BLOK ŞİFRELER İÇİN DOĞRUSAL OLMAMA ÖLÇÜTÜ

Güzin Yıldırım, Melek D. Yücel
ODTÜ *Elektrik Mühendisliği* Bölümü, TÜBİTAK-BİLTEN

Özet

Kriptografik amaçlarla kullanılmakta olan blok şifrelerin ne kadar güvenilir olduğunu anlamak üzere literatürde değişik ölçütler geliştirilmiştir. Doğrusal olmama özelliği, bu amaçla kullanılan önemli bir ölçüttür. Bu çalışmada, literatürdeki doğrusal olmama tanımları arasında bağlantı kurularak bazılarının eşdeğerliği gösterilmektedir. Geleneksel tanımlarla ölçülen doğrusal olmama özelliği, yerleşim permütasyon ağları şeklinde tasarlanmış şifrelerin yerleşim kutularına giren ikil sayısına bağlı olduğundan, farklı boyutlardaki blok şifrelerin doğrusallıklarının karşılaştırılabilmesine olanak vermemektedir. Bu çalışmada tanımlanan normalize edilmiş doğrusal olmama faktörleri ise, şifrenin yerleşim kutusu boyutlarından bağımsızdır. Bu ölçütlerden biri kullanılarak, iyi bilinen üç blok şifrenin doğrusal olmama özellikleri karşılaştırılmış; doğrusal olmama faktörleri DES için %42, SAFER K-64 için %68 ve doğrusallıktan en uzak olan LOKI97 için %84 olarak hesaplanmıştır.

Anahtar Sözcükler: Blok şifre, yerleşim kutusu, doğrusal olmama ölçütü.

1. Giriş

Kriptografi, ham verilerin, kullanıcı tarafından belirlenen anahtarlarla birleştirilerek şifrelenmiş verilere dönüştürülmesi işidir.

İki çeşit kriptografik algoritma grubu vardır: simetrik ve asimetrik algoritmalar. Asimetrik yöntemlerde şifreleme ve şifre çözme için farklı anahtarlar kullanılırken, simetrik şifreler iki kullanıcı arasında önceden belirlenmiş tek bir anahtar kullanırlar. Asimetrik algoritmaların simetrik olanlara üstünlüğü, anahtar dağıtımı probleminin olmaması, simetrik *algoritmaların diğerlerinden iyi tarafı ise, çok daha* hızlı çalışmalarıdır. Bu nedenle günümüzde iki grup algoritmayı birlikte kullanan sistemler tercih edilmektedir. Hem asimetrik hem de simetrik algoritmalar için kullanılabilen blok şifrelerin özelliği, algoritmaya girdi olarak verilen belirli uzunluktaki bloklara karşılık, yine sabit uzunlukta şifrelenmiş bloklar oluşturulmasıdır. Ötelemeli (iterasyonlu) blok şifreler ise bir döngü içinde tanımlanan basit bir fonksiyonu pek çok (çoğunlukla 8 veya 16) kez tekrar ederler.

Ötelemeli blok şifrelerin önemli bir bölümü, yerleşim permütasyon ağları yapısındadır. *Bu döngüsel yapının* her adımında, bir yerleştirme işlemi ve onu izleyen doğrusal bir permütasyon işlemi yapılır. Yerleştirme işlemini gerçekleştiren yerleşim kutuları (*s-kutuları*), girişteki ikil gruplarını çıkış ikillerine bağlayan tablolardır. Yerleşim kutuları ötelemenin her adımında aynı olabileceği gibi farklı da seçilebilir. Permütasyon işlemiyle, yerleşim kutuları çıktısında oluşan ikillerin yerleri, doğrusal bir şekilde yeniden düzenlenir.

Yerleşim-permütasyon ağları yapısında tasarlanmış blok şifrelerin doğrusal olmayan bölümü, yerleşim kutularıdır. Bu nedenle literatürdeki doğrusal olmama incelemeleri tüm blok şifre üzerinde değil, şifrenin yerleşim kutuları üzerinde gerçekleştirilmektedir.

