AES S-kutusuna Benzer S-kutularının Cebirsel İfadelerini Elde Etmek İçin Yeni Bir Yöntem

[1]Osman KARAAHMETOĞLU, [1]M.Tolga SAKALLI, [2]Ercan BULUŞ

[1]Trakya Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği, Edirne
[1]Trakya Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği, Edirne
[2]Namık Kemal Üniversitesi, Çorlu Mühendislik Fakültesi, Bilgisayar Mühendisliği, Çorlu-Tekirdağ
okaraahmetoglu@fintek.com.tr, tolga@trakya.edu.tr, ercanbulus@nku.edu.tr

ABSTRACT

S-boxes are vital elements in the design of symmetric ciphers. Moreover, S-boxes are only nonlinear and the most important component of a block cipher. To date, the techniques for the construction of S-boxes have included pseudo-random generation, finite field inversion, power mappings and heuristic techniques. From these techniques, the use of finite field inversion operation in the construction of an S-box yields linear approximation and difference distribution tables in which the entries are close to uniform. Therefore, inversion mapping or power mapping over a finite field are so popular design techniques in the design of algebraic S-boxes. However, the place of an affine transformation added to an algebraic S-box changes the number of terms in the algebraic expression of an S-box. In this study, we present a new method to resolve the algebraic expression of AES S-box like S-boxes according to the given probable cases.

Key words: S-boxes, AES S-box, Algebraic Expression

1. GİRİŞ

S-kutuları blok ve akan şifreleme algoritmalarında kullanılan ve şifreye güvenliğini veren en önemli yapıdır. Bir S-kutusu n giriş bitinin farklı m çıkış bitine dönüşümünü yapar ve şifrede yerdeğiştirme görevini yerine getirir. S-kutularının doyurması gereken bazı kriptografik özellikler vardır [1]. Bunlar sırasıyla doğrusal olmama, doğrusal saldırılar için önemli olan LAT (Linear Approximation Table-Doğrusal Yaklaşım Tablosu), diferansiyel saldırılar için önemli olan DDT (Difference Distribution Table-Fark Dağılım Tablosu-XOR Tablosu), bütünlük (completeness), çığ (avalanche), katı çığ (strict avalanche) gibi verilebilir.

Bunun yanında şifreye yapılan saldırılar S-kutusunu hedef almaktadır ve S-kutusunun bu saldırılara karşı dayanıklılığı şifrenin de gücü ile ilişkilidir. Dolayısıyla saldırılara karşı dayanıklı S-kutusu tasarımları gerçekleştirilmelidir. 2001 yılında AES (Advanced Encryption Standard) olarak seçilen doğrusal ve diferansiyel saldırılara dayanıklı olan Rijndael şifresi Nyberg'in [2] önerdiği sonlu cisimde ters haritalama tabanlı 8-bit giriş ve 8-bit çıkışlı bir S-kutusunu kullanmaktadır ve cebirsel ifadesi aşağıdaki gibidir:

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

Rijndael şifresinde kullanılan S-kutusunun en önemli sakıncası yukarıda gösterilen cebirsel ifadenin basitliğidir. Bu basit cebirsel ifade interpolasyon saldırıları gibi bazı cebirsel saldırılara neden olabilmektedir. İnterpolasyon saldırılarına karşı, AES S-kutusunun tek terimden oluşmasının getirdiği zayıflık ters haritalama işleminin sonuna eklenen bir doğrusal dönüşüm ile giderilmeye çalışılmıştır. Böylelikle aşağıdaki ifadeden de görüldüğü gibi AES S-kutusunun cebirsel ifadesindeki terim sayısı kullanılan doğrusal dönüşüm sayesinde 1'den 9'a çıktığı Lagrange interpolasyonu kullanılarak gösterilmiştir [3][4].

$$S(x) = "05"x^{254} + "09"x^{253} + "f9"x^{251} + "25"x^{247} + "f4"x^{239} + "01"x^{223} + "b5"x^{191} + "8f"x^{127} + "63".$$

Diğer yandan AES şifresine ek olarak literatürde Square [5], Shark [6] gibi şifrelerde kullanılan S-kutuları sonlu cisim $GF(2^n)$ üzerine ters haritalama tabanlıdır ve $GF(2)$ üzerine ikili bir doğrusal dönüşümü ters haritalama işleminin çıkışında kullanmaktadırlar. Buna ek olarak literatürdeki diğer bir blok şifre olan Camellia [7] ise ikili bir doğrusal dönüşümü ters haritalama işleminden önce ve sonra kullanmaktadır. Bu da doğrusal dönüşümün kullanılacağı yere ilişkin olarak üç farklı durumu işaret etmektedir:

- İkili doğrusal dönüşümü ters haritalama işleminden sonra kullanmak (durum 1, örnek AES),
- İkili doğrusal dönüşümü ters haritalama işleminden önce kullanmak (durum 2),
- İkili doğrusal dönüşümleri ters haritalama işleminden hem önce hem de sonra kullanmak (durum 3, örnek Camellia).

