AES S-KUTUSUNA ALTERNATİF CEBİRSEL OLARAK KUVVETLENDİRİLMİŞ BİR S-KUTUSU ÖNERİSİ

[1]M.Tolga SAKALLI, [2]Bora ASLAN, [3]Ercan BULUŞ, [1]Andaç Şahin MESUT, [1]Fatma BÜYÜKSARAÇOĞLU

[1]Trakya Üniversitesi, Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği, Edirne
[2]Kırklareli Üniversitesi, Lüleburgaz Meslek Yüksekokulu, Lüleburgaz, Kırklareli
[3]Namık Kemal Üniversitesi, Çorlu Mühendislik Fakültesi, Bilgisayar Mühendisliği, Çorlu-Tekirdağ
tolga@trakya.edu.tr, boraaslan@trakya.edu.tr, ercanbulus@corlu.edu.tr, andacs@trakya.edu.tr, fbuyuksaracoglu@trakya.edu.tr

ABSTRACT

Although there are several design techniques of S-boxes, recently inversion mapping based S-boxes has become so popular because they give good cryptographic properties. Generally, this type of S-box design is finished after adding an affine transformation to the output of these S-boxes to improve algebraic expression of the S-boxes. However, in Camellia, an additional affine transformation is used before the input of the S-box as well. In our study, we show how we can improve algebraic expression of these S-boxes according to the place affine transformation is added and propose algebraically improved an S-box based on inversion mapping over GF(2^8).

Key words: S-boxes, algebraic improvement, an S-box propose

1.GİRİŞ

Boole fonksiyonları ve vektörel boole fonksiyonları (S-kutuları) blok ve akan şifreleme yöntemlerinde kullanılan, doğrusal olmayan ve şifreye güvenliğini veren en önemli elemanlardır. S-kutuları için kriptografik özelliklerden biri olan doğrusal olmama özelliği önemli bir özelliktir. Bununla beraber 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 kriptografik özellikler S-kutularının doyurması gerektiren özellikler olarak karşımıza çıkmaktadır [1].

S-kutularının tasarım tekniklerine örnek olarak pseudo-random üretim, sonlu cisimde ters haritalama, sonlu cisimde üs haritalama ve heuristik teknikler verilebilir. Sonlu cisimde ters alma işlemi, üs haritalama işleminin özel bir durumu olarak görülebilir ve bu iki teknik ile doğrusal olmama ölçüsü yüksek ve diğer kriptografik özellikleri iyi S-kutuları elde edilebilir. Bunun yanında bu tasarım teknikleri kullanılarak tasarlanan S-kutuları, monomial tabanlı polinomlara dayalı üs haritalama ve ters alma gibi cebirsel işlemler tabanlı olduğu için doğrusal denklik [2] ve S-kutularının cebirsel ifadesinde bazı basit cebirsel yaklaşımlar [3] gibi istenmeyen özellikleri de beraberinde getirmektedir. Yine de bu istenmeyen özellikler şifreye bir saldırı olarak hala kullanılamamışlardır. 2001 yılında AES (Advanced Encryption Standard) olarak seçilen doğrusal [4] ve diferansiyel [5] saldırılara dayanıklı olan Rijndael şifresi Nyberg'in [6] önerdiği sonlu cisimde ters haritalama tabanlı 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 ve bu basit cebirsel ifade interpolasyon saldırıları [7] gibi bazı cebirsel saldırılara neden olabilmektedir. Bu problemin üstesinden gelebilmek için S-kutusu tasarımında ters haritalama işleminden sonra bir affine (doğrusal) dönüşüm kullanılmıştır. Bu dönüşüm doğrusal ve diferansiyel saldırılara karşı herhangi bir iyileştirme sağlamamakla beraber $GF(2^8)$'de S-kutusu ifadesini daha karmaşık hale getirmektedir. Bununla beraber $GF(2^8)$ üzerine, $GF(2^8)$ indirgenemez polinom $X^8 + X^4 + X^3 + X + 1$ ile tanımlanmıştır, Lagrange interpolasyonu kullanılarak elde edilen AES S-kutusunun cebirsel ifadesi aşağıdaki gibi verilebilir

