İKİ DÖNGÜLÜ BİR BLOK ŞİFRELEME ALGORİTMASININ LİNEER KRİPTANALİZ UYGULAMASI

M. Tolga SAKALLI[1] Ercan BULUŞ[2] Fatma BÜYÜKSARAÇOĞLU[3]

[1,2,3]Bilgisayar Mühendisliği Bölümü
Mühendislik-Mimarlık Fakültesi
Trakya Üniversitesi, 22100, Edirne
[1]e-posta: tolga@trakya.edu.tr [2] e-posta: ercanb@trakya.edu.tr
[3] e-posta: fbuyuksaracoglu@trakya.edu.tr

Anahtar sözcükler: Lineer Kriptanaliz, SPN (Substitution-Permutation Network), Şifreleme

ABSTRACT

Cryptanalysis is very important for designing strong encryption algorithms. Because they reveal weaknesses of a cryptosystem. From this perspective there have been two successful cryptanalysis methods: Linear cryptanalysis and Differential cryptanalysis. In our study, we present an application of linear cryptanalysis of two round SPN which is a block cipher and we use a 16-bit input as plaintext and a 16-bit output as ciphertext. After accumulating 100 plaintext/ciphertext pairs, we have obtained a 4-bit of 16-bit key using linear cryptanalysis method. We have presented linear cryptanalsis method for this SPN in detail.

1. GİRİŞ

Şifreleme, Sezar'dan başlayarak gelişmekte, verinin her türlü iletiminde verinin gizlenmesi ve güvenli bir şekilde iletilmesi için kullanılmaktadır. Şifreleme işlemini sağlayan şifreleme algoritmaları bir kriptosistemin temel öğesidir. Bir kriptosistem; şifreleme algoritması, anahtar, açık metin ve şifreli metinden oluşmaktadır. Günümüzde kullanılan modern şifreleme algoritmaları üç ana kategoriye ayrılmaktadır. Bunlardan ilki simetrik şifreleme algoritmalarıdır. Blok şifreleme algoritmaları bu kategoriye girer. Bu tür algoritmalarda şifreleme ve deşifreleme işlemeleri aynı anahtarı kullanır. Kullanılan anahtara gizli anahtar denir. İkinci ana kategori asimetrik şifreleme algoritmalarıdır ve şifreleme için gizli anahtarı kullanırken deşifreleme için açık anahtarı, yani herkesin erişebileceği anahtarı, kullanır. Son kategoriye ait şifreleme algoritmaları ise, hash algoritmalarıdır. Bunlar verinin sıkı bir temsilini oluşturmak için kullanılırlar ve kimlik denetiminin sağlanmasında büyük rol oynarlar.

Blok şifreleme algoritmaları günümüzde kriptografide önemli bir yer taşımaktadır. Bu algoritmalara örnek olarak DES (Data Encryption Standard) [7], AES (Advanced Encryption Standard) [8] verilebilir.

Modern şifreleme algoritmalarının gücü söz konusu olduğunda algoritmanın kullandığı anahtarın uzunluğu, algoritmanın döngü sayısı, yapısı, kriptanaliz yöntemlerine karşı dayanıklılığı büyük önem taşımaktadır. Kriptanaliz, açık metni yada anahtarı elde etme bilimidir. Düşmanın saldırı yapılan kriptosistemi bildiği kabul edilir (Kerckhoffs'un prensibi) ve bu koşul altında kriptosistemin en önemli öğesi olan şifreleme algoritması tasarlanır. Düşmanın bir kriptosisteme saldırabilmesi için sahip olması gereken veriler vardır. Bu sahip olduğu verilere göre saldırı modellerinden birini seçebilir. Bu saldırı modellerinden en yaygın olanları şunlardır: *Sadece şifreli metin saldırısı*; Düşman şifreli metin dizisine sahiptir, *Bilinen açık metin saldırısı*; Düşman açık metin dizisine ve bunların şifreli metin dizisine sahiptir, *Seçilmiş açık metin saldırısı*; Düşman bir açık metin dizisini seçebilir ve bunların şifreli metinlerini oluşturabilir, *Seçilmiş şifreli metin saldırısı*; Düşman bir şifreli metin dizisi seçebilir ve bunların açık metinlerini oluşturabilir.