Bu bahsedilen durumlardan durum 2 ve durum 3 ile tasarlanacak S-kutuları cebirsel ifadesindeki terim sayısı açısından durum 1 ile tasarlanacak S-kutusuna göre önemli bir iyileştirme sunmaktadır [8]. Buna ek olarak uygulanacak doğrusal dönüşümün yeri diğer kriptografik özellikleri değiştirmemektedir. Bu çalışmada belirtilen durumlara göre tasarlanacak S-kutuları için sonlu cisim teorisinden de faydalanılarak hızlı, durum 2 ve durum 3 ile tasarlanacak S-kutularının neden terim sayısında iyileştirme yaptığını açıklayıcı bir yöntem geliştirilmiştir. Buna ek olarak sunulan yöntem Lagrange interpolasyonuna alternatif ve daha hızlı bir yöntemdir.

2. MATEMATİK ALTYAPI

Bu bölümde makale boyunca kullanılacak olan matematiksel alt yapının bir sunumu yapılacaktır. Sonlu cisimler teorisi ile ilgili olarak daha ayrıntılı bilgi [9] ve [10]'dan elde edilebilir. Bu makalede gerekli görüldüğünde cisim elemanları hexadecimal gösterimde ifade edilebilir. Dolayısıyla α, $GF(2^n)$ sonlu cismini üretmek için kullanılan ilkel eleman olmak üzere;

$$b_{n-1}\alpha^{n-1} + b_{n-2}\alpha^{n-2} + ... + b_0\ ,\ b_i \in \{0,1\}$$

sonlu cisim elemanı $(b_{n-1}b_{n-2}...b_0)$ bitlerini içeren hexadecimal sayı olarak temsil edilebilir.

$F = GF(p),\ K = GF(p^n)$ ve $\lambda \in K$ olsun. O zaman alt cisim F 'in λ 'ya göre trace (iz) fonksiyonu

$$Tr_F^K(\lambda) = \lambda + \lambda^p + \lambda^{p^2} + ... + \lambda^{p^{n-1}}$$

şeklinde ifade edilebilir ve karışıklığın olmayacağı durumlarda Tr_F^K ifadesindeki alt ve üst indisler göz ardı edilebilir.

$\{\alpha_0.....\alpha_{n-1}\}$, $GF(2)$ üzerine $GF(2^n)$ 'in herhangi bir tabanı olmak üzere; $\{\beta_0.....\beta_{n-1}\}$ buna karşı gelen dual taban ve $f(x_0, x_1, ..., x_{n-1}) = (f_0(x), ..., f_{n-1}(x))$ ise $GF(2^n)$ üzerine bir permütasyon olsun. O zaman $g(x) = \sum_{i=0}^{n-1} \alpha_i f_i(x_0, ...x_{n-1})$ de $GF(2^n)$ üzerine bijektif bir haritadır. $f(x)$ 'in her çıkış koordinatı, $x = \sum_{i=0}^{n-1} x_i\alpha_i$ olmak üzere, (1) ifadesindeki gibi verilebilir [11][12].

$$f_i(x) = Tr(g(x)\,\beta_i) \tag{1}$$

Buna ek olarak (1) ifadesinde β_i dual taban değerleri (2) ifadesinde gösterildiği gibi hesaplanabilir [11][12].

$$\beta_i = \sum_{k=0}^{n-1} b_{ki}\alpha_k \tag{2}$$

(2) ifadesinde $B = \left[b_{ij}\right] = A^{-1}$ ve $A = \left[a_{ij}\right]$ olmak üzere $n \times n$ boyutundaki A matrisi elemanları

$$a_{ij} = Tr(\alpha_i\alpha_j), \qquad 0 \le i, j \le n-1 \tag{3}$$

(3) ifadesindeki gibi gösterilebilir. $A = \left[a_{ij}\right]$ şeklindeki A matrisi (4) ifadesinde açık biçimde gösterilmiştir.

$$A = \begin{bmatrix} Tr(\alpha_0\alpha_0) & Tr(\alpha_0\alpha_1) & ..... & Tr(\alpha_0\alpha_{n-1}) \\ Tr(\alpha_1\alpha_0) & Tr(\alpha_1\alpha_1) & ..... & Tr(\alpha_1\alpha_{n-1}) \\ & & . & \\ & & . & \\ Tr(\alpha_{n-1}\alpha_0) & Tr(\alpha_{n-1}\alpha_1) & .... & Tr(\alpha_{n-1}\alpha_{n-1}) \end{bmatrix} \tag{4}$$

Böylece giriş bitlerine uygulanacak dönüşüm işleminden sonraki çıkış koordinatları (5) ifadesi ile gösterilebilir.

$$f_i\ ,\quad 0 \le i \le n\text{-}1 \tag{5}$$

Giriş bitlerine uygulanacak doğrusal dönüşüm sonucu elde edilen çıkış bitlerini kullanarak doğrusal dönüşümün cebirsel ifadesi (6)'daki gibi elde edilebilir.

$$A(x) = \sum_{i=0}^{n-1} f_i\alpha^i \tag{6}$$

Örnek 1, yukarıdaki tanım ve matematik alt yapıyı kullanarak AES S-kutusunun doğrusal dönüşümünün cebirsel ifadesinin elde edilişini göstermektedir.