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

Yukarıda gösterilen cebirsel ifade cebirsel derece açısından iyi olmakla beraber cebirsel ifadedeki terim sayısı açısından iyi değildir. Lui Jing-mei vb. [8]'deki çalışmalarında AES S-kutusunun cebirsel

çözümü üzerine yeni bir gösterim geliştirmişler ve bu gösterim ile S-kutusunun cebirsel ifadedeki terim sayısının 9'dan 255'e çıkaran bir iyileştirme sunmuşlardır. Çalışmalarında doğrusal matris ve doğrusal sabitten oluşan doğrusal dönüşümü ters alma işleminden sonra kullanmayıp, doğrusal matrisi ters alma işleminden önce kullanıp doğrusal sabiti ters alma işleminden sonra XOR işlemine sokarak S-kutusu tasarımını iyileştirme yoluna gitmişlerdir.

AES şifresine ek olarak literatürde Square [9], Shark [10] gibi şifrelerde kullanılan S-kutuları bir 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 [11] ise ikili bir doğrusal dönüşümü ters haritalama işleminden önce ve sonra kullanmaktadır. Bu da ortaya 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 dönüşümü ters haritalama işleminden hem önce hem de sonra kullanmak (durum 3, örnek Camellia).

Bu çalışmada verilen durumlara göre durum 1'deki cebirsel ifadenin durum 2 ve durum 3 ile iyileştirilebileceğini gösterilmiştir. Buna ek olarak 8-bit girişli ve 8-bit çıkışlı cebirsel açıdan kuvvetlendirilmiş yine AES S-kutusunun tasarımın da kullanılan indirgenemez polinom $X^8 + X^4 + X^3 + X + 1$ tabanlı bir S-kutusu önerisi gerçekleştirilmiştir. Ayrıca ters haritalama tabanlı bir S-kutusu yerine $X \to X^{127}$ üs haritalama tabanlı ve cebirsel açıdan kuvvetlendirilmiş bir S-kutusu örneği de çalışmamızda sunulmuştur.

2.MATEMATİK ALT YAPI

Bu bölümde makale boyunca kullanılacak olan matematiksel alt yapının bir sunumu yapılacaktır. Sonlu cisimler teorisi ile ilgili olarak daha ayrıntılı bilgi [12] ve [13]'den elde edilebilir. Bu makalede gerekli görüldüğünde cisim elemanları hexadecimal notasyonda 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 [13][15].

$$f_i(x) = Tr(g(x)\,\beta_i) \qquad (1)$$

Buna ek olarak (1) ifadesinde β_i dual taban değerleri (2) ifadesinde gösterildiği gibi hesaplanabilir [13][15].

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

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

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

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

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

Böylece giriş bitlerine uygulanacak ters haritalama işleminden sonraki çıkış koordinatları ya da giriş bitlerine uygulanacak doğrusal dönüşüm işleminden sonraki çıkış koordinatları (5) ifadesi ile gösterilebilir.

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

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 ve (9) ifadesinde verilen doğrusal dönüşümü düşünelim. Bu doğrusal dönüşüm ikili bir dönüşümdür ve $p(X)=X^8+X^4+X^3+X+1$ indirgenemez polinomu ile oluşturulan sonlu cisimde 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;

$$\begin{aligned} x_0 &= Tr(\beta^{228}X) \\ x_1 &= Tr(\beta^{204}X) \\ x_2 &= Tr(\beta^{179}X) \\ x_3 &= Tr(\beta^{2}X) \\ x_4 &= Tr(\beta^{73}X) \\ x_5 &= Tr(\beta^{48}X) \\ x_6 &= Tr(\beta^{23}X) \\ x_7 &= Tr(\beta^{253}X) \end{aligned} \quad (6)$$