Bu çalışmada, literatürden alınan geleneksel doğrusal olmama tanımları arasında bağlantı kurularak, bazılarının eşdeğerliği gösterilmektedir. Bu tanımlarla ölçülen doğrusal olmama özelliği, yerleşim permütasyon ağları şeklinde tasarlanmış şifrelerin yerleşim kutularına giren ve çıkan ikil sayısına bağlıdır. Bu nedenle, farklı büyüklükte yerleşim kutularına sahip blok şifreler, doğrusal olmama özelikleri açısından doğrudan karşılaştırılamazlar. Bu bildiride, iki değişik normalize edilmiş doğrusal *olmama faktörü tanımlanarak, üç tanınmış blok şifre* (DES, SAFER K-64 ve LOKI-97) için hesaplanmıştır. Bu şifrelerden LOKI-97'nin %84'lük doğrusal olmama değeri ile en iyi başarımı gösterdiği gözlemlenmiş; SAFER için %68, ve DES için %42'lik değerler elde edilmiştir.

Doğrusal olmama özelliğinin yüksek olması, şifrenin doğrusal kriptanalize karşı güvenli olabilmesi için gereklidir. Doğrusal kriptanaliz, kriptanalizin önemli bir koludur. Doğrusal kriptanalizin temel mantığı, şifrenin girdi, çıktı ve anahtar ikilleri arasında doğrusal bir ilişki kurulabilmesine dayanır. P şifreleme algoritmasına giren metni, C şifrelenmiş metni, K ise anahtarı gösteren vektörler olmak üzere, bu vektörlerin elemanlarını sırasıyla P_i, C_j, ve K_k olarak gösterirsek,

giren ikillerden a, çıkan ikillerden b ve anahtara ait c adet ikil arasında doğrusal bir ilişki kurulabilmesi için:

$$P_{i_1} \oplus ... \oplus P_{i_a} \oplus C_{j_1} \oplus ... \oplus C_{j_c} = K_{k_1} \oplus ... \oplus K_{k_b} \quad (1)$$

denkleminin sağlanması yeterlidir. Bazı a, b ve c değerleri için (1) denklemini sağlayan doğrusal algoritmalar doğrusal kriptanaliz ile çözülebilecekleri için, doğrusal olmama özelliği, güvenilir blok şifre tasarımında önemli bir rol oynamaktadır.

2. Temel Tanımlar

Aşağıdaki temel tanımlar, $f: Z_2^n \to Z_2$ formundaki Boole fonksiyonları için verilmektedir.

Tanım 1: $a_1, a_2 ..... a_n \in Z_2$ ve $w, x \in Z_2^n$ olmak üzere, (2) denklemi şeklinde yazılabilen fonksiyonlara doğrusal işlevler denir.

$$f(\mathbf{x}) = a_1 x_1 \oplus a_2 x_2 \oplus ..... \oplus a_n x_n = \mathbf{w} \cdot \mathbf{x} \quad (2)$$

Tanım 2: Doğrusal fonksiyonlara sabit bir $c \in Z_2$ eklenmesiyle doğrusalımsı*(affine)* fonksiyonlar oluşur.

$$f(\mathbf{x}) = a_1 x_1 \oplus ... \oplus a_n x_n \oplus c = \mathbf{w} \cdot \mathbf{x} + c \quad (3)$$

denklemiyle tanımlanan $f(\mathbf{x})$, doğrusalımsı bir işlevdir; aynı zamanda (c=0 durumunda) doğrusaldır.