Örnek 1. AES S-kutusunun tasarımında kullanılan doğrusal dönüşümü düşünelim. $P(x) = x^8 + x^4 + x^3 + x + 1$ indirgenemez polinomu ile oluşturulan sonlu cisimde bu ikili doğrusal dönüşümün cebirsel ifadesini bulmaya çalışalım. α, $P(x)$ polinomunun bir kökü olsun. $\beta = \alpha + 1$ ise ilkel elemanımız olsun (α, tüm cisim elemanlarını üretmemektedir). O zaman x_i giriş biti değerleri β değerlerine bağlı olarak Bölüm 2' de verilen tanımlara göre;

$$\begin{aligned} x_0 &= Tr(\beta^{228}x), & x_4 &= Tr(\beta^{73}x), \\ x_1 &= Tr(\beta^{204}x), & x_5 &= Tr(\beta^{48}x), \\ x_2 &= Tr(\beta^{179}x), & x_6 &= Tr(\beta^{23}x), \\ x_3 &= Tr(\beta^{2}x), & x_7 &= Tr(\beta^{253}x). \end{aligned} \tag{7}$$

(7) ifadesindeki gibi elde edilebilir. AES S-kutusunda kullanılan doğrusal matrisin [3] çıkış koordinatları $f_0, f_1, ..., f_7$ ise (8) ifadesindeki gibi elde edilebilir.

$$\begin{aligned} f_0 &= Tr(\beta^{166}x) + 1, & f_4 &= Tr(\beta^{72}x), \\ f_1 &= Tr(\beta^{53}x) + 1, & f_5 &= Tr(\beta^{76}x) + 1, \\ f_2 &= Tr(\beta^{36}x), & f_6 &= Tr(\beta^{51}x) + 1, \\ f_3 &= Tr(\beta^{11}x), & f_7 &= Tr(\beta^{26}x). \end{aligned} \tag{8}$$

Doğrusal matris çıkış koordinatlarını kullanarak doğrusal dönüşümün cebirsel ifadesi polinom taban değerlerinin $\{1, \alpha, \alpha^2, ..., \alpha^7\}$ olduğu bilgisinden yola çıkarak (6) ifadesinde verildiği gibi

$$A(x) = f_0 + \alpha f_1 + \alpha^2 f_2 + \alpha^3 f_3 + ... + \alpha^7 f_7$$

şeklinde tekrar yazılabilir. Bunun yanında $GF(2^8)$ sonlu cisminde $\{1, \alpha, \alpha^2, ..., \alpha^7\}$ polinom taban değerleri β cinsinden

$$\alpha = \beta^{25}, \alpha^2 = \beta^{50}, \alpha^3 = \beta^{75}, \alpha^4 = \beta^{100}, \alpha^5 = \beta^{125},$$
$$\alpha^6 = \beta^{150}, \alpha^7 = \beta^{175}$$

şeklinde verilebilir. Elde edilen polinom taban değerleri $A(x)$ ifadesinde yerine konursa doğrusal dönüşümün cebirsel ifadesi $A(x)$ aşağıdaki şekli alır:

$$\begin{aligned}A(x) = &(\beta^{166}x + (\beta^{166})^2x^2 + \ldots\ldots + (\beta^{166})^{128}x^{128})\\ &+ \beta^{25}(\beta^{53}x + (\beta^{53})^2x^2 + \ldots\ldots + (\beta^{53})^{128}x^{128})\\ &+ \beta^{50}(\beta^{36}x + (\beta^{36})^2x^2 + \ldots\ldots + (\beta^{36})^{128}x^{128})\\ &+ \beta^{75}(\beta^{11}x + (\beta^{11})^2x^2 + \ldots\ldots + (\beta^{11})^{128}x^{128})\\ &+ \beta^{100}(\beta^{72}x + (\beta^{72})^2x^2 + \ldots\ldots + (\beta^{72})^{128}x^{128})\\ &+ \beta^{125}(\beta^{76}x + (\beta^{76})^2x^2 + \ldots\ldots + (\beta^{76})^{128}x^{128})\\ &+ \beta^{150}(\beta^{51}x + (\beta^{51})^2x^2 + \ldots\ldots + (\beta^{51})^{128}x^{128})\\ &+ \beta^{175}(\beta^{26}x + (\beta^{26})^2x^2 + \ldots\ldots + (\beta^{26})^{128}x^{128}) + "63".\end{aligned}$$

$A(x)$ ifadesindeki x teriminin katsayısı A_0'ı

$\beta^{166}, \beta^{(53+25) \bmod 255}, \beta^{(50+36) \bmod 255}, \beta^{(75+11) \bmod 255}, \beta^{(175+26) \bmod 255}$
$\beta^{(100+72) \bmod 255}, \beta^{(125+76) \bmod 255}, \beta^{(150+51) \bmod 255},$

değerlerinin toplamı şeklinde ifade edilebileceğinden yola çıkarak

$$A_0 = \beta^{166} + \beta^{78} + \beta^{86} + \beta^{86} + \beta^{172} + \beta^{201} + \beta^{201} + \beta^{201},$$
$$A_0 = "2A" + "78" + "DC" + "DC" + "7A" + "2D" + "2D" + "2D",$$
$$A_0 = "05"$$

şeklinde elde edebiliriz. Diğer terimlerin katsayıları da aynı şekilde elde edildikten sonra sonuçlanan cebirsel ifade aşağıdaki gibidir:

$$\begin{aligned}A(x) = &"63" + "05"x + "09"x^2 + "f9"x^4 + "25"x^8 +\\ &"f4"x^{16} + "01"x^{32} + "b5"x^{64} + "8f"x^{128}.\end{aligned}$$

3. CEBİRSEL İFADENİN ELDE EDİLMESİ İÇİN ÖNE SÜRÜLEN YENİ YÖNTEM

Bu bölümde öne sürülen cebirsel yöntem ile birlikte bu yöntem için gerekli teori ve tanımlar sunulacaktır.

