GF(2^8) DE TASARLANAN BİR S-KUTUSUNUN CEBİRSEL İFADESİNİN LAGRANGE İNTERPOLASYONU YÖNTEMİYLE ELDE EDİLMESİ

[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@corlu.edu.tr

ÖZET

S-kutuları blok ve akan şifreleme yöntemlerinde kullanılan ve şifreye güvenliğini veren en önemli yapıdır. Son zamanlarda sonlu cisimde ters haritalama ya da üs alma yöntemleri doğrusal ve diferansiyel saldırılara karşı iyi sonuçlar verdikleri için popüler olmuş tasarım yöntemleridir. Bu çalışmada 8-bit giriş ve 8-bit çıkışlı herhangi bir S-kutusunun GF(2^8) de tasarlandığı indirgenemez polinoma göre cebirsel ifadesini hesaplayan Lagrange interpolasyonu uygulaması geliştirilmiştir. Lagrange interpolasyonu yöntemi ile sonlu cisimde tasarlanacak herhangi bir S-kutusunun interpolasyon saldırılarına karşı dayanıklılığı incelenebilecektir. Buna ek olarak Lagrange interpolasyonu yöntemi için 2 ana algoritma geliştirilerek bu algoritmaların karmaşıklık ve performans değerlendirmesi de çalışmamızda sunulmuştur.

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. 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 [1].

Bunun yanında şifreye yapılan saldırılar S-kutularını 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 çıkmıştır.

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

Jakobsen ve Knudsen [3] tarafından sunulmuş olan interpolasyon saldırılarının karmaşıklığı polinomsal ifadedeki terim sayısına ve elde edilen polinomun derecesine bağlıdır. Çalışmamızda herhangi bir 8-bit giriş ve 8-bit çıkışlı bir S-kutusunun GF(2^8) de tasarlandığı indirgenemez polinoma göre cebirsel ifadesini hesaplayan Lagrange interpolasyonu uygulaması geliştirilmiştir. Geliştirilen uygulama ile sonlu cisimde tasarlanan 8-bit giriş 8-bit çıkışlı bir S-kutusunun interpolasyon saldırılarına karşı dayanıklılığı incelenebilecektir. Buna ek olarak performans açısından daha iyi yöntemler geliştirmede referans olacak Lagrange interpolasyonu yönteminin performans değerlendirmesi de çalışmamızda verilmiştir.

2 MATEMATİK ALTYAPI

Bu bölümde makale boyunca kullanılacak olan matematiksel alt yapının bir sunumu yapılacaktır. Sonlu cisimler teorisi ile ilgili olarak daha ayrıntılı bilgi [4] ve [5]'den elde edilebilir. *p* asal sayı, *n* pozitif tamsayı olma şartı ile $m = p^n$ ise *m.* dereceden bir sonlu cisim vardır demektir ve p^n elemanlı bir sonlu cisim Galois cismi olarak tanımlanır, $GF(p^n)$ ya da F_{p^n} şeklinde ifade edilir. $GF(p^n)$, $n>1$ için $GF(p)$ uzayındaki *n*. dereceden indirgenemez polinom kullanılarak elde edilir.

$GF(p)$ uzayında *n.* dereceden bir polinom, (1) ifadesindeki gibi gösterilebilir.

$a_i \in GF(p), a_n \neq 0$ için

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i \quad (1)$$

Teorem 1: Z_m kümesi *m* asal sayı ise cisimdir.

Tanım 1: Z_m bir cisim olmak üzere $Z_m(x) = \left\{ \sum_{i=0}^{n} a_i x^i : a_i \in Z_m, n \geq 0 \right\}$ kümesi, Z_m üzerine bir polinom halka olarak isimlendirilir. $Z_m(x)$ kümesinin bir elemanı Z_m cismi üzerine polinom olarak isimlendirilir. Pozitif dereceli bir polinom $f(x) = \sum_{i=0}^{n} a_i x^i$ için, derece($g(x)$) < derece($f(x)$), derece($h(x)$) < derece($f(x)$) ve $f(x) = g(x)h(x)$ şartlarını sağlayacak şekilde iki polinom varsa $f(x)$ polinomu Z_m üzerine indirgenebilir aksi takdirde indirgenemez polinom olarak tanımlanabilir.