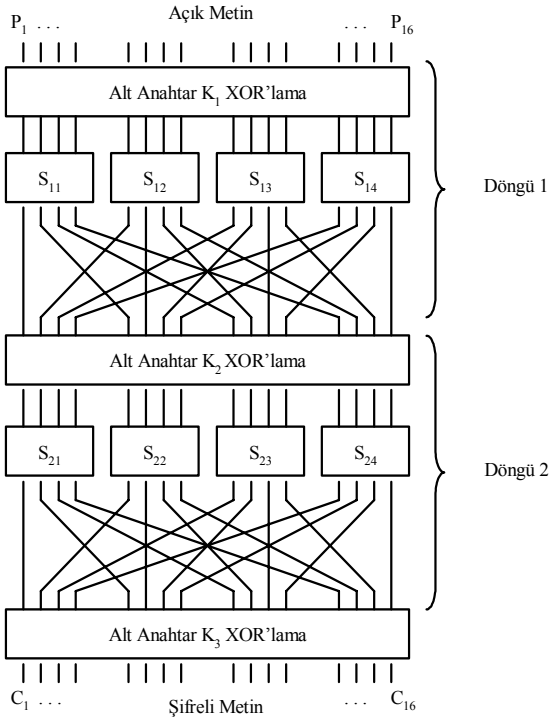
Yukarıda bahsedilen kriptanaliz yöntemlerinin başarılı sayılabilmesi için *brute-force* saldırısı yani tüm olası anahtarların şifrelenmiş mesaj üzerinde denenerek anlamlı bir mesaj etme işleminden daha az maliyete sahip olması gerekmektedir. DES algoritması 56 bit anahtara sahiptir. 2^{56} deşifreleme işlemi algoritmanın kırılmasını sağlayacaktır (olasılığı 1 olarak).

DES, 1974 yılında tasarlandığından beri iki saldırı yöntemi başarıyla gerçekleştirilmiştir. Bunlar lineer kriptanaliz [2] ve diferansiyel kriptanalizdir [3]. Bu saldırılardan lineer kriptanaliz, bilinen açık metin saldırısı için DES'in kırılmasında 2^{43} açık metin/şifreli metin gerekmektedir. Anahtarı elde etmek için 2^{43} şifreleme işlemi yaparak saldırı gerçeklenir. Fakat bu saldırı için 256 terabyte veri biriktirmek gerekmektedir.

Çalışmamızda iki döngülük, 16 bit girişi ve 16 bit çıkışı olan bir SPN (Substitution-Permutation Network – Yerdeğiştirme-Permütasyon Ağı) [1,4] algoritması için lineer kriptanaliz uygulaması gerçekleştirilmiştir ve 16 bit anahtarın 4 biti başarı ile elde edilmiştir.

2. SPN ALGORİTMASI

R döngüden oluşan bir SPN algoritması (R+1) tane N bit anahtar gerektirir. Her döngü üç katmana sahiptir. Anahtar karıştırma safhasında N bit döngü girişi alt anahtar ile XOR işlemine tabi tutulur. Yerdeğiştirme safhasında anahtar safhasının çıkışı n genişliğinde M alt bloğa bölünür (N=M.n) ve her alt blok n × n yani n bit girişe n bit çıkışa sahip bir S kutusuna giriş olur. Lineer transformasyon (permütasyon) safhasında yerdeğiştirme safhasının çıkışı, tersine çevrilebilir N bit lineer transformasyon yolu ile işlenir. Bu aşamada bit pozisyonlarının yerleri değiştirilir. Son döngüde lineer transformasyon işlemi göz ardı edilir. Çalışmamızda son döngüdeki lineer transformasyon işlemi göz ardı edilmemiştir. Kriptanaliz uygulamasında kullanacağımız SPN algoritması *şekil 1*'de gösterilmektedir. *Şekil 3*'te ise bu algoritmada kullanılan S kutusu ve permütasyonun özellikleri görülmektedir.