Tanım 3: $f(\mathbf{x})$ fonksiyonuna ait doğruluk tablosu f_t, $\mathbf{x}$ vektörünün alabileceği tüm değerler için,

$$f_t = \{f(\alpha_0), ... f(\alpha_{2^n-1})\} \quad (4)$$

olarak tanımlanır. Burada α_i (i=0,1, ...,2^n-1) vektörü, $\mathbf{x}$ vektörünün alabileceği tüm değerleri ifade etmektedir.

Tanım 4: $f(\mathbf{x})$ fonksiyonuna ait dizin vektörü $\mathbf{f_s}$. (5) denkleminde verildiği gibi tanımlanır.

$$\mathbf{f_s} = \{(-1)^{f(\alpha_0)}, (-1)^{f(\alpha_1)}, ...(-1)^{f(\alpha_{2^n-1})}\} \quad (5)$$

Dikkat edilirse, $\mathbf{f_s}$ dizinini bulabilmek için, f_t doğruluk tablosundaki 0'ların 1, ve 1'lerin -1'le yer değiştirmesi yeterlidir.

Tanım 5: İki fonksiyon arasındaki Hamming uzaklığı, bu işlevlerin doğruluk tabloları arasındaki fark vektörünün (diğer bir deyişle, işlevlerin farkının doğruluk tablosunun) Hamming ağırlığına eşittir [1].

Z_2'de tanımlanan toplama veya fark işlevlerinin eşdeğer olduğu hatırlanırsa:

$$d_H(f,g) = w_H(f(\mathbf{x}) \oplus g(\mathbf{x})), \quad (6)$$

Buradaki Hamming ağırlığı w_H, vektörün sıfırdan farklı elemanlarının (yani 1'lerin) sayısını, t takısı ise (4) denklemiyle tanımlanan doğruluk tablosunu göstermektedir.

3. Doğrusal Olmama Ölçütünün Farklı Tanımları

Doğrusal olmama ölçütü ilk olarak J. F. Dillon tarafından 1972'de tanımlandı. Dillon, bir Boole fonksiyonu için doğrusal olmama ölçütünü, tüm giriş vektörleri üzerinde tarama yapıldığında işlevin doğrusal bir fonksiyonla aynı değeri vermediği durumların sayısı olarak tanımladı [2].

$$N_f = \min \#\{\mathbf{x} \in Z_2^n \mid f(\mathbf{x}) \neq \mathbf{w} \cdot \mathbf{x} + c\} \quad (7)$$

(7) denkleminde $\#\{.\}$ ifadesi belirli bir olayın sayısını göstermektedir ve minimum bulma işlemi, olası tüm w vektörleri ve c katsayıları üzerinden yapılmaktadır. (7) ile verilen tanımda, bir işlevin tüm $\mathbf{x}$ değişkenleri üzerinden incelenmesi, o fonksiyonun doğruluk tablosunun incelenmesi anlamına gelmektedir. O halde, doğrusal olmama ölçütü, bir fonksiyonun doğruluk tablosundan doğrusalımsı bir fonksiyonun doğruluk tablosuna ulaşmak için değiştirilmesi gereken ikillerin sayısıdır. Öyleyse:

$$\begin{aligned} N_f &= \min \#\{\mathbf{x} \in Z_2^n \mid f(\mathbf{x}) \neq \mathbf{w} \cdot \mathbf{x} + c\} \quad (7) \\ &= \min_{\mathbf{w}} \#\{f_t(\mathbf{x}) \neq (\mathbf{w} \cdot \mathbf{x} + c)_t\} \\ &= \min_{\mathbf{w}} w_H\{f_t(\mathbf{x}) \oplus (\mathbf{w} \cdot \mathbf{x} + c)_t\} \\ &= \min_{\mathbf{w}} d_H(f(\mathbf{x}), (\mathbf{w} \cdot \mathbf{x} + c)) \quad (7a) \end{aligned}$$