Tanım 1. $L(x) = \sum_{i=0}^{t} \beta_i x^{2^i}$ şeklinde ve β_i, $GF(2^n)$'in elemanı olmak üzere verilen özel biçime sahip polinoma $GF(2^n)$ üzerine doğrusallaştırılmış polinom denir.

Tanım 2. Bir tamsayı d'yi içeren $\bmod N$'e göre cyclotomic koset

$$C_d = \{d, dp, \ldots, dp^{n-1}\} \pmod N$$

şeklinde bir kümedir ve d, $dp^n \equiv d \pmod N$ olacak şekilde en küçük tamsayıdır.

Önerme 1. A, $GF(2^n)$ üzerine doğrusal bir haritalama olsun. O zaman $A(x)$, $x \in GF(2^n)$ olmak üzere $GF(2^n)$ üzerine doğrusallaştırılmış bir polinoma dayalı olarak

$$A(x) = \sum_{i=0}^{n-1} \beta_i x^{2^i}$$

şeklinde ifade edilebilir.

Önerme 2. F_2^n üzerine tersi alınabilir doğrusal dönüşümlerin kümesi ile $GF(2^n)$ üzerine doğrusallaştırılmış polinomların kümesi arasında birebir ilişki vardır [4].

Önerme 3. $GF(2^n)$'in bir fonksiyonu $F(x) = x^d$ olsun ve bu fonksiyon $f(x_1,\ldots,x_n) = (f_1(x),\ldots,f_n(x))$ boole fonksiyonuna karşılık gelsin. O zaman $f(x_1,\ldots,x_n)$'nin çıkış koordinatlarına uygulanan doğrusal bir dönüşüm ile elde edilen boole fonksiyonuna karşılık gelen $G(x)$ aşağıdaki şekilde ifade edilir.

$$G(x) = \sum_{i=0}^{n-1} b_i x^{d2^i}, \quad c_i \in GF(2^n)$$

Eğer doğrusal dönüşüm, affine bir dönüşüm ile yer değiştirilirse, o zaman $G(x)$,

$$G(x) = \sum_{i=0}^{n-1} b_i x^{d2^i} + c_n, \quad c_i \in GF(2^n)$$

şeklinde yazılabilir [4]. Gerçekte yukarıdaki tanım ve teoriler ışığı altında bir üs haritalamadan sonra uygulanacak doğrusal dönüşüm sonucunda üs fonksiyonu d'nin cyclotomic kosetinde bulunan terimler cebirsel ifadede yer alacaktır diyebiliriz.

Örnek 2. AES S-kutusunun cebirsel ifadesi, Örnek 1' de elde edilen doğrusal dönüşümün cebirsel ifadesinde x yerine x^{254} koyarak ve $x \in GF(2^n)$ için $x^a = x^{a \bmod 2^n - 1}$ olduğundan yola çıkarak

$$\begin{aligned}S(x) = &"63" + "05"x^{254} + "09"x^{254\times2} + "f9"x^{254\times4} + "25"x^{254\times8} +\\ &"f4"x^{254\times16} + "01"x^{254\times32} + "b5"x^{254\times64} + "8f"x^{254\times128},\end{aligned}$$

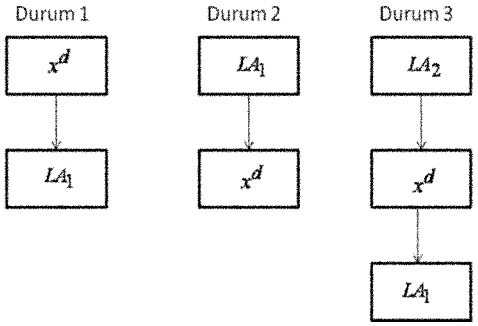
$$\begin{aligned}S(x) = &"63" + 05"x^{254} + "09"x^{253} + "f9"x^{251} + "25"x^{247} +\\ &"f4"x^{239} + "01"x^{223} + "b5"x^{191} + "8f"x^{127}\end{aligned}$$

şeklinde elde edilebilir.

Teorem 1. $GF(2^n)$'in bir fonksiyonu $F(x) = x^d$ olsun ve bu fonksiyon $f(x_1,\ldots,x_n) = (f_1(x),\ldots,f_n(x))$ boole fonksiyonuna karşılık gelsin. $G(x)$ ise $f(x_1,\ldots,x_n)$ sabitlenirken $x_1,\ldots,x_n$ giriş bitlerine doğrusal bir dönüşüm uygulanarak elde edilen bir boole haritasına karşılık gelen bir fonksiyon olsun. O zaman $G(x)$,

$$G(x) = \sum_{i=0}^{2^n-1} b_i x^i \qquad wt(i) > wt(d) \text{ için } b_i = 0$$

şeklinde ifade edilir [13]. Teorem 1, doğrusal dönüşümün üs fonksiyonunun önüne uygulandığında oluşacak cebirsel ifadenin terimleri üzerindeki etkisini göstermektedir ve d üs fonksiyonunun Hamming ağırlığına eşit ve küçük Hamming ağırlığında üsse sahip terimlerin cebirsel ifadede ortaya çıkacağını göstermektedir. Kısacası, Teorem 1 durum 2 için cebirsel ifadedeki terim sayısı hakkında bilgi vermektedir.