Şekil-1. SPN Algoritması (N =16, M = n = 4, R = 2)

Çalışmamızda 2 döngülük SPN algoritması için $P_1,P_2,....,P_{16}$ açık metin bitlerini, C_1, $C_2,....,C_{16}$ şifreli metin bitlerini temsil etmektedir. Ayrıca K, anahtarı temsil etmekte ve $K_{1,1}$ anahtar biti için ilk indis döngü numarasını ikincisi ise anahtarın bit pozisyonunu vermektedir. U, S kutusuna giriş bitlerini temsil etmekte ve $U_{1,1}$ giriş biti için ilk indis döngü numarasını ikincisi ise giriş bitinin pozisyonunu vermektedir. V, S kutusuna ait çıkış bitlerini temsil etmekte ve $V_{1,1}$ çıkış biti için ilk indis döngü numarasını ikincisi ise çıkış bitinin pozisyonunu vermektedir. S_{11}, S kutusu için ilk indis döngü numarasını ikinci indis ise o S kutusunun döngüdeki yerini gösterir.

SPN algoritmasının deşifreleme işleminde düzgün olarak deşifreleme yapabilmek için alt anahtarların ters şekilde uygulanması, S kutularında ters haritalamanın kullanılması, alt anahtar bitlerinin permütasyona göre hareket ettirilmesi ve son döngüde biz permütasyon kullandığımız için yerdeğiştirmenin ilk katmanından önce permütasyon kullanılması gerekir.

3. LİNEER KRİPTANALİZ

Lineer kriptanaliz, 1993 yılında Matsui [2] tarafından DES algoritmasına kriptanalitik bir saldırı tipi olarak keşfedilmiştir. Modern şifreleme algoritmalarının tasarımında dikkate alınması gereken önemli bir unsurdur.

Lineer kriptanaliz, yerdeğişirme kutularının (S kutusu) lineer ifadelere dönüştürülmesi ve lineer ifadeleri birleştirerek bilinmeyen anahtar bitlerini elde etme prensibine dayanır. Bu işlem için son döngüde yerine getirilen yerdeğiştirmelerden önceki durum bitleri ile açık metin bitleri arasında lineer bir ilişki bulunması gereklidir. Bu lineer ifade olası tüm anahtar bitleri ile test edilir ve anahtar bitlerinin sapması teorik olarak elde edilen sapma ile karşılaştırılır. En yüksek sapma (1/2 den + yada -) değerine sahip anahtar bizim aradığımız hedef anahtardır. Aradığımız hedef anahtar yanlış ise sapma 0 değerine yakın olacaktır.

a \ *b*	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	8	8	8	8	8	8	8	8	8	8	8	8	8	8	8
1	8	8	6	6	8	8	6	14	10	10	8	8	10	10	8	8
2	8	8	6	6	8	8	6	6	8	8	10	10	8	8	2	10
3	8	8	8	8	8	8	8	8	10	2	6	6	10	10	6	6
4	8	10	8	6	6	4	6	8	8	6	8	10	10	4	10	8
5	8	6	6	8	6	8	12	10	6	8	4	10	8	6	6	8
6	8	10	6	12	10	8	8	10	8	6	10	12	6	8	8	6
7	8	6	8	10	10	4	10	8	6	8	10	8	12	10	8	10
8	8	8	8	8	8	8	8	8	6	10	10	6	10	6	6	2
9	8	8	6	6	8	8	6	6	4	8	6	10	8	12	10	6
A	8	12	6	10	4	8	10	6	10	10	8	8	10	10	8	8
B	8	12	8	4	12	8	12	8	8	8	8	8	8	8	8	8
C	8	6	12	6	6	8	10	8	10	8	10	12	8	10	8	6
D	8	10	10	8	6	12	8	10	4	6	10	8	10	8	8	10
E	8	10	10	8	6	4	8	10	6	8	8	6	4	10	6	8
F	8	6	4	6	6	8	10	8	8	6	12	6	6	8	10	8

Şekil-2. Lineer Yaklaşım Tablosu : N(a,b) değerleri[1]

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

a

Giriş	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
Çıkış	1	5	9	13	2	6	10	14	3	7	11	15	4	8	12	16

b

Şekil-3. a-) S kutusuna 4 bit girişe karşılık 4 bit çıkış
b-) 16 bitin pozisyonlarının değişim permütasyonu

