giriş bitini değiştirildiğinde j. ve k. çıkış bitleri arasında maksimum korelasyona denk düşer [7][8][9].

2.5. MOSAC ve MOBIC özellikleri

Eğer f fonksiyonunun bir ya da daha fazla giriş biti değiştiğinde çıkış biti $\frac{1}{2}$ olasılık ile değişiyor ise MOSAC (Maximum Order SAC) [12] [13] özelliği sağlanmış olur. (13) bu denkliği göstermektedir.

$$wt(a_j^{\Delta x_i}) = 2^{n-1} \qquad \forall \Delta x, j \tag{13}$$

(13) ifadesine göre $\Delta x \neq= (0,0,0\ldots,0)$ olmak üzere tüm Δx vektörleri için çığ vektörü bitlerinin Hamming ağırlığının 2^{n-1} olması gerekir.

MOBIC (Maximum Order BIC) ölçütü (14) ifadesi ile tanımlanabilir.

$$MOBIC(a_j, a_k) = max \left| corr(a_j^{\Delta x}, a_k^{\Delta x}) \right| \qquad \Delta x \in (0,1)^n, \neq \{0,\ldots,0\} \tag{14}$$

Bir f fonksiyonunun maksimum dereceden bit bağımsızlığı aynı çıkış bitleri haricindeki $MOBIC(a_j, a_k)$ değerlerinin maksimumudur. Bu ifade de (15) de gösterilmektedir.

$$MOBIC(f) = maxMOBIC(a_j, a_k) \qquad j \neq k \tag{15}$$

2.6. Doğrusal Yaklaşım Tablosu

Doğrusal yaklaşım tablosu (Lineer Approximation Table) (LAT)[14][15][16], doğrusal kriptanalize karşı S-kutularının gücünü test etmeye yarayan önemli bir ölçüttür. S-kutusunun doğrusal yaklaşım tablosundaki maksimum olan değerin minimum olması doğrusal saldırıların başarısını zorlaştıracaktır.

$S : GF(2^n) \rightarrow GF(2^n)$ olmak üzere n-bit giriş ve n-bit çıkışa sahip bir S-kutusu olsun. O zaman herhangi verilen $a, b, \Gamma_a, \Gamma_b \in GF(2^n)$, için $N_L(\Gamma_a, \Gamma_b)$, herhangi $\Gamma_a \neq 0$ ve Γ_b için $x \in GF(2^n)$ olmak üzere $\Gamma_a \bullet x = \Gamma_b \bullet S(x)$ denklemini sağlayan değerlerin sayısını tanımlar ve (16) ifadesindeki gibi gösterilir. (17) ifadesinde ise S için Γ_a giriş maskesi ve Γ_b çıkış maskesi olmak üzere herhangi giriş ve çıkış maskesi değerine göre LAT tablosu değerinin nasıl bulunduğu gösterilmektedir. Buradaki $\bullet$ işlemi nokta ürün [1] işlemidir.

$$N_L(\Gamma_a, \Gamma_b) = \#\{x \in GF(2^n) : \Gamma_a \bullet x = \Gamma_b \bullet S(x)\}^{\,2} \tag{16}$$

$$LAT(\Gamma_a, \Gamma_b) = \#\{x \in GF(2^n) : \Gamma_a \bullet x = \Gamma_b \bullet S(x)\} - 2^n \tag{17}$$

n-bit giriş ve n-bit çıkışa sahip bir S-kutusunun LAT tablosu $2^n \times 2^n$ boyutunda bir tablo olacaktır. Bu tablodaki en büyük değerin küçük olması istenir. Diğer yandan bir S-kutusu için doğrusal olmama ölçüsü NLM_s değeri LAT değeri ile ilişki olarak (18) ifadesi kullanılabilir.

$$NLM_s = 2^{n-1} - maks\,|LAT_s(\Gamma_a, \Gamma_b)| \tag{18}$$

AES şifreleme algoritmasının S-kutusunun LAT dağılım tablosu oluşturulduğunda en büyük değerin mutlak değerinin 16 olduğu görülür. (18) ifadesine göre AES S-kutusu 112 doğrusal olmama ölçütüne sahiptir dolayısı ile % 93 doğrusal değildir.