Şekil 1. AES S-kutusu Benzeri S-kutuları Tasarımında Olası Durumların Gösterimi

Şekil 1, S-kutusu tasarımında doğrusal dönüşümün yeri ile ilgili olarak olası durumların gösterimini yapmaktadır. Şekil 1'e dayalı olarak durum 1, 2 ve 3 için cebirsel ifadenin hesaplanması aşağıdaki gibi özetlenebilir.

Durum 1 için;

- Verilen teoriyi kullanarak LA_1 doğrusal dönüşümüne karşılık gelen ve bu dönüşümün cebirsel ifadesi olan $LA_1(x)$ 'i hesapla,
- $LA_1(x)$ 'te x yerine x^d koy,
- $LA_1(x^d)$, S-kutusunun cebirsel ifadesidir.

Durum 2 için;

- Verilen teoriyi kullanarak LA_1 doğrusal dönüşümüne karşılık gelen ve bu dönüşümün cebirsel ifadesi olan $LA_1(x)$ 'i hesapla,
- x^d 'de x yerine $LA_1(x)$ 'i koy,
- S-kutusunun cebirsel ifadesini $(LA_1(x))^d$ ifadesini hesaplayarak elde et.

Durum 3 için;

- Verilen teoriyi kullanarak LA_1 ve LA_2 doğrusal dönüşümlerine karşılık gelen ve bu dönüşümlerin cebirsel ifadesi olan $LA_1(x)$ ve $LA_2(x)$ 'i hesapla,
- $LA_1(x^d)$ 'de x yerine $LA_2(x)$ 'i koy,
- S-kutusunun cebirsel ifadesini $LA_1(LA_2(x)^d)$ ifadesini hesaplayarak elde et.

Örnek 3. $n=8$ ve $GF(2^8)$, AES tanımlamalarında olduğu gibi $P(x)=x^8+x^4+x^3+x+1$ indirgenemez polinomu ile tanımlanmış olsun. Buna ek olarak LA_1 ve LA_2 doğrusal dönüşümlerinin cebirsel ifadesi aşağıdaki gibi olsun.

$$LA_1(x) = "63"+"05"x+"09"x^2+"f9"x^4+"25"x^8+"f4"x^{16}+"01"x^{32}+ "b5"x^{64}+"8f"x^{128}$$

$$LA_2(x) = "33"+"52"x+"77"x^2+"13"x^4+"e0"x^8+"fe"x^{16}+"9e"x^{32}+ "96"x^{64}+"27"x^{128}$$

S-kutusu $x \to x^{254}$ haritalaması ile birlikte durum 2'de olduğu gibi tasarlanırsa cebirsel ifadesi aşağıdaki gibi elde edilebilir:

$$S(x) = (LA_1(x))^{254},$$

$$S(x) = ("63"+"05"x+"09"x^2+\ldots+"b5"x^{64}+"8f"x^{128})^{254}.$$

S-kutusu $x \to x^{254}$ haritalaması ile birlikte durum 3'te olduğu gibi tasarlanırsa cebirsel ifadesi aşağıdaki gibi elde edilebilir:

$$S(x) = "63"+05"(LA_2(x))^{254}+"09"(LA_2(x))^{253}+"f9"(LA_2(x))^{251}+ "25"(LA_2(x))^{247}+"f4"(LA_2(x))^{239}+"01"(LA_2(x))^{223}+"b5"(LA_2(x))^{191}+ "8f"(LA_2(x))^{127},$$

$$\begin{aligned} S(x) = {} & 05"("33"+"52"x+"72"x^2+\ldots+"9e"x^{32}+"96"x^{64}+"27"x^{128})^{254}+ \\ & "09"("33"+"52"x+"72"x^2+\ldots+"9e"x^{32}+"96"x^{64}+"27"x^{128})^{253}+ \\ & "f9"("33"+"52"x+"72"x^2+\ldots+"9e"x^{32}+"96"x^{64}+"27"x^{128})^{251}+ \\ & . \\ & . \\ & "8f"("33"+"52"x+"72"x^2+\ldots+"9e"x^{32}+"96"x^{64}+"27"x^{128})^{127}+"63". \end{aligned}$$

Tablo1. Örnekte verilen durum 3'e göre tasarlanan S-kutusu

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	C3	18	27	80	15	34	FD	F7	2B	FE	6B	77	F0	CA	D4	72
1	1A	1B	E3	D6	CF	6A	D1	B1	21	10	9D	40	85	D0	F9	9F
2	66	48	C1	57	8A	E8	78	B4	E9	CE	D9	98	68	8C	99	BB
3	0A	49	95	AC	08	6C	C8	4E	14	DE	2A	4F	17	CD	A7	19
4	89	E6	B0	0F	28	1E	E1	94	74	BD	1C	2E	F6	3E	61	9E
5	13	97	64	3D	0B	EE	60	88	F4	7A	8D	6D	24	32	C2	79
6	C9	59	9C	AF	AB	01	63	C5	E5	D8	36	26	05	C7	07	75
7	AA	4D	50	7F	F3	B6	51	F5	BE	4C	20	ED	5A	83	52	84
8	E7	A9	AE	56	91	62	3A	06	C4	73	44	0C	22	DC	B8	5E
9	BA	C6	8B	DD	86	B9	B5	03	41	16	42	A1	69	11	87	55
A	53	5B	58	CB	29	B3	2C	6E	45	A8	33	EF	92	8F	DA	FF
B	B7	CC	31	A5	EB	E2	23	96	AD	C0	47	82	F2	7B	67	D7
C	A3	38	D2	BC	3C	02	FB	43	3B	2F	A0	09	FC	00	39	4A
D	7C	6F	76	30	A4	A2	7D	FA	12	B2	9A	04	3F	93	F1	71
E	81	90	DB	46	5D	7E	EC	5F	D3	E4	5C	E0	D5	37	EA	65
F	F8	8E	DF	9B	54	2D	0D	BF	35	1D	0E	70	A6	25	1F	4B