Teorem 2: $f(x)$ fonksiyonu Z_m cisminde derecesi birden büyük bir polinom olsun. $\frac{Z_m(x)}{f(x)}$ polinomu, $f(x)$ polinomu indirgenemez ise cisimdir.

Çalışmamız $p = 2$ olmak üzere $GF(2^n)$ sonlu cisminde tasarlanan yapılar ile ilgili olduğundan α, $GF(2^n)$ sonlu cismini üretmek için kullanılan ilkel eleman olmak üzere ;

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

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

3 LAGRANGE INTERPOLASYONU

Blok şifreleyiciler üzerinde cebirsel bir saldırı türü olan interpolasyon saldırısı Jakobsen ve Knudsen tarafından sunulmuştur [3]. Bu saldırı S-kutusunun cebirsel ifadesindeki terim sayısı ve yine bu ifadenin cebirsel derecesine dayanmaktadır. Dolayısıyla bu ifadedeki yüksek derece ve yüksek sayıdaki terim sayısı saldırıyı zorlaştıracaktır.

Tanım 2: *R* bir cisim olmak üzere $x_1,\ldots,x_n, y_1,\ldots,y_n \in R$ x_i değerlerinin birbirinden farklı olması koşulu ile cisim 2*n* elamana sahip olsun. *R* cisminde en fazla (*n*-1). dereceden olan bir polinom olan $S(x)$ matematiksel olarak (2) deki gibi ifade edilir.

$$S(x) = \sum_{i=1}^{n} y_i \prod_{1 \leq j \leq n, j \neq i} \frac{x - x_j}{x_i - x_j}. \quad (2)$$

Nyberg doğrusal kriptanaliz ve diferansiyel kriptanalize karşı güçlü olan ve ters haritalamayı temel alan aşağıda matematiksel ifadesi bulunan bir S-kutusu sunmuştur [2] :

$$s(x) = x^{-1}, x \in GF(2^n), f(0) = 0. \quad (3)$$

Bu S-kutusunun zayıf tarafı cebirsel yapısının basit olmasıdır. Bu zaaf şifreleyicinin interpolasyon saldırılarına maruz kalmasına neden olabileceği için bu zaafın giderilmesi amacı ile Shark, Square ve AES şifreleme algoritmalarındaki S-kutularında ters haritalamadan sonra doğrusal dönüşüm kullanılmıştır [6]. Diğer yandan Camellia [7] şifreleme algoritmasında kullanılan S-kutusunun tasarımında ters haritalamadan hem önce hem de sonra doğrusal dönüşüm kullanılmıştır.

Örnek 1. Tablo 1'de verilen ve $GF(2^4)$ sonlu cisminde $x \to x^{-1}$ ters haritalama işlemi ile elde edilen bir S-kutusunun cebirsel ifadesinin x^{14} olduğunu Lagrange interpolasyonu ile gösterelim. Örnekte gösterilen ve 1'den f'e kadar olan değerler hexadecimal değerler olup 4-bitlik değerleri temsil etmektedir. Buna ek olarak (2) ifadesinde verilen matematiksel ifadede çıkarma işlemi yerine toplama işlemi kullanılmıştır. Bunun nedeni olarak $GF(2)$ de toplama ve çıkarma işlemlerinin aynı işlemler olduğu söylenebilir.

Tablo1. $GF(2^4)$ sonlu cisminde $x^4 + x + 1$ indirgenemez polinomu kullanılarak ters alma işlemi ile elde edilmiş S-kutusu

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

$$S(x)_0 = 0.\frac{x+1}{0+1}.\frac{x+2}{0+2}.\frac{x+3}{0+3}.\frac{x+4}{0+4}.\frac{x+5}{0+5}.\frac{x+6}{0+6}.\frac{x+7}{0+7}.\frac{x+8}{0+8}.\frac{x+9}{0+9}.\frac{x+a}{0+a}.\frac{x+b}{0+b}.\frac{x+c}{0+c}.\frac{x+d}{0+d}.\frac{x+e}{0+e}.\frac{x+f}{0+f}$$

$$S(x)_1 = 1.\frac{x}{1+0}.\frac{x+2}{1+2}.\frac{x+3}{1+3}.\frac{x+4}{1+4}.\frac{x+5}{1+5}.\frac{x+6}{1+6}.\frac{x+7}{1+7}.\frac{x+8}{1+8}.\frac{x+9}{1+9}.\frac{x+a}{1+a}.\frac{x+b}{1+b}.\frac{x+c}{1+c}.\frac{x+d}{1+d}.\frac{x+e}{1+e}.\frac{x+f}{1+f}$$