Bu da, f fonksiyonunun kendisine en yakın olan doğrusalımsı fonksiyona uzaklığıdır. (3) numaralı denklemi kullanarak yazılabilecek tüm doğrusalımsı fonksiyonlara k_j denirse (7a) denklemi:

$$N_f = \min_{i=0,.....2^{n+1}-1} d_H(f, k_i) \quad (8)$$

haline gelir. Böylece, $f(\mathbf{x})$ fonksiyonun kendine en yakın doğrusalımsı işleve olan uzaklığı olan N_f, o fonksiyonun ne ölçüde doğrusal olmadığının bir göstergesi olarak tanımlanmış olur. Literatürdeki bir çok makalede, (7) veya (8) denklemleriyle verilen tanımlar, eşdeğer olarak kullanılmaktadır [3 - 8].

(8) denklemindeki k_i, (3) denklemini kullanarak yazılabilecek tüm doğrusalımsı fonksiyonları göstermektedir. Bu fonksiyonlara ait dizinlere $k_{i,s}$ adı verilerek, Zhang, Zheng ve Imai tarafından [9] verilen diğer bir tanım ise aşağıdaki gibidir:

$$N_f = 2^{n-1} - \frac{1}{2}\max\left\{\left|\mathbf{f_S}\cdot\mathbf{k_{i,S}}\right|, 0 \le i \le 2^n - 1\right\} \quad (9)$$

4. Normalize Edilmiş Doğrusal Olmama Ölçütleri

(7), (8) ve (9) denklemlerinin zayıf yönü, N_f faktörünü n sayısına bağlı olarak tanımlamaları nedeniyle, değişik giriş ikil sayısına sahip fonksiyonların karşılaştırılmaları için uygun olmamalarıdır. Literatürde (9) denkleminden daha sıklıkla kullanılan (8) denklemindeki tanım, doğrusal olmama özelliğini mükemmel olarak sağlayabilen bir fonksiyonun doğruluk tablosunun, doğrusalımsı fonksiyonların doğruluk tablolarından olabildiğince farklı olması gerektiğini göstermektedir. Doğrusalımsı fonksiyonların bir özelliği de, giriş vektörünü sabit bir vektör kadar kaydırınca, sonucun tüm giriş vektörleri için ya hiç etkilenmemesi, ya da her zaman değişmesidir. Çünkü, eğer $f(\mathbf{x})$ işlevi doğrusalımsı ise herhangi bir $\mathbf{a}$ vektörü için $f(\mathbf{x}+\mathbf{a}) = f(\mathbf{x}) + f(\mathbf{a})$ olacağından, tüm $\mathbf{x}$'ler için hesaplanan $f(\mathbf{x})$ ve $f(\mathbf{x}+\mathbf{a})$ değerleri ya birbirine eşittir ($f(\mathbf{a})=0$ durumu), ya da tümü farklıdır ($f(\mathbf{a})=1$ durumu). Öyleyse, $\#\{.\}$ ifadesi belirli bir olayın sayısını göstermek üzere, herhangi bir $\mathbf{a}$ vektörü için:

$$f(\mathbf{a}) = 0 \;\Rightarrow\; \#\{\mathbf{x} \mid f(\mathbf{x}) = f(\mathbf{x}+\mathbf{a})\} = 2^n \quad (10a)$$
$$f(\mathbf{a}) = 1 \;\Rightarrow\; \#\{\mathbf{x} \mid f(\mathbf{x}) = f(\mathbf{x}+\mathbf{a})\} = 0 \quad (10b)$$

eşitliği, tüm doğrusalımsı işlevler tarafından sağlanır. Bu nedenle, doğrusal olmama özelliği maksimum olan bir $f(\mathbf{x})$ işlevi, (10) denklemindeki iki durumdan da olabildiğince uzak olmalıdır [1, 4, 10]. Böyle bir $f(\mathbf{x})$ işlevinin verilen her $\mathbf{a}$ vektörü için:

$$\#\{\mathbf{x} \mid f(\mathbf{x}) = f(\mathbf{x}+\mathbf{a})\} = 2^{n-1} \quad (11)$$

denklemini sağlaması beklenebilir [11].