Tablo 1' de verilen S-kutusu [12] $x \to x^{254}$ üs haritalaması ve Örnek 3'te verilen LA_1 ve LA_2 doğrusal dönüşümleri ile birlikte durum 3'e göre tasarlanmıştır. S-kutusunun cebirsel ifadesi 255 terim içermektedir ve bu ifade aşağıda kısaca gösterilmiştir. Ek-A da bu S-kutusunun aşağıda verilen yöntem kullanılarak elde edilen cebirsel ifadesi ayrıntılı olarak gösterilmiştir.

$$S(x) = "1c"x^{254} + "1e"x^{253} + "16"x^{252} + "98"x^{251} + \ldots + "87"x^2 + "e7"x + "c3".$$

Gerek durum 2 de gerekse durum 3'te cebirsel ifadenin elde edilmesinde gerekli olan 9 terimli doğrusal dönüşümün 254' üncü kuvvetini almak yüksek iş yükü olarak görülebilir. Bunun için biz hızlı bir hesaplama yöntemi geliştirdik ve bu yöntem tüm $x \to x^{254}$ haritalama tabanlı tasarlanacak S-kutuları için uygulanabilir. Bu hesaplama yöntemi aşağıdaki gibi verilebilir:

- İlk olarak $LA_2(x)^2, LA_2(x)^4, LA_2(x)^8, LA_2(x)^{16}, LA_2(x)^{32}, LA_2(x)^{64}$ ifadelerini çarpma ve kare alma işlemlerini kullanarak elde et. Bu işlem 6 polinom çarpma işlemine denk düşer.
- $LA_2(x)^{127}$ ifadesini yukarıdaki ifadeleri çarparak elde et. Bu işlem de 5 polinom çarpma işlemine denk düşer.
- $LA_2(x)^{191} = LA_2(x)^{127}.LA_2(x)^{64}$,
  $LA_2(x)^{223} = LA_2(x)^{191}.LA_2(x)^{32}$,
  $LA_2(x)^{239} = LA_2(x)^{223}.LA_2(x)^{16}$,
  $LA_2(x)^{247} = LA_2(x)^{239}.LA_2(x)^{8}$,
  $LA_2(x)^{251} = LA_2(x)^{247}.LA_2(x)^{4}$,
  $LA_2(x)^{253} = LA_2(x)^{251}.LA_2(x)^{2}$,
  $LA_2(x)^{254} = LA_2(x)^{253}.LA_2(x)^{1}$ ifadelerini çarparak elde et. Bu işlemlerde 7 çarpma işlemi eder ve sonuç olarak 18 polinom çarpma işlemi ile istenen tüm doğrusal dönüşümlerin üsleri elde edilir.

Durum 2 için ise hesaplama yöntemi aşağıdaki gibi verilebilir:

- İlk olarak $LA_1(x)^2, LA_1(x)^4, LA_1(x)^8, LA_1(x)^{16}, LA_1(x)^{32}, LA_1(x)^{64}, LA_1(x)^{128}$ ifadelerini çarpma ve kare alma işlemlerini kullanarak elde et. Bu işlem 7 polinom çarpma işlemine denk düşer.
- $LA_1(x)^{254}$ ifadesini yukarıdaki ifadeleri çarparak elde et. Bu işlem de 6 polinom çarpma işlemine denk düşer. Bu işlemlerde toplam 13 polinom çarpması ile sonuçlanır.

4. SONUÇLAR

Çalışmamızda AES S-kutusu benzeri S-kutularının cebirsel ifadesinin hesaplanması için hızlı ve cebirsel ifadelerinde bulundurdukları terim sayılarını tasarlandıkları üs haritalamasına göre gösteren bir yöntem geliştirilmiştir. Örneğin Tablo 1'de verilen ve $x \to x^{254}$ haritalaması tabanlı S-kutusunun cebirsel ifadesi 255 terim içermekte ve cebirsel ifadesinin derecesi 254'tür. Bu cebirsel ifade geliştirilen yöntemle 40 milisaniye civarında bir sürede 2 GHz işlemcili bir bilgisayar ile elde edilmiştir. Buna ek olarak diğer üslerle tasarlanacak S-kutuları için benzeri hesaplama yöntemleri geliştirilebilir ve görünürde ki hesaplama ile ilgili yüksek iş yükü çok makul seviyelere indirilebilir. Verilen hesaplama yönteminde sonlu cisimde çarpma işlemleri çok hızlı olarak gerçeklenebileceği için polinomsal çarpma işlemi üzerinde durulmuştur. Diğer yandan S-kutusu durum 2 ya da durum 3 ile $x \to x^7$ haritalama yöntemi ile tasarlanmış olsaydı cebirsel ifadesinin 93 terim içereceği ve derecesinin de 224 olacağı söylenebilirdi. Nitekim bu tip bir S-kutusu için de bu uygulanmış ve bahsedilen sonuçlar gözlenmiştir.