$$S(x)_2 = 9.\frac{x}{2+0}.\frac{x+1}{2+2}.\frac{x+3}{2+3}.\frac{x+4}{2+4}.\frac{x+5}{2+5}.\frac{x+6}{2+6}.\frac{x+7}{2+7}.\frac{x+8}{2+8}.\frac{x+9}{2+9}.\frac{x+a}{2+a}.\frac{x+b}{2+b}.\frac{x+c}{2+c}.\frac{x+d}{2+d}.\frac{x+e}{2+e}.\frac{x+f}{2+f}$$

$$S(x)_3 = e.\frac{x}{3+0}.\frac{x+1}{3+1}.\frac{x+2}{3+2}.\frac{x+4}{3+4}.\frac{x+5}{3+5}.\frac{x+6}{3+6}.\frac{x+7}{3+7}.\frac{x+8}{3+8}.\frac{x+9}{3+9}.\frac{x+a}{3+a}.\frac{x+b}{3+b}.\frac{x+c}{3+c}.\frac{x+d}{3+d}.\frac{x+e}{3+e}.\frac{x+f}{3+f}$$

. .....

. .....

. .....

$$S(x)_d = 4.\frac{x}{d+0}.\frac{x+1}{d+1}.\frac{x+2}{d+2}.\frac{x+3}{d+3}.\frac{x+4}{d+4}.\frac{x+5}{d+5}.\frac{x+6}{d+6}.\frac{x+7}{d+7}.\frac{x+8}{d+8}.\frac{x+9}{d+9}.\frac{x+a}{d+a}.\frac{x+b}{d+b}.\frac{x+c}{d+c}.\frac{x+e}{d+e}.\frac{x+f}{d+f}$$

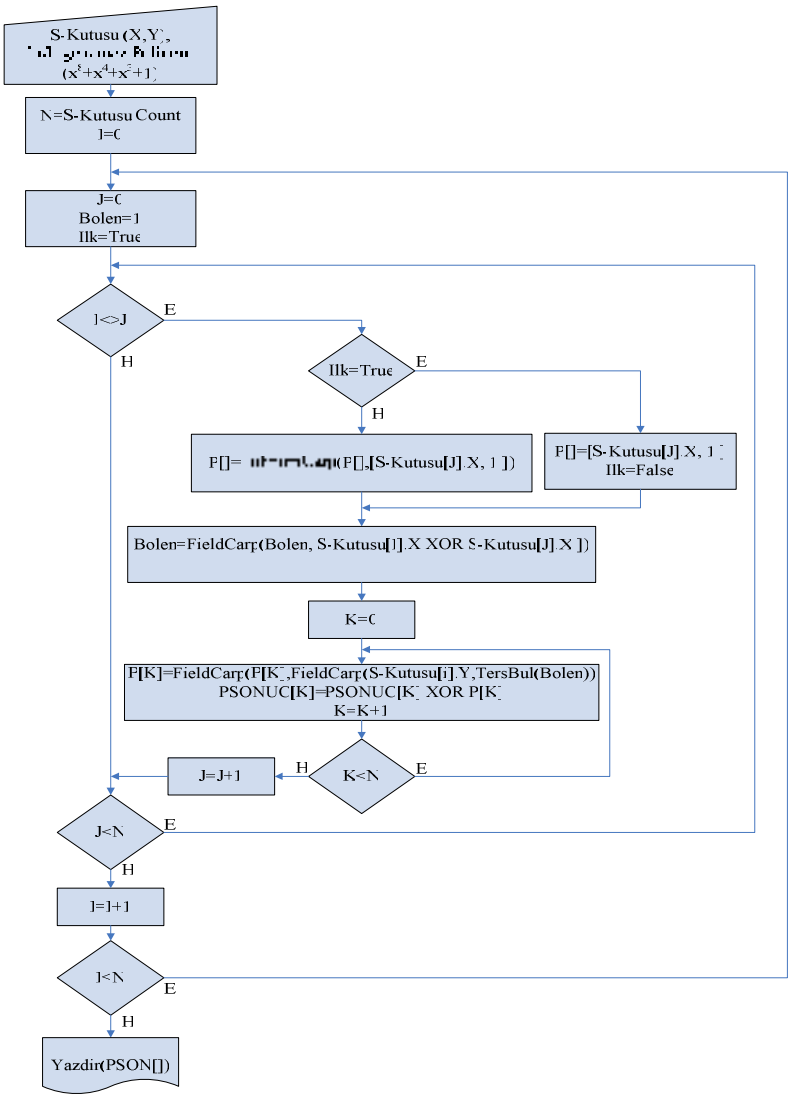
$$S(x)_e = 3.\frac{x}{e+0}.\frac{x+1}{e+1}.\frac{x+2}{e+2}.\frac{x+3}{e+3}.\frac{x+4}{e+4}.\frac{x+5}{e+5}.\frac{x+6}{e+6}.\frac{x+7}{e+7}.\frac{x+8}{e+8}.\frac{x+9}{e+9}.\frac{x+a}{e+a}.\frac{x+b}{e+b}.\frac{x+c}{e+c}.\frac{x+d}{e+d}.\frac{x+f}{e+f}$$