2.7. Fark Dağılım Tablosu

Fark dağılım tablosu (Difference Distribution Table-DDT), diferansiyel kriptanalize karşı S-kutularının gücü hakkında bilgiler verir[17][16]. n-bit giriş ve n-bit çıkışa sahip bir S-kutusunun DDT tablosu $2^n \times 2^n$ boyutunda bir tablo olacaktır. S-kutusunun boyutuna göre oluşturulan tablodaki değerlerin maksimum olanın minumum olmasi istenir.

$S : GF(2^n) \rightarrow GF(2^n)$ olmak üzere n-bit giriş ve n-bit çıkışa sahip bir S-kutusu olsun. Herhangi verilen $a, b \in GF(2^n)$ için DDT(a,b) ifadesi $a \neq 0$ ve b için $S(x) \odot S(x \odot a) = b$ denklemini sağlayan değerlerin sayısıdır, (19 ifadesindeki gibi yazılır. Burada a giriş farkı, b ise çıkış farkı olarak isimlendirilir.

$$DDT(a, b) = \#\{x \in GF(2^n) : S(x) + S(x + a) = b\} \tag{19}$$

AES şifresinin S-kutusu düşünülür ise 256 satır ve 256 sütundan oluşan fark dağılım tablosunun en büyük değeri 4'tür. Dolayısı ile AES S-kutusu 4 uniform dağılıma sahiptir.

3. 4 bitlik bir S-kutusunun kriptografik özelliklerinin incelenmesi

AES S-kutusu gibi ters haritalama tabanı olarak üretilen 4 bit girişli ve 4 bit çıkışlı bir S-kutusu aşağıda gösterilmektedir. S-kutusu üretilirken $x^4 + x^3 + x^2 + x + 1$ polinomu indirgenemez polinom olarak seçilmiştir.

Giriş		Çıkış	
Bin.	Hex.	Bin.	Hex.
0000	0	0000	0
0001	1	0001	1
0010	2	1111	F
0011	3	1010	A
0100	4	1000	8
0101	5	0110	6
0110	6	0101	5
0111	7	1001	9
1000	8	0100	4
1001	9	0111	7
1010	A	0011	3
1011	B	1110	E
1100	C	1101	D
1101	D	1100	C
1110	E	1011	B
1111	F	0010	2

Yukarıda verilen S-kutusunun doğrusal yaklaşım tablosu tablo 1'de verilmiştir. Bu tabloda en büyük mutlak değer 4 tür.

[1] $x, u \in Z_n^2$ olmak uzere $x \bullet w = x_1 w_1 \oplus x_2 w_2 \oplus \ldots \oplus x_n w_n$

[2] $\#\psi : \psi$ kümesinin eleman sayısı

Tablo 1: S-kutusunun LAT dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	-2	0	2	0	2	0	-2	-2	0	-2	4	2	0	2	4
2	0	0	0	0	2	2	-2	-2	0	4	4	0	2	-2	2	-2
3	0	2	0	-2	-2	4	2	4	-2	0	2	0	0	-2	0	2
4	0	0	2	-2	0	0	2	-2	0	0	2	-2	4	4	-2	2
5	0	2	2	4	0	-2	2	0	-2	4	0	-2	-2	0	0	2
6	0	0	-2	2	2	2	4	0	4	0	-2	-2	2	-2	0	0
7	0	-2	-2	4	-2	0	0	2	2	0	4	2	0	2	-2	0
8	0	-2	0	-2	0	-2	4	2	0	2	0	2	0	2	4	-2
9	0	0	4	0	0	4	0	0	2	2	-2	2	-2	2	-2	-2
A	0	-2	4	2	2	0	-2	4	0	-2	0	-2	2	0	2	0
B	0	4	0	0	-2	-2	-2	2	2	2	-2	2	4	0	0	0
C	0	2	2	0	4	-2	2	0	0	-2	2	4	0	-2	-2	0
D	0	0	-2	-2	4	0	-2	2	2	2	0	0	-2	2	0	4
E	0	2	2	0	-2	0	0	-2	4	-2	2	0	-2	0	4	2
F	0	4	-2	2	2	2	0	0	-2	-2	0	0	0	4	2	-2