Çalışmamızda S kutusu ve permütasyon özellikleri [1] ve [4]'ten alınmıştır. *Şekil 2* kullandığımız S kutusunun lineer yaklaşımı göstermektedir. S kutusuna girişlerin $X_1,...,X_4$ ve çıkışların $Y_1,...Y_4$ olduğunu varsayalım. *Şekil 2*'deki a ve b 4 bitlik ikili vektörler olmak üzere $X_1 \oplus X_3 \oplus Y_3 = 0$ denkleminin 1/2 değerinden sapmasını hesaplayalım. Denkleme baktığımızda a = (1010) ve b = (0010) olduğunu görürüz çünkü denklem $1.X_1 \oplus 0.X_2 \oplus 1.X_3 \oplus 0.X_4 \oplus 0.Y_1 \oplus 0.Y_2 \oplus 1.Y_3 \oplus 0.Y_4 = 0$ şeklinde açılabilir ve a giriş vektörünü b ise çıkış vektörünü temsil etmektedir. Diğer bir deyişle $a_1.X_1 \oplus a_2.X_2 \oplus a_3.X_3 \oplus a_4.X_4 \oplus b_1.X_1 \oplus b_2.X_2 \oplus b_3.X_3 \oplus b_4.X_4 = 0$ denkleminden $a = (a_1,a_2,a_3,a_4)$ ve $b = (b_1,b_2,b_3,b_4)$ ikili değerlerini çekmiş oluruz. Bu ikili vektörlerin hexadecimal değerleri lineer yaklaşım tablosuna giriş değerleridir. Denklemimiz için N(A,2)=6 bulunur. Bu da denklemin 16 olası değerden 6'sında doğru sonucu verdiğini gösterir. Sapma,

$\varepsilon = (N(a,b)-8)/16$, $\varepsilon = (6-8)/16$, $\varepsilon = -1/8$ bulunur. Eğer N(A,2) değeri 8 olsaydı sapma 0, 8'den büyük olsaydı sapma + olacaktı.

Farklı döngüleri birleştirirken Matsui'nin DES algoritmasında ortaya koyduğu gibi tüm sapma, $\varepsilon=2^{n-1}.\varepsilon_1.\varepsilon_2....\varepsilon_n$ ile hesaplanır. Burada n denklem sayısını göstermektedir ve denklemlere ait sapmalar tüm algoritma için sapmanın değerinin hesaplanmasında kullanılmıştır.

İki döngülü SPN için şifreli metin bitleri ve açık metin bitleri için bir yaklaşım düşünelim ve bu yaklaşım için sapmayı hesaplayalım. İki döngü için S kutularının sapmasını yazarsak;
$S_{12} : X_{1,5} \oplus X_{1,7} \oplus X_{1,8} \oplus Y_{1,6} = 0$ ($\varepsilon_1 = +1/4$ sapma)
$S_{22} : X_{2,6} \oplus Y_{2,6} \oplus Y_{2,8} = 0$ ($\varepsilon_2 = -1/4$ sapma)
N(B,4) = 12 olduğundan $\varepsilon_1 = (12-8)/16 = +1/4$
N(4,5) = 4 olduğundan $\varepsilon_2 = (4-8)/16 = -1/4$ olur.

İlk döngüdeki S kutusu için yaklaşımı tekrar yazalım.
$S_{12} : P_5 \oplus K_{1,5} \oplus P_7 \oplus K_{1,7} \oplus P_8 \oplus K_{1,8} = V_{1,6}$ (1)

(XOR işleminde $Y_{1,6}$ değerini karşı tarafa geçirmek sonucu değiştirmez). (1) yaklaşımı +1/4 sapma ile meydana gelir. $U_{2,6} = V_{1,6} \oplus K_{2,6}$ olduğundan

$S_{22} : U_{2,6} = V_{2,6} \oplus V_{2,8}$ (2)

S_{22} kutusu için (2) yaklaşımı -1/4 sapma ile meydana geldiğinden 1 ve 2 yi birleştirdiğimizde
$P_5 \oplus K_{1,5} \oplus P_7 \oplus K_{1,7} \oplus P_8 \oplus K_{1,8} \oplus K_{2,6} \oplus V_{2,6} \oplus V_{2,8} = 0$ yaklaşımı için