5. KAYNAKLAR

[1] Sakallı M. T., Buluş E., Şahin A., Büyüksaraçoğlu F., "*Ters Haritalama Tabanlı S-kutularının Cebirsel Açıdan İyileştirilmesi*", ISC'07 Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara-Türkiye, 13–14 Aralık 2007.

[2] Nyberg K., "*Differentially uniform mappings for cryptography*", Proceedings of Eurocrypt'93, Lecture Notes in Computer Science, Springer, Berlin, vol. 765, pp. 55-64, 1994.

[3] Federal Information Processing Standards Publication (FIPS 197), *Advanced Encryption Standard (AES)*, 26 November 2001.

[4] Youssef A. M., Tavares S. E., Gong G., "*On Some probabilistic approximations for AES-like s-boxes*", Discrete Mathematics, Elsevier, 2006.

[5] Daemen J., Knudsen L.R., Rijmen V., "*The block cipher Square*", Fast Software Encryption, Lecture Notes in Computer Science, Springer, Berlin, vol.1267, pp. 149-165, 1997.

[6] Rijmen V., Daemen J., Preneel B., Bosselaers A., De Win E., "*The cipher Shark*", Fast Software Encryption, Lecture Notes in Computer Science, Springer, Berlin, vol.1039, pp. 99–112, 1996.

[7] Aoki K., Ichikawa T., Kanda M., Matsui M., Moriai S., Nakajima J., Tokita T., "*Camellia: a 128-bit block cipher suitable for multiple platforms-design and analysis*", Proceedings of Seventh Annual International Workshop on Selected Areas in Cryptography, SAC'2000, Lecture Notes in Computer Science, vol. 2012, pp. 39-56, Springer, Berlin, 2001.

[8] Aslan B., Sakallı M. T., Buluş E., *Classifying 8-bit to 8-bit S-boxes based on Power Mappings from the point of DDT and LAT Distributions*, International Workshop on the Arithmetic of Finite Fields, WAIFI 2008, Lecture Notes in Computer Science, vol. 5130, pp. 123-133, Springer, Berlin, 2008.

[9] McEliece R. J., *Finite fields for Computer Scientists and Engineers*, Kluwer Academic Publishers, Dordrecht, 1987.

[10] Lidl R., Niederreiter H., *Introduction to finite fields and their applications*, Revised Edition, 1994.

[11] Youssef A. M., Tavares S.E.., "*Affine equivalence in the AES round function*", Discrete Applied Mathematics, Elsevier, (2005).

[12] Sakallı M. T., Aslan B., Buluş E., Şahin A., Büyüksaraçoğlu F., *AES S-Kutusuna Alternatif Cebirsel Olarak Kuvvetlendirilmiş Bir S-Kutusu Önerisi*, Ağ ve Bilgi Güvenliği Ulusal Sempozyumu-ABG'08, Girne-Kuzey Kıbrıs Türk Cumhuriyeti, Mayıs-2008.

[13] Youssef A. M., Gong G., "*On the Interpolation Attacks on Block Ciphers*", 7 th International Workshop on Fast

Software Encryption (FSE 2000), Lecture Notes in Computer Science, vol. 1978, pp. 109-120, 2000.