Tablo 2: S-kutusunun DDT dağılımı

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	4	0	0	0	0	2	2	0	2	0	2	0	2	2	0
2	0	0	0	2	0	0	0	2	0	4	2	0	2	2	0	2
3	0	0	2	0	0	0	0	2	2	0	2	2	2	0	4	0
4	0	0	0	0	0	2	2	0	2	0	2	0	0	4	2	2
5	0	0	0	0	2	0	2	0	2	2	0	4	2	0	0	2
6	0	2	0	0	2	2	2	4	0	0	2	0	2	0	0	0
7	0	2	2	2	0	0	4	2	2	0	0	0	0	0	0	2
8	0	0	0	2	2	2	0	2	0	0	0	2	0	0	2	4
9	0	2	4	0	0	2	0	0	0	2	0	0	2	0	2	2
A	0	0	2	2	2	0	2	0	0	0	0	0	4	2	2	0
B	0	2	0	2	0	4	0	0	2	0	0	2	2	2	0	0
C	0	0	2	2	0	2	2	0	0	2	4	2	0	0	0	0
D	0	2	2	0	4	0	0	0	0	0	2	2	0	2	0	2
E	0	2	0	4	2	0	0	0	2	2	2	0	0	0	2	0
F	0	0	2	0	2	2	0	2	4	2	0	0	0	2	0	0

4 bitlik bir S-kutusu için doğrusal kriptanalizden korunmak için ideal bir ölçüttür. Doğrusal kriptanaliz S-kutularının doğrusal ifadelere dönüştürülmesi ve doğrusal ifadeleri birleştirerek bilinmeyen anahtar bitlerini elde etme prensibine dayanır. Doğrusal kriptanaliz, şifreli metin bitleri ile açık metin bitleri arasındaki yüksek olasılıkta doğrusal ifadelerin meydana gelme avantajını kullanır. Bunun yolu da S-kutularından geçer. Saldırganın algoritmayı bildiği (Kerchoffs kuralı) ve belli sayıda açık metin ve şifreli metinlere sahip olduğu varsayılır. S-kutularının büyüklüğü, aktif S-kutularının (doğrusal ifade içinde olan) sayısının artışı ve doğrusal sapması küçük S-kutularının tasarımı doğrusal kriptanalizin uygulanmasını engelleyici faktörlerdir. Bu açıdan LAT dağılımı S-kutusunun gücü açısından önemli bilgiler vermektedir.

Diğer yandan S-kutusunun DDT dağılımı tablo 2'de verilmiştir. Buradaki en büyük değer 4 tür. 4 bitlik bijektif bir S-kutusu için en iyi değerdir. Bu açıdan bakıldığında diferansiyel kriptanalize karşı iyi bir S-kutusudur denilebilir. Diferansiyel kriptanaliz, doğrusal kriptanalize benzemekle beraber seçilmiş açık metin saldırısı modeline dayanmaktadır. Yani açık metin çiftlerindeki özel farkların sonuçlanan şifreli metinlerde oluşturduğu farkın etkisini analiz eder. Bu farklar mümkün olan anahtarların olasılıklarını ve en yüksek mümkün anahtarı ortaya koymak için tayin edilir. Kısacası bu saldırıda birçok sayıda açık metin ve şifreli metin çiftlerini üretilir. Bu çiftler arasındaki özel farklara karşılık şifreleme algoritmasının son döngüsündeki S-kutusundan önceki durum bitleri farkı bulunur. Bu farka göre her açık ve şifreli metin çiftleri için olası anahtar değerleri denenir ve eğer uygun bir değer yakalanır ise sayaç değeri bulunan anahtar değeri için 1 arttırılır. Yüksek olasılığı yakalayan anahtar değeri aranan hedef anahtar olarak kabul edilir.