$\varepsilon = 2.\varepsilon_1.\varepsilon_2$, $\varepsilon=2.1/4.-1/4 = -1/8$

olarak bulunur.
Ayrıca $V_{2,6} \oplus K_{3,6} = C_6$, $V_{2,8} \oplus K_{3,14} = C_{14}$ olduğundan $P_5 \oplus K_{1,5} \oplus P_7 \oplus K_{1,7} \oplus P_8 \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} \oplus C_6 \oplus C_{14} = 0$ denklemi için sapmanın -1/8 olduğunu görürüz. Eğer $\Sigma K = K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus K_{3,6} \oplus K_{3,14} = 0$ yada 1 olduğundan yola çıkarak ΣK değerini sabitlersek

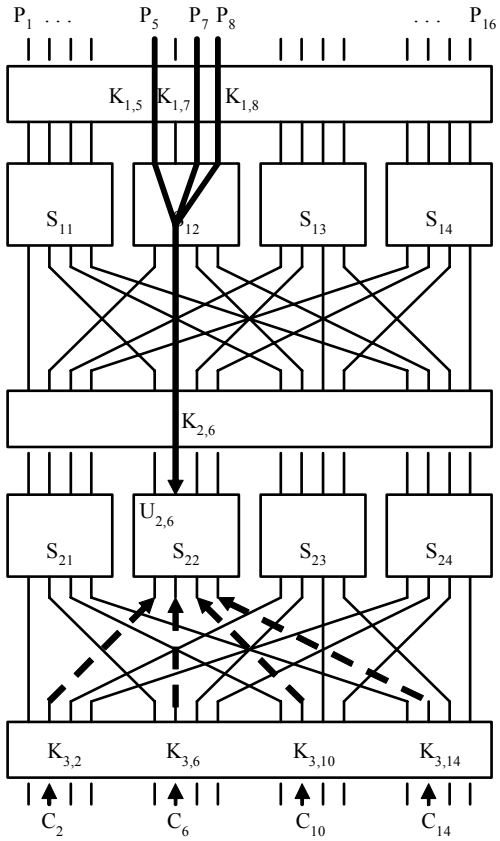
$P_5 \oplus P_7 \oplus P_8 \oplus C_6 \oplus C_{14} = 0$ (3)

(3) denklemi için sapmamız -1/8 ($\Sigma K = 0$) yada +1/8 ($\Sigma K = 1$) olacaktır. Açık metin bitleri ile şifreli metin bitleri arasında lineer bir yaklaşım elde etmiş olduk.

4. İKİ DÖNGÜLÜK SPN ALGORİTMASINA LİNEER KRİPTANALİZ SALDIRISI

Şekil 1'deki SPN algoritmasına lineer kriptanaliz saldırısı yapabilmek için açık metin bitleri ile son döngüde S kutusuna yada kutularına giriş bitleri arasında lineer bir yaklaşım bulmalı ve bu yaklaşımı kullanarak anahtar bitlerine saldırı yapmamız gerekmektedir. İlk olarak *şekil 4*'te görüldüğü gibi P_5,

P_7, P_8 açık metin bitleri ile $S_{1,2}$ kutusuna giriş olan $U_{2,6}$ biti arasında lineer bir yaklaşım bulalım. Daha sonra anahtar bitlerini sabitleyerek $K_{3,2}$, $K_{3,6}$, $K_{3,10}$, $K_{3,14}$ bitlerinin neler olduğunu bulmaya çalışalım.



Şekil-4. Lineer Kriptanaliz Saldırısı

$P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus V_{1,6} = 0$ (+1/4 sapma ile) (4)

$V_{1,6} \oplus K_{2,6} = U_{2,6}$ (5)

(4) ve (5) eşitliğini birleştirirsek
$P_5 \oplus P_7 \oplus P_8 \oplus K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6} \oplus U_{2,6} = 0$ eşitliği +1/4 sapma ile meydana gelir diyebiliriz. Ayrıca anahtar bitlerini $\Sigma K = K_{1,5} \oplus K_{1,7} \oplus K_{1,8} \oplus K_{2,6}$ şeklinde sabitlersek ve bu ifadenin alacağı 0 ve 1 değerine göre
$P_5 \oplus P_7 \oplus P_8 \oplus U_{2,6} = 0$ ifadesinin +1/4 yada -1/4 sapmaya sahip olacağını buluruz.