(10) ve (11) denklemlerini 2^n 'ye bölerek, 2^n, 0 ve 2^{n-1} sayılarını sırasıyla 1, 0 ve 1/2 olasılıkları halinde ifade etmek de mümkündür. (11) denklemindeki olasılığın 1/2'ye eşit olması durumu en yüksek ölçüde doğrusal olmama anlamına geleceğinden, bu olasılıktan yüzde sapma olarak başka bir çalışmamızda [11] tanımladığımız ε değeri de, $f(\mathbf{x})$ fonksiyonunun doğrusal olmama özelliğinden sapmasının ölçüsü kullanılabilir:

$$(1-\varepsilon)/2 \le \#\{f(\mathbf{x}) = f(\mathbf{x}+\mathbf{a})\}/2^n \le (1+\varepsilon)/2 \quad (12)$$

(12) denklemindeki $\varepsilon = 0$ ise (11) denklemi, $\varepsilon = 1$ ise (10) denklemi sağlanacaktır. Tüm $\mathbf{a}$ vektörleri için (12)'yi sağlayan en büyük sapma olan ε değerine ε_f dersek, $\varepsilon_f = 0$ durumu, $f(\mathbf{x})$ işlevinin doğrusal olmama özelliğinden hiç sapma olmadığını (yani doğrusal olmama özelliğinin en çok olduğunu), $\varepsilon_f = 1$ durumu ise sapmanın %100 olduğunu gösterecektir; yani $\varepsilon_f = 1$ olması, $f(\mathbf{x})$'in doğrusal olduğu anlamına gelecektir. O halde:

$$\varepsilon_f = \text{maksimum}_{\mathbf{a}}\{\varepsilon\}$$
$$= \text{maks}_{\mathbf{a}}\left\{\left|\#\{f(\mathbf{x}) = f(\mathbf{x}+\mathbf{a})\} - 2^{n-1}\right| / 2^{n-1}\right\} \quad (13)$$

olarak tanımlayacağımız parametre (0, 1] aralığında değişirken, 100 ε_f değeri, $f(\mathbf{x})$'in yüzde kaç doğrusal bir işlev olduğunu ölçecektir. Bu durumda:

$$N_f = 1 - \varepsilon_f = 1 - \text{maks}_{\mathbf{a}}\{\varepsilon\}$$
$$= 1 - \text{maks}_{\mathbf{a}}\left\{\left|\#\{f(\mathbf{x}) = f(\mathbf{x}+\mathbf{a})\} - 2^{n-1}\right| / 2^{n-1}\right\} \quad (14)$$

ifadesiyle tanımlayacağımız N_f parametresi, doğrusal olmamanın ölçütü olarak kullanılabilir. Bu ölçüt, n sayısından bağımsız olarak [0, 1) aralığında değerler alacak; değişik giriş ikili sayısına sahip fonksiyonların karşılaştırılmalarına olanak verecek; ve 100 N_f değeri de, $f(\mathbf{x})$'in yüzde kaç oranında doğrusal olmayan bir işlev olduğunu ölçecektir. Dikkat edilirse, (13) denklemindeki ε_f'nin sıfıra, (14) denklemindeki N_f'nin de bire eşit olması için, (11) eşitliğini tüm $\mathbf{a}$ vektörleri için sağlayabilen $f(\mathbf{x})$ işlevlerinin varlığı gereklidir.