4. Sonuçlar

Bu çalışmada S-kutularının kriptografik özellikleri anlatılmıştır. S-kutularının şifreleme algoritmalarının en önemli yapılarından biri olduğu düşünülürse, kriptografik özellikler açısından güçlü S-kutularını şifre içerisinde kullanmak önemlidir. Çalışmamızda ayrıca AES şifreleme algorimasının benzeri olarak, $GF(2^4)$'te ters haritalama yöntemi ile bir S-kutusu oluşturulmuştur. Bu S-kutusu DDT ve LAT gibi çok önemli iki kriptografik özellik açısında değerlendirilmiştir.

5. Kaynaklar

[1] FIPS 197,"Advanced Encryption Standard", *National Bureau of Standards,*, Publication 197, 2001.

[2] FIPS 46-3, "Data Encryption Standard", *National Bureau of Standards,*, Publication 46-3, 1999.

[3] Aslan, B., "Boole fonksiyonları ve S-kutularının Kriptografik Özelliklerinin İncelenmesi ve Ters Haritalama Tabanlı Cebirsel Açıdan Güçlendirilmiş Bir S-kutusu Önerisi", *Yüksek Lisans Tezi*,2008, 5-6.

[4] Sakallı, M. T., Buluş, E., Büyüksaraçoğlu F., Şahin, A., " S-kutularında Doğrusal Eşitlik-Affine equivalence in S-boxes", *IEEE Sinyal işleme ve İletişim Uygulamaları Kurultayı*, 2006

[5] Nyberg, K., " Differentially uniform mappings for cryptography", *Advances in Cryptology-EUROCRYPT'93*, 1994, 55-64.

[6] Kam, J.B., Davida, G.I. " Structured Design of Substitution Permutation Encryption Networks", *IEEE Transactions on Computers*, 1979, 747-753.

[7] Kavut, S., Yucel, M.D. " On Some Cryptographic Properties of Rijndael", *Lecture Notes in Computer Science: Information Assurance in Computer Networks*, 2001, 300-311.

[8] Vergili, İ., " Analysis of Security Criteria for Block Ciphers", *Yüksek Lisans Tezi*, 2000.

[9] Aras, E., " Analysis of Security Criteria for Block Ciphers", *Yüksek Lisans Tezi*, 1999.

[10] Feistel, H., "Cryptography and Computer Privacy", *Scientific American*, 1973, 15-23.

[11] Webster, A.F., "On the Design of S-boxes", *Advances in Cryptology: Proceedings of CRYPTO'85*, 1986, 523-534.

[12] Aras, E., Yucel, M.D., "Performance Evaluation of Safer K-64 and S-Boxes of Safer Family", *Turkish Journal of Electrical Eng. & Computer Sciences*, 2001, 161-175.

[13] Mister, S., Adams, C.M., "Practical S-Box Design", *SAC'96- Third Annual Workshop on Selected Areas in Cryptography*, 1996, 61-76.

[14] Matsui, M., "The First Experimental Cryptanalysis of the Data Encryption Standard", *Advances in Cryptology, CRYPTO'94*, 1994, 1-11.

[15] Çeçen, S., "Nonlinearity and Propagation Characteristics of Substitution Boxes", *Yüksek Lisans Tezi*, 2001.

[16] Heys, H., Adams, C.M. "A Tutorial on Linear and Differential Cryptanalysis", *Cryptologia*, 2002, 189-221.

[17] Biham, E., Shamir, A. "Differential Cryptanalysis of DES-like Cryptosystems", *Journal of Cryptology*,1999, 3-72.