Bu aşamadan sonra kısmi deşifreleme işlemi yapmamız gerekmektedir. Çünkü lineer kriptanaliz bilinen açık metin saldırısı olduğundan bizim belli sayıda açık metine ve bunların şifreli metinlerine sahip olmamız gerekmektedir. Matsui saldırıda gerekli bilinen açık metinlerinin sayısının ε^{-2} ile orantılı olduğunu göstermiştir. Eğer L gerekli açık metin/ şifreli metin sayısını temsil ederse

$L = c.\varepsilon^{-2}$ (6)

(6) ifadesi bize kullanmamız gereken açık metin/şifreli metin çiftlerinin sayısını verecektir. Burada c küçük bir sabit değeri temsil eder. Çalışmamızda açık metin bitleri ile S kutusuna giriş biti arasında +1/4 sapma bulduğumuza göre ve c sabit değerini 6 seçersek sahip olmamız gereken açık metin/şifreli metin sayısı $L = 6.4^2 = 96$'dır. Biz çalışmamızda 100 adet açık metin/şifreli metin çifti kullandık. Yani öncelikle *şekil 1* algoritması için rasgele 100 açık metin/şifreli metin ürettik. Algoritmadaki anahtar bitlerinin $K_{3,2}$, $K_{3,6}$, $K_{3,10}$, $K_{3,14}$ bulunabilmesi için her açık metin/şifreli metin çiftinin işlenmesi gerekmektedir. Bu işleme bir örnek *tablo 2*'de (*şekil 4*'teki yöntem kullanılmıştır) gösterilmiştir. Anahtar bitlerinin bulunabilmesi için tüm olası anahtar değerler denenerek, çalışmamızda 4 bit anahtar arandığından bu 16 olası değer demek, $P_5 \oplus P_7 \oplus P_8 \oplus U_{2,6} = 0$ ifadesini bir anahtar değeri tuttuğunda sayacı o anahtar değeri için bir attırdık ve bunu tüm açık metin/şifreli metin çiftleri için yaptık. Sonuçta 1/4 değerine en yakın sonucu veren yada 1/2 değerinden en büyük mutlak sapmaya uğrayan anahtar, uygulamada kullanılan $K_{3,2}$, $K_{3,6}$, $K_{3,10}$, $K_{3,14}$ bitlerini bize verecektir. *Tablo 1* bu anahtar değerinin (0,1,1,1) olduğunu göstermektedir. 0,24 sapma değeri en büyük olan ve 1/4'e en yakın olandır. *Tablo 1*'deki sapma, L = 100 olduğu için (7) den hesaplanır. Ancak $\Sigma K = 0$ yada $\Sigma K = 1$ olabileceğinden sapmanın mutlağını düşünerek anahtarı belirlemeliyiz

$\varepsilon = (\text{sayaç}-50)/100$ (7)

.

Hedef Anahtar						
$K_{3,2}$	$K_{3,6}$	$K_{3,10}$	$K_{3,14}$	$P_5 \oplus P_7 \oplus P_8 \oplus U_{2,6} = 0$ Sayısı (sayaç)	Sapma	Mutlak Sapma
0	0	0	0	60	0,10	0,10
0	0	0	1	36	-0,14	0,14
0	0	1	0	49	-0,01	0,01
0	0	1	1	38	-0,12	0,12
0	1	0	0	41	-0,09	0,09
0	1	0	1	63	0,13	0,13
0	1	1	0	39	-0,11	0,11
0	**1**	**1**	**1**	**74**	**0,24**	**0,24**
1	0	0	0	49	-0,01	0,01
1	0	0	1	44	-0,06	0,06
1	0	1	0	45	-0,05	0,05
1	0	1	1	51	0,01	0,01
1	1	0	0	57	0,07	0,07
1	1	0	1	50	0,00	0,00
1	1	1	0	50	0,00	0,00
1	1	1	1	54	0,04	0,04