Rothaus, doğrusallığa en uzak fonksiyonların kendisi tarafından tanımlanan bükük (bent) fonksiyonlar [12, 13] olduğunu göstermiştir. Bükük fonksiyonlar sadece çift sayıda giriş ikili (n çift) için tanımlıdır; ve bükük bir $f(\mathbf{x})$ işlevi için (7) denklemiyle tanımlanan N_f değerinin:

$$N_f = 2^{n-1} - 2^{(n/2)-1} \quad (15)$$

olduğu kanıtlanmıştır. (14) denklemiyle verilen N_f

parametresi tanımında normalizasyon faktörü olarak kullandığımız 2^{n-1} değeri yerine ($2^{n-1}-2^{(n/2)-1}$) seçerek, [0, 1] aralığında değişen yeni bir doğrusal olmama ölçütü de tanımlayabiliriz [11]:

$$\underline{N_f}=1-\text{maks}_{\mathbf{a}}\{\,|\,[\#\{f(\mathbf{x})=f(\mathbf{x}+\mathbf{a})\}/(2^{n-1}-2^{(n/2)-1})]-1\,|\,\} \qquad (16)$$

(14) denklemiyle tanımladığımız N_f parametresinin, literatürde (7), (8) ve (9) eşitlikleri ile tanımlanmış olan N_f değerinin 2^{n-1}'e bölünerek normalize edilmiş haline eşit olacağı kanıtlanabilir [11]. Aynı şekilde, (16) denklemiyle verilen $\underline{N_f}$ parametresi de N_f değerini (15) eşitliğindeki maksimum değerle normalize ederek bulunabilir[11]. Bu bölümün başında ayrıntısı verilmiş olan (7) denkleminden (8)'e geçişe ek olarak, çok daha fazla işlem basamağı içeren (8) eşitliğinden (9) ve (11) numaralı denklemlere geçişler de, yine aynı çalışmamızda gösterilmektedir [11].

5. Yerleşim Kutuları için Doğrusal Olmama Ölçütü ve Üç Örnek

Önceki bölümlerde, doğrusal olmama özelliği *n* ikillik vektörleri Z_2'ye eşleyen fonksiyonlar:

$$f_j : Z_2^n \rightarrow Z_2 \text{ için tanımlanmıştı.}$$

Blok şifrelerin yerleşim kutuları ise genel olarak *n* ikillik vektörleri *m* ikillik vektörlere eşlerler:

$$S:\ Z_2^n \rightarrow Z_2^m$$

S işlevinin herhangi bir çıkış vektörü, *m* tane f_j alt fonksiyonunu içermektedir. Literatürde, yerleşim kutularına ait doğrusal olmama ölçütünün, (7), (8), (9) ve (11) denklemlerinde her bir f_j alt fonksiyonu için verilen tanımlarla nasıl ilişkilendirileceğine dair pek çok yöntem önerilmiştir [9, 14, 15]. Kriptografik açıdan, *m* tane alt fonksiyon ve bunların tüm doğrusal kombinasyonları için hesaplanan en düşük doğrusal olmama faktörünü, yerleşim kutusunun doğrusal olmama ölçütü olarak seçmek uygun görülmüştür [1]:

$$N_S = \min_g \{N_g \mid g = \oplus_{j=1}^{m} c_j \cdot f_j,\ c_j \in Z_2,\ g \neq 0\} \qquad (17)$$

Bu tanımda, alt fonksiyonların tüm doğrusal kombinasyonları gözönüne alınmaktadır; çünkü tanımlanan *Ns* değişkeninin iyi bir ölçüt olabilmesi için basit transformasyonlardan etkilenmemesi gereklidir [1]. (17) denklemindeki alt fonksiyonlara ait N_g faktörleri normalize edilmiş $\underline{N_g}$ faktörleri olarak seçilirse, yerleşim kutularının doğrusal olmama faktörleri de, kutuların boyutundan bağımsız olarak bulunacaktır.

Bu çalışmada, üç blok şifrenin (DES, SAFER K-64 ve LOKI-97) s-kutuları için normalize edilmiş doğrusal olmama faktörleri ($\underline{N_S}$) hesaplanmış ve bulunan değerler Tablo 1'de gösterilmiştir.