(6) ifadesindeki gibi elde edilebilir. Doğrusal matris çıkışı koordinatlar $f_0, f_1, ..., f_7$ ise (9) ifadesinde verilen ikili matrisi kullanılarak (7) ifadesindeki gibi elde edilebilir.

$$\begin{aligned} f_0 &= Tr(\beta^{166}X)+1 \\ f_1 &= Tr(\beta^{53}X)+1 \\ f_2 &= Tr(\beta^{36}X) \\ f_3 &= Tr(\beta^{11}X) \\ f_4 &= Tr(\beta^{72}X) \\ f_5 &= Tr(\beta^{76}X)+1 \\ f_6 &= Tr(\beta^{51}X)+1 \\ f_7 &= Tr(\beta^{26}X) \end{aligned} \quad (7)$$

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

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

şeklinde yazılabilir. Bunun yanında

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

şeklinde verilebileceğinden polinom taban değerleri $A(X)$ ifadesinde yerine konursa

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

$A(X)$ ifadesindeki X teriminin katsayısı A_0

$\beta^{166}, \beta^{(53+25) \bmod 255}, \beta^{(50+36) \bmod 255}, \beta^{(75+11) \bmod 255}, \beta^{(100+72) \bmod 255}, \beta^{(125+76) \bmod 255}, \beta^{(150+51) \bmod 255}, \beta^{(175+26) \bmod 255}$ değerlerinin toplamı şeklinde ifade edilebilir. Dolayısıyla

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

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

$$A(X) = \text{"63"} + \text{"05"}\,X + \text{"09"}\,X^2 + \text{"}f9\text{"}\,X^4 + \text{"25"}\,X^8 + \text{"}f4\text{"}\,X^{16} + \text{"01"}\,X^{32} + \text{"}b5\text{"}\,X^{64} + \text{"8}f\text{"}\,X^{128}.$$

Ters haritalama işleminden sonra (9) ifadesindeki doğrusal dönüşüm kullanılarak elde edilen AES S-kutusunun cebirsel ifadesi, $A(X)$ ifadesinde X yerine X^{-1} konarak giriş bölümünde gösterildiği gibi elde edilebilir. [1] ve [14] de verilen tanım ve teoriler ışığı altında durum 2 ve durum 3 cebirsel ifadede 9'dan 255'e artan terim sayısı ile bir iyileştirme yapacaktır. Bunu nedenini [14] de verilen teori ile şöyle açıklayabiliriz: Durum 2 de S kutusunun cebirsel ifadesini $A(X)$ formunda elde edilen doğrusal dönüşümün $S(X) = A(X)^{254}$ şeklinde 254. kuvvetini alarak elde ederiz. Bu alınan kuvvet değeri 7 hamming ağırlığına sahip olduğu için sonuçlanan cebirsel ifadenin terim sayısı

$$T.S = 1 + C\binom{8}{1} + C\binom{8}{2} + \ldots + C\binom{8}{7}$$

şeklinde elde edilebilir. Bunun ötesinde durum 3 için terim sayısı formülasyonu aynı olacaktır çünkü herhangi bir doğrusal dönüşüm çıkışı önceki örnekte gösterildiği gibi $L(X)$ ile ifade edilirse ve ters haritalama işleminden sonra kullanılacak doğrusal dönüşüm AES S-kutusunun kullandığı doğrusal dönüşüm seçilirse durum 3 için sonuçlanan cebirsel ifade

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

şeklinde olacaktır. Buna ek olarak alınan her üs aynı cyclotomic kosette olduğunda sonuçlanan cebirsel ifadedeki terim sayısı 255 olacaktır. Hatta (254, 253, 251, 247, 239, 223, 191, 127) üs fonksiyonları aynı cyclotomic kosette olduğu için bu üs fonksiyonlarının herhangi biri ile tasarlanacak S-kutusu cebirsel ifadesi de 255 terime sahip olacaktır.