EK-A: Tablo 1'de Verilen S-kutusunun Cebirsel İfadesi

$$
\begin{aligned}
S(x) = {} & '1c'x^{254} + '1e'x^{253} + '16'x^{252} + '98'x^{251} + '07'x^{250} \\
& + '58'x^{249} + '86'x^{248} + 'e2'x^{247} + 'b5'x^{246} + '11'x^{245} \\
& + '06'x^{244} + '8e'x^{243} + 'ba'x^{242} + '9e'x^{241} + 63x^{240} \\
& + 'a4'x^{239} + '22'x^{238} + '3c'x^{237} + 'e4'x^{236} + '1a'x^{235} \\
& + '9a'x^{234} + '18'x^{233} + 'dd'x^{232} + '99'x^{231} + '8b'x^{230} \\
& + '4c'x^{229} + '98'x^{228} + 'de'x^{227} + '25'x^{226} + 'f8'x^{225} \\
& + '75'x^{224} + 'bb'x^{223} + '81'x^{222} + 'fd'x^{221} + 'd0'x^{220} \\
& + 'c9'x^{219} + '04'x^{218} + '74'x^{217} + 'f6'x^{216} + 'b2'x^{215} \\
& + '39'x^{214} + '49'x^{213} + '0a'x^{212} + 'f9'x^{211} + '49'x^{210} \\
& + '3b'x^{209} + '6c'x^{208} + 'a7'x^{207} + '66'x^{206} + 'e3'x^{205} \\
& + '72'x^{204} + '42'x^{203} + 'b7'x^{202} + '5d'x^{201} + '4f'x^{200} \\
& + '8d'x^{199} + 'db'x^{198} + '38'x^{197} + '9a'x^{196} + '68'x^{195} \\
& + 'e5'x^{194} + '82'x^{193} + '50'x^{192} + '73'x^{191} + 'bd'x^{190} \\
& + '06'x^{189} + 'a7'x^{188} + 'f3'x^{187} + '1d'x^{186} + '28'x^{185} \\
& + '46'x^{184} + '94'x^{183} + '04'x^{182} + 'cf'x^{181} + '8c'x^{180} \\
& + 'c8'x^{179} + '6e'x^{178} + '59'x^{177} + '32'x^{176} + '51'x^{175} \\
& + 'e9'x^{174} + 'a8'x^{173} + '91'x^{172} + 'a5'x^{171} + 'e7'x^{170} \\
& + '63'x^{169} + 'd5'x^{168} + 'a0'x^{167} + '1b'x^{166} + '96'x^{165} \\
& + 'd3'x^{164} + '85'x^{163} + '58'x^{162} + 'af'x^{161} + 'c9'x^{160} \\
& + '88'x^{159} + '5e'x^{158} + '2f'x^{157} + 'a6'x^{156} + '9a'x^{155} \\
& + '27'x^{154} + '84'x^{153} + '59'x^{152} + '91'x^{151} + 'c0'x^{150} \\
& + '83'x^{149} + '2b'x^{148} + '1b'x^{147} + 'bc'x^{146} + '19'x^{145} \\
& + '30'x^{144} + '93'x^{143} + '96'x^{142} + '52'x^{141} + '2e'x^{140} \\
& + '11'x^{139} + '3e'x^{138} + '28'x^{137} + 'e3'x^{136} + 'f4'x^{135} \\
& + '95'x^{134} + '2c'x^{133} + '0f'x^{132} + '26'x^{131} + '99'x^{130} \\
& + 'fb'x^{129} + '63'x^{128} + '7e'x^{127} + '88'x^{126} + '14'x^{125} \\
& + 'a3'x^{124} + 'dd'x^{123} + '94'x^{122} + '20'x^{121} + 'b4'x^{120} \\
& + '70'x^{119} + '7e'x^{118} + 'b1'x^{117} + 'f6'x^{116} + '0d'x^{115} \\
& + '92'x^{114} + '1f'x^{113} + '0b'x^{112} + '62'x^{111} + '0d'x^{110} \\
& + '3e'x^{109} + '16'x^{108} + 'd6'x^{107} + 'f8'x^{106} + 'e7'x^{105} \\
& + '47'x^{104} + '30'x^{103} + '42'x^{102} + 'cb'x^{101} + '26'x^{100} \\
& + '05'x^{99} + '3b'x^{98} + '26'x^{97} + '8c'x^{96} + 'a8'x^{95} + '75'x^{94} \\
& + 'a1'x^{93} + '09'x^{92} + 'd9'x^{91} + '6a'x^{90} + 'd1'x^{89} + '5a'x^{88} \\
& + '45'x^{87} + '29'x^{86} + 'd1'x^{85} + 'c8'x^{84} + '5e'x^{83} + '97'x^{82} \\
& + '28'x^{81} + '79'x^{80} + '59'x^{79} + 'c3'x^{78} + '48'x^{77} + '6f'x^{76} \\
& + 'e8'x^{75} + '79'x^{74} + '3b'x^{73} + 'de'x^{72} + 'a5'x^{71} + 'b5'x^{70} \\
& + 'eb'x^{69} + '9c'x^{68} + 'c3'x^{67} + 'de'x^{66} + '0d'x^{65} + '23'x^{64} \\
& + 'f9'x^{63} + '8a'x^{62} + 'fe'x^{61} + '5d'x^{60} + 'b1'x^{59} + '7c'x^{58} \\
& + '46'x^{57} + '5a'x^{56} + 'f9'x^{55} + '10'x^{54} + 'ee'x^{53} + '55'x^{52} \\
& + '9d'x^{51} + '8f'x^{50} + 'c8'x^{49} + 'e6'x^{48} + '9d'x^{47} + 'c2'x^{46} \\
& + 'fe'x^{45} + '59'x^{44} + '3b'x^{43} + '1f'x^{42} + '1f'x^{41} + 'bc'x^{40} \\
& + '02'x^{39} + '20'x^{38} + 'e6'x^{37} + 'e6'x^{36} + '8b'x^{35} + '7c'x^{34} \\
& + 'b9'x^{33} + '81'x^{32} + '56'x^{31} + '95'x^{30} + '09'x^{29} + '02'x^{28} \\
& + '4d'x^{27} + '6d'x^{26} + '34'x^{25} + '5a'x^{24} + '1d'x^{23} + '02'x^{22} \\
& + '3e'x^{21} + 'fb'x^{20} + '41'x^{19} + '51'x^{18} + 'e6'x^{17} + 'ef'x^{16} \\
& + '5d'x^{15} + 'c7'x^{14} + 'b1'x^{13} + '78'x^{12} + 'bf'x^{11} + 'fc'x^{10} \\
& + 'd2'x^{9} + '51'x^{8} + 'fa'x^{7} + 'bc'x^{6} + 'a5'x^{5} + 'f6'x^{4} \\
& + '15'x^{3} + '87'x^{2} + 'e7'x + 'c3'
\end{aligned}
$$

EK-B: Tablo 1'de Verilen S-kutusunun Tasarımında Kullanılan LA_1 ve LA_2 Doğrusal Dönüşümlerinin İkili Matris Formunda Gösterimi

$$
L_{A1}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 10001111 \\ 11000111 \\ 11100011 \\ 11110001 \\ 11111000 \\ 01111100 \\ 00111110 \\ 00011111 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}
$$

$$
L_{A2}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 10000011 \\ 11000001 \\ 11100000 \\ 01110000 \\ 00111000 \\ 00011100 \\ 00001110 \\ 00000111 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}
$$