Bu şifrelerden DES (Veri Şifreleme Standardı), 64 ikillik giriş metnini 56 ikillik anahtar kullanarak 64 ikillik çıkış metnine çeviren simetrik bir blok şifredir. 8 tane 6x4'lük yerleşim kutusu içerir [16]. SAFER K-64 (Güvenli ve Hızlı Şifreleme Yöntemi) 64 ikillik ham veriden 64 ikillik bir anahtarla 64 ikillik şifre oluşturan simetrik bir blok şifredir. Üstel ve logaritmik yerleşim kutuları olarak adlandırılan iki çeşit yerleşim kutusu vardır [17, 18] ve bu yerleşim kutuları birbirinin tersi işleve sahiptir. LOKI-97 ise 128 ikillik veriyi 128 ikillik şifreye çevirir; DES ve SAFER'ın aksine asimetrik bir blok şifredir. İki çeşit yerleşim kutusu bulunan LOKI-97 bu yerleşim kutularını iki katmanlı bir yerleşim-permütasyon ağında kullanır [19].

Tablo 1'e göre LOKI-97, DES ve SAFER K-64'e oranla daha doğrusallıktan uzak yerleşim kutularına sahiptir. SAFER K-64'un iki yerleşim kutusu da aynı derecede doğrusallık göstermektedir; bunun nedeni, iki yerleşim kutusu fonksiyonunun tam birbirinin tersi olmasıdır. Birbirinin tersi olan fonksiyonlar doğrusalımsı fonksiyonlara aynı uzaklıktadırlar; bu nedenle de aynı doğrusal olmama değerine sahiptirler.

Tablo1: DES, SAFER K-64 ve LOKI-97'nin Normalize Edilmiş Doğrusal Olmama Faktörleri

DES (6x4)		SAFER K-64		LOKI-97	
S_1	0.500	$S_{\text{üstel}}$		S_1	
S_2	0.571				
S_3	0.571	8x8	0.683	11x8	0.842
S_4	0.571				
S_5	0.428	$S_{\text{logaritma}}$		S_2	
S_6	0.643				
S_7	0.500	8x8	0.683	13x8	0.940
S_8	0.571				

Tablo 1'den çıkarılabilecek başka bir sonuç ise, yerleşim kutusuna giren ikil sayısı arttıkça daha yüksek doğrusal olmama değerlerinin gözlenmiş olmasıdır. LOKI-97'nin ikinci s-kutusu, %94'lük başarımıyla, neredeyse mükemmel doğrusal olmama durumuna aday görünmektedir.

7. Sonuçlar

Doğrusal olmama özelliği blok şifreler için kullanılan bir güvenilirlik ölçütüdür. Doğrusal olmama, bir fonksiyonun tüm değişkenleri üzerinde doğrusalımsı fonksiyonlardan farklı sonuç verdiği durumların sayısı olarak tanımlanabileceği gibi, bir fonksiyonun kendine *en yakın doğrusalımsı fonksiyona olan Hamming* uzaklığı olarak da tanımlanabilir. Pek çok farklı doğrusal olmama tanımları bulunmakla birlikte, bu tanımlar esas olarak birbirinin aynıdır; eşdeğerlikleri gösterilebilir.

Literatürdeki tüm doğrusal olmama tanımları, fonksiyona giren ikil sayısına bağlı olarak yapılmakta, bu durum farklı boyutlu yerleşim kutularına sahip olan blok şifrelerin karşılaştırılabilmesine engel olmaktadır. Bu çalışmada 14. ve 16. denklemlerle tanımladığımız normalize edilmiş doğrusal olmama ölçütleri ise bu sorunu ortadan kaldırmaktadır.

Normalize edilmiş doğrusal olmama ölçütü kullanılarak, üç tanınmış blok şifre karşılaştırılmıştır. Yerleşim kutularının en düşük doğrusal olmama faktörlerine bakılırsa, DES %42, SAFER K-64 %68, LOKI-97 ise %84 düzeyinde doğrusallıktan uzaktır. LOKI-97'nin diğer yerleşim kutusu için bulunan %94 değeri ise, mükemmel doğrusal olmama durumuna oldukça yakın görünmektedir.