3.S-KUTUSU TASARIMI

Bu bölümde durum 3'e göre $X \to X^{127}$ ve $X \to X^{254}$, $X \in GF(2^8)$ olmak üzere 8 bit giriş ve 8 bit çıkışlı cebirsel açıdan geliştirilmiş iki S-kutusunun tasarımı gerçekleştirilecektir. Bu iki S-kutusunun tasarım yapısı aşağıdaki gibi verilebilir:

Adım1.

$$P = L_{A1}(X) = L_{A1(n\times n)}.(X_0, X_1, \ldots, X_{n-1})^T \oplus L_{AS1}.$$

Adım 2.

K = $(P)^{254}$ veya K = $(P)^{127}$.

Adım3.

$$S(X) = L_{A2(n\times n)}.(K_0, K_1, \ldots, K_{n-1})^T \oplus L_{AS2}.$$

Yukarıdaki adımlarda P ve K ara adımlardaki 8-bit değerleri, L_{A1} ve L_{A2} ikili doğrusal dönüşümdeki ikili doğrusal matrisleri $L_{A_{S1}}$ ve $L_{A_{S2}}$ ise doğrusal dönüşümdeki ikili doğrusal sabitleri temsil etmektedir. Çalışmamızda indirgenemez polinom $p(X) = X^8 + X^4 + X^3 + X + 1$ kullanılmıştır. Bu polinom kullanılarak önce $GF(2^8)$ cismi üretilmiştir. Daha sonra doğrusal dönüşüm işlemleri ya da $X \to X^{127}$, $X \to X^{254}$ gibi üs işlemleri adımlarda belirtilen şekilde uygulanarak S-kutuları elde edilmiştir.

$$L_{A1}(X) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,0\,0\,0\,1\,1 \\ 1\,1\,0\,0\,0\,0\,0\,1 \\ 1\,1\,1\,0\,0\,0\,0\,0 \\ 0\,1\,1\,1\,0\,0\,0\,0 \\ 0\,0\,1\,1\,1\ 0\,0\,0 \\ 0\,0\,0\,1\,1\,1\ 0\,0 \\ 0\,0\,0\ 0\,1\,1\,1\ 0 \\ 0\,0\,0\,0\,0\,1\,1\,1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \qquad (8)$$

$$L_{A2}(X) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1\,0\,0\,0\,1\,1\,1\,1 \\ 1\,1\,0\,0\,0\,1\,1\,1 \\ 1\,1\,1\,0\,0\,0\,1\,1 \\ 1\,1\,1\,1\,0\,0\,0\,1 \\ 1\,1\,1\,1\,1\,0\,0\,0 \\ 0\,1\,1\,1\,1\,1\,0\,0 \\ 0\,0\,1\,1\,1\,1\,1\,0 \\ 0\,0\,0\,1\,1\,1\,1\,1 \end{bmatrix} \cdot \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \qquad (9)$$

S-kutusu tasarımında sırasıyla $L_{A1}(X)$ ve $L_{A2}(X)$ şeklinde kullanılan doğrusal dönüşümler (8) ve (9) ifadelerinde verilmiştir. Buna ek olarak tasarlanan S kutuları da Tablo 1 ve Tablo 2 de ikili değerler hexedecimal notasyonda olacak şekilde sunulmuştur. Örnek 2, Tablo 1 de verilen S-kutusunun cebirsel ifadesininin elde edilişini vermektedir.