$$S(x)_f = 8.\frac{x}{f+0}.\frac{x+1}{f+1}.\frac{x+2}{f+2}.\frac{x+3}{f+3}.\frac{x+4}{f+4}.\frac{x+5}{f+5}.\frac{x+6}{f+6}.\frac{x+7}{f+7}.\frac{x+8}{f+8}.\frac{x+9}{f+9}.\frac{x+a}{f+a}.\frac{x+b}{f+b}.\frac{x+c}{f+c}.\frac{x+d}{f+d}.\frac{x+e}{f+e}$$

$$S(x) = S(x)_0 + S(x)_1 + S(x)_2 + S(x)_3 + S(x)_4 + S(x)_5 + S(x)_6 + S(x)_7 + S(x)_8 + S(x)_9 + S(x)_a + S(x)_b + S(x)_c + S(x)_d + S(x)_e + S(x)_f$$

$$S(x) = x^{14}$$

Algoritma 1. Lagrange Interpolasyonu Akış Diyagramı



Algoritma 1'de Lagrange interpolasyonunun akış diyagramı görülmektedir. Lagrange interpolasyonu algoritması ile indirgenemez bir polinomla tanımlanan sonlu cisimde $n \times n$ S-kutusunun cebirsel ifadesi bulunur. Lagrange interpolasyonu algoritmasında S-kutusunun (x_i, y_i) giriş çıkış çiftleri için payın cebirsel ifadesi, $(i \neq j)$ için tüm giriş değerlerinin sonlu cisimde $(x + x_i)$ şeklinde yazılması ile elde edilen ifadelerin birbirleriyle polinomsal olarak çarpılmasıyla elde edilir. Lagrange interpolasyonu ile payda değeri, $(i \neq j)$ için $(x_i + x_j)$ ifadelerinin polinom çarpma işlemine tabi tutulmasıyla elde edilir. Yukarıda anlatılan sonlu cisimde polinom çarpma işlemleri sonucunda elde edilen pay paydaya bölündükten sonra y_i değeri ile çarpılır ve aşama değeri elde edilir. Elde edilen değer önceki aşama değeri ile sonlu cisimde toplanır (mod 2 de toplama ya da XOR işlemine tabi tutulur). Sonlu cisimde payın paydaya bölünmesi işlemi sonlu cisimde tersi alınan paydanın pay ile çarpılmasıyla gerçeklenir. Tüm bu işlemler tüm S-kutusu giriş ve çıkış değerleri için tekrarlanır. Sonlu cisim elemanları arasında yapılan çarpma işlemleri sonucunda elde edilen elemanın sonlu cismin elemanı olabilmesi için kullanılan indirgenemez polinom ile indirgeme yapılır.

4 LAGRANGE INTERPOLASYONU ANALİZLERİ

$GF(2^8)$ sonlu cisminde $x^8 + x^4 + x^3 + x + 1$ indirgenemez polinomu kullanılarak tasarlanan AES S-kutusunun cebirsel ifadesi Lagrange interpolasyonu ile [8] ve [9]'daki çalışmalarda verildiği gibi,

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

şeklinde elde edilebilir.