Kaynakça

[1] Willi Meier and Othmar Staffelbach, "Nonlinearity Criteria For Cryptographic Functions", Advances in Cryptology: Proc. EUROCRYPT'89, Springler-Verlag, s. 549-562, 1989.

[2] J. F. Dillon, "A Survey of Bent Functions. The NSA Technical Journal, s. 191-215, 1972.

[3] Josef P. Pieprzyk, "Nonlinearity of Exponent Permutations", Advances in Cryptology: Proc. EUROCRYPT'89, Springler-Verlag, s. 81-93, 1989.

[4] Kaisa Nyberg, "Constructions of Bent Functions and Difference Sets", Advances in Cryptology: Proc. EUROCRYPT'90, Springler-Verlag, s. 152-161, 1991.

[5] Kaisa Nyberg, "On the Construction of Highly Nonlinear Permutations", Advances in Cryptology: Proc.EUROCRYPT'92, s.93-99, 1993.

[6] C. Carlet, "Partially Bent Functions", Advances in Cryptology: Proc. CRYPTO'92, Springler-Verlag, s. 281-291. 1993.

[7] T. Beth and C. Ding, "On Almost Perfect Nonlinear Permutations", Advances in Cryptology: Proc. CRYPTO'93, Springler-Verlag, s. 66-77, 1994.

[8] C. Carlet, "Two New Classes of Bent Functions", Advances in Cryptology: Proceedings of EUROCRYPT'93, Springler-Verlag, s. 78-102, 1994.

[9] X.Zhang, Y.Zheng, H.Imai, "Relating Differential Distribution Tables to Other Properties of Substitution Boxes", Designs, Codes and Cryp., 19, s. 45-63, 1998.

[10] B. Preneel, W. V. Leekvijck, L. V. London, R. Govaerts and J. Vandewalle, " Propagation *Characteristics of Boolean Functions*", Advances in Cryptology: Proc.EUROCRYPT'90, s. 162-174, 1991.

[11] G.Yıldırım, "Nonlinearity and Avalanche Properties of Block Ciphers", Yüksek Lisans Tezi, ODTÜ Elektrik-Elektronik Müh. Böl., 2000.

[12] O. S. Rothaus, "On Bent Functions", Journal of Combinatorial Theory, s. 300-305, 1976.

[13] Xian-Mo Zhang, "On the Difficulty of Constructing Cryptographically Strong Substitution Boxes", Journal of Universal Computer Science, sayı 2, s. 147-162, 1996.

[14] J.Pieprzyk, and G.Finkelstein, "Permutations that Maximize Non-Linearity and Their Cryptographic Significance", Advances in Cryptology: Proc. CRYPTO'88, Springler-Verlag, s. 63-74, 1989.

[15] Jennifer Sebery, Xian-Mo Zhang and Yuliang Zheng, "Relationships Among Nonlinearity Criteria", Journal of Universal Computer Science, sayı 1, s. 45-51, 1997.

[16] D. R, Stinson, "Cryptography: Theory and Practice", CRC Press, 1995.

[17] J.Kelsey, B.Shneier and D.Wagner, "Key Schedule Weaknesses in SAFER+", s.1-14, 1999.

[18] J.L. Massey, "SAFER K-64: A Byte-Oriented Block-Ciphering Algorithm", Fast Software Encryption, Proc. Cambridge Security Workshop, Cambridge, U.K., Springler-Verlag, s. 1-17, 1994.

[19] Lawrence Brown, Josef Pieprzyk and Jennifer Seberry, "LOKI- A Cryptographic Primitive for Authentication and Secrecy Applications", Advances in Cryptology: Proc. CRYPTO'98, Springler-Verlag, s. 229-236, 1998.