Örnek 2. 1. doğrusal dönüşüm $L_{A1}(X)$ ve Tablo 1 de AES S-kutusuna alternatif olarak verilen S-kutusunun kabaca cebirsel ifadesinin elde edilişi.

$$L_{A1}(X) = \text{"33"} + \text{"52"}\,X + \text{"77"}\,X^2 + \text{"13"}\,X^4 + \text{"}E0\text{"}\,X^8 + \text{"}FE\text{"}\,X^{16} + \text{"9}E\text{"}\,X^{32} + \text{"96"}\,X^{64} + \text{"27"}\,X^{128}.$$

$$S(x) = \text{"63"} + \text{"05"} L_{A1}(X)^{254} + \text{"09"} L_{A1}(X)^{253} + \text{"}f9\text{"} L_{A1}(X)^{251} +$$
$$\text{"25"} L_{A1}(X)^{247} + \text{"}f4\text{"} L_{A1}(X)^{239} + \text{"01"} L_{A1}(X)^{223} +$$
$$\text{"}b5\text{"} L_{A1}(X)^{191} + \text{"}8f\text{"} L_{A1}(X)^{127}.$$

Tablo 1 de önerilen S-kutusu $X \to X^{254}$ üs haritalama fonksiyonu, 1. doğrusal dönüşüm L_{A1} ve üs haritalama işleminden sonra L_{A2} dönüşümünü kullanarak elde edilirken, Tablo 2 deki S-kutusu $X \to X^{127}$ üs fonksiyonu, 1. doğrusal dönüşümde $L_{A_{S1}}$ sabiti olan hex. "33" yerine hex. "A9" ve 2. doğrusal dönüşüm kullanılarak elde edilmiştir. Ayrıca iki S-kutusunun da AES S-kutusunda olduğu gibi sabit nokta içermemesine özen gösterilmiştir.

Tablo 1. $X \to X^{254}$ Üs Haritalama Fonksiyonu Kullanılarak Elde Edilen S-kutusu Önerisi

	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 2. $X \to X^{127}$ Üs Haritalama Fonksiyonu Kullanılarak Elde Edilen S-kutusu

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

4.SONUÇLAR

Çalışmamızda cebirsel açıdan iyileştirilmiş iki S-kutusu örneği verilmiştir. Bu iyileştirme üs haritalama işleminden önce ve sonra kullanılan doğrusal dönüşümler vasıtasıyla gerçekleştirilmiştir. Örneklerle de bu iyileştirmenin nasıl gerçekleştirildiği gerekli alt yapı verilerek gösterilmiştir. Buna ek olarak herhangi bir üs fonksiyonu için r üs fonksiyonunun hamming ağılığı olmak üzere $GF(2^n) \to GF(2^n)$ şeklindeki üs haritalamalar için cebirsel ifadedeki terim sayısı

$$T.S = 1 + C(n,1) + C(n,2) + ... + C(n,r)$$

şeklinde verilebilir. Örneğin, $X \to X^7$ üs fonksiyonu S-kutusunun tasarımında kullanılsaydı 7 değerinin hamming ağırlığı 3 olduğu için S kutusunun cebirsel ifadesindeki terim sayısı durum 1, durum 2 ve durum 3 için sırasıyla 9, 93, 93 şeklinde olacaktı.

KAYNAKLAR

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

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

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

[4] M. Matsui, "Linear cryptanalysis method for DES Cipher", Adv. Cryptology, Proceedings of Eurocrypt'93, Lecture Notes in Computer Science, Springer, Berlin, 1994.

[5] E. Biham, A. Shamir, "Differential cryptanalysis of DES-like cryptosystems", J.Cryptology, 1991.

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

[7] T. Jakobsen, L. Knudsen, "The interpolation attack on block ciphers", Fast Software Encryption, Lecture Notes in Computer Science, Springer, Berlin, vol. 1267, pp. 28-40, 1997.

[8] L. Jing-mei, W. Bao-dian, C. Xiang-guo, W. Xin-mei, "Cryptanalysis of Rijndael S-box and improvement", Applied Mathematics and Computation, Elsevier, 2005.

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

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

[11] K. Aoki, T. Ichikawa, M. Kanda, M. Matsui, S. Moriai, J. Nakajima, T. Tokita, "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.

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

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

[14] A. M. Youssef, G. Gong, " On the Interpolation Attacks on Block Ciphers", 7 the International Workshop on Fast Software Encryption, pages 109–120, 2000.