AES S-kutusu, $x \to x^{-1}$ ters haritalamasını takip eden bir doğrusal dönüşümden oluşur. AES S-kutusuna uygulanan Lagrange interpolasyonunda da görüldüğü gibi AES S-kutusu biri sabit değer olmak üzere 9 terimden oluşmaktadır. Terim sayısının az olması AES S-kutusunun cebirsel saldırılara karşı zayıf kalmasına neden olabilir. AES S-kutusundaki oluşabilecek bu zayıflık doğrusal dönüşümün yeri değiştirilerek ya da ek bir doğrusal dönüşümün ters haritalama işleminden önce uygulanması ile giderilebilir. Doğrusal dönüşüm üst haritalamadan önce, sonra veya hem önce hem de sonra olmak üzere üç farklı şekilde uygulanabilir [9] [10]. Bu çalışmada doğrusal dönüşüm üst haritalamadan hem önce hem de sonra kullanılarak tasarlanan bir S-kutusunun Lagrange interpolasyonu ile cebirsel ifadesi elde edilmiştir.

$$L_{A1}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{bmatrix} \quad (4)$$

$$L_{A2}(x) = \begin{bmatrix} f_0 \\ f_1 \\ f_2 \\ f_3 \\ f_4 \\ f_5 \\ f_6 \\ f_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_0 \\ x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \\ x_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} \quad (5)$$

İndirgenemez polinom $x^8 + x^4 + x^3 + x + 1$ tabanlı $GF(2^8)$ cisminde $x \to x^{254}$ ($GF(2^8)$ de $x \to x^{-1}$) üst haritalamasından önce ve sonra sırasıyla (4) (5) ifadelerindeki $L_{A1}(x)$ ve $L_{A2}(x)$ doğrusal dönüşümleri uygulanarak Tablo 2' deki S-kutusu elde edilmiştir [11]. Elde edilen bu S-kutusu $GF(2^8)$ sonlu cismindeki S-kutusu giriş ve çıkış değerleri ile sonlu cisimde toplama ve çarpma işlemleri gerçekleştirilerek Lagrange interpolasyonuna tabi tutulmuştur.

EK-A'da verilen $S(x)$ ifadesinden de görüleceği gibi Tablo 2'de yukarıda anlatıldığı şekilde elde edilen S-kutusunun giriş ve çıkış değerleri için Lagrange interpolasyonu kullanılarak 255 terime sahip cebirsel ifade elde edilmiştir. Lagrange interpolasyonu yöntemi sonlu cisim aritmetiği ile cebirsel olarak tasarlanmış herhangi bir S-kutusuna uygulanabilir.

Tablo 1. $x \to x^{254}$ Üst Haritalama Uygulanarak Elde Edilen 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

5 PERFORMANS ANALİZLERİ

Bu bölümde Lagrange interpolasyonu algoritmasının karmaşıklığı hesaplanmakta, çalışma zamanı ölçülmekte ve algoritma üzerinde iyileştirmeler yapılmaktadır. Bu iyileştirmeler sonunda ortaya çıkan farklı Lagrange interpolasyon algoritmaları için, karmaşıklık ve çalışma zamanı kriterleri bazında kıyaslamalar yapılmıştır.

Kıyaslamalarda kullanılan yöntemlerde Lagrange Normal olarak isimlendirilen Lagrange interpolasyon algoritması 3. bölümde sunulan Lagrange interpolasyonu algoritmasıdır. Lagrange interpolasyonu algoritmasını incelediğimizde payda kısmı 1'den n'e kadar $(x - x_j)$ ifadelerinin $(i \neq j)$ şartı ile çarpımından oluşmaktadır. $GF(2^n)$ deki tüm elamanlar için bu çarpımı yapmak yerine, önce 1'den n'e kadar tüm $(x - x_j)$ ifadelerini çarpıp bir polinom elde edelim. Daha sonra bu polinomu her nokta için $(i = j)$ için $(x - x_j)$ ifadesini bölerek payı hesaplayalım. Böylelikle $(n-1)^2$ çarpma yerine $(n-1)$ çarpma ve $(n-1)$ bölme işlemi yapılarak Lagrange interpolasyonu gerçeklenebilir. Bu yöntemi Lagrange Paydalı olarak isimlendirdik. Lagrange interpolasyonu algoritmasını incelediğimizde paydayı oluşturan $(i + j)$ ifadelerinin $(i \neq j)$ şartı ile sonlu cisimde çarpımlarının sonucunun $GF(2^n)$ de 1 olmasından yola çıkarak payda çarpımlarının hesaplanması ve payın paydaya bölünmesi işlemini Lagrange interpolasyonu algoritmasından çıkarabiliriz. Bu yöntemi ise Lagrange Paydasız olarak isimlendirdik.

Tablo 2. Lagrange Interpolasyon Yöntemleri Çalışma Zamanı Kontrolü

Yöntem	Zaman		
	Dakika	Saniye	Milisaniye
Lagrange Normal	02	55	838
Lagrange Paydalı	00	06	552
Lagrange Paydasız	00	04	56

Tüm bu yöntemler için uygulamalar geliştirilmiş olup, doğru cebirsel ifadeyi oluşturduğu görülmüştür. Bu yöntemlerin çalışma zamanları ölçülerek yapmış olduğumuz kıyaslama Tablo 3'de görülmektedir.

Bu üç farklı yöntemin zaman karmaşıklığı n cinsinde hesaplanmış olup aşağıda verilmiştir:

Lagrange Normal:
$= (2*(n-1)+n)*n = 3n^2 - 2n$ çarpma

Lagrange Paydalı:
$= n + n*(2n-1)$ çarpma $+ n$ bölme
$= 2n^2$ çarpma $+ n$ bölme

Lagrange Paydasız:
$= n + n*n$ çarpma $+ n$ bölme
$= n^2 + n$ çarpma $+ n$ bölme

6 SONUÇLAR

Bu çalışmada üs haritalaması tabanlı 8-bit giriş, 8-bit çıkışlı S-kutularının sonlu cisimde Lagrange interpolasyonu yöntemi ile cebirsel ifadeleri elde edilmiştir.

Klasik Lagrange interpolasyon algoritmasındaki polinom çarpımı sayısında yapılan iyileştirmelerle çalışma zamanında iyileşmeler sağlanmıştır. Lagrange Paydalı olarak isimlendirilen yöntemde, önce n elaman birbiriyle bir defaya mahsus çarpılmış olup $(i = j)$ için $(x - x_j)$ ifadesine bölünmüştür. Yapılan çarpma işlemi sayısı azalmasına rağmen $(n-1)$ bölme işlemi eklenmiştir. Buna rağmen çalışma zamanında Tablo 3'den de görüldüğü büyük bir iyileşme sağlanmıştır. 5. bölümde ifade edildiği gibi $GF(2^n)$ sonlu cisminde Lagrange interpolasyonu algoritmasında paydadaki tüm terimlerin çarpımının sonucunun 1 olacağından paydanın çıkarılması sonucu yaklaşık olarak 2,5 saniyelik bir iyileşme daha sağlanmıştır.

Bu çalışma Lagrange interpolasyonu algoritmasında sonlu cisimde çarpma ve bölme işlemlerini hızlandıracak yöntemler geliştirerek genişletilebilir. Ayrıca üs haritalamalı S-kutularının cebirsel ifadelerini, zaman karmaşıklığı ve çalışma zamanı açısından, daha hızlı şekilde elde edecek farklı yöntemler geliştirilebilir.

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

[3] 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.

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

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

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

[7] 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.

[8] B: Aslan, M. T. Sakallı, E. Buluş, Üs Haritalama Tabanlı Cebirsel 8-bit giriş 8-bit çıkışlı S-kutularının Sınıflandırılması, Ağ ve Bilgi Ulusal Sempozyumu 2, Girne-Kıbrıs, 2008.

[9] B:Aslan, M. T. Sakallı, E. Buluş, 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, Siena-Italy, Springer-Verlag, 2008.

[10] M. T. Sakallı, E. Buluş, A. Şahin, F. Büyüksaraçoğlu, Sonlu Cisim Teorisini Kullanarak Ters Haritalama Tabanlı Bir S-kutusunun Cebirsel ifadesini Elde Etme - Obtaining Algebraic expression of an S-box Based on Inversion Mapping Using Finite Field Theory, IEEE 15. Sinyal İşleme ve İletişim Uygulamaları Kurultayı-SİU 2007, Eskişehir-TÜRKİYE, Haziran-2007.

[11] M. T. Sakallı, E. Buluş, A. Şahin, F. Büyüksaraçoğlu, 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.

EK-A:

Tablo 1 deki S-kutusunun cebirsel ifadesi

$$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} + "3F"x^{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} + "82"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} + "F6x^{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} + "90"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} + "8C"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} + "DF"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} + "E0"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} + "B0"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} + "F5"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".$$