Tablo 1. Lineer Saldırı için Deneysel Sonuçlar

Açık Metin	Şifreli Metin	Olası Anahtar				P_5 ,P_7 ,P_8 8=1000			Çıkış Bitleri				Çıkış Bitleri ile $K_{3,2}$,$K_{3,6}$,$K_{3,10}$,$K_{3,14}$ Bitlerinin	XOR sonucunun ters S Kutusu				$P_5 \oplus P_7 \oplus P_8 \oplus U_{2,6}$
(Hex.)	(Hex.)	$K_{3,2}$	$K_{3,6}$	$K_{3,10}$	$K_{3,14}$	P_5	P_7	P_8	C_2	C_6	C_{10}	C_{14}	XOR sonucu	$U_{2,5}$	$U_{2,6}$	$U_{2,7}$	$U_{2,8}$	
28DA	E0A0	0	0	0	0	1	0	0	1	0	0	0	1000	0	1	1	1	0
		0	0	0	1	1	0	0	1	0	0	0	1001	1	1	0	1	0
		0	0	1	0	1	0	0	1	0	0	0	1010	1	0	0	1	1
		0	0	1	1	1	0	0	1	0	0	0	1011	0	1	1	0	0
		0	1	0	0	1	0	0	1	0	0	0	1100	1	0	1	1	1
		0	1	0	1	1	0	0	1	0	0	0	1101	0	0	1	0	1
		0	1	1	0	1	0	0	1	0	0	0	1110	0	0	0	0	1
		0	1	1	1	1	0	0	1	0	0	0	1111	0	1	0	1	0
		1	0	0	0	1	0	0	1	0	0	0	0000	1	1	1	0	0
		1	0	0	1	1	0	0	1	0	0	0	0001	0	0	1	1	1
		1	0	1	0	1	0	0	1	0	0	0	0010	0	1	0	0	0
		1	0	1	1	1	0	0	1	0	0	0	0011	1	0	0	0	1
		1	1	0	0	1	0	0	1	0	0	0	0100	0	0	0	1	1
		1	1	0	1	1	0	0	1	0	0	0	0101	1	1	0	0	0
		1	1	1	0	1	0	0	1	0	0	0	0110	1	0	1	0	1
		1	1	1	1	1	0	0	1	0	0	0	0111	1	1	1	1	0

Tablo 2. Örnek bir açık metin/şifreli metin üzerinde yapılan işlemlerin gösterilimi

Tablo 1'deki anahtar değerleri için diğer yüksek sapmalar kısmi deşifrelemeyi etkileyen S kutusu özelliklerinden dolayı meydana gelmiş olabilir.

5. SONUÇ

Çalışmamızda iki döngülük bir SPN algoritması için lineer kriptanaliz uygulaması gerçekleştirdik ve 16 bit anahtarın 4 bitini başarıyla elde ettik. Kullandığımız algoritma iki döngüden oluşmakta idi. Daha fazla döngü sayısına sahip algoritmaların kırılması söz konusu olduğunda lineer yaklaşımda kullanılan S kutularının (aktif S kutuları) sayısının artması lineer yaklaşımdaki sapmanın büyüklüğünün minimum olması demektir. Bu da daha fazla açık metin/şifreli metin çiftine sahip olmamız gerektiği anlamına gelmektedir. Ayrıca daha küçük sapmaya sahip S kutularının tasarımı algoritmayı güçlendirecektir. Çünkü S kutuları algoritmanın lineer olmayan tek yapısıdır ve algoritmaya gücünü veren elemanıdır. Modern şifreleme algoritmalarının tasarımında lineer kriptanaliz önemli bir yer tutmaktadır.

KAYNAKLAR

[1] Stinson D. R., Cryptography: Theory and Practice, Second Ed.,CRC Press, 2002.

[2] Matsui M. Linear Cryptanalysis Method for DES Cipher. Advances in Cryptology– EUROCRYPT'93, 386-397, 1993

[3] Biham E., Shamir A., Differential Cryptanalysis of the full 16-round DES, Advances in Cryptology: Proceedings of CRYPTO'92, Springer-Verlag, Berlin , pp 487-496, 1993.

[4] Heys H., A Tutorial on Linear and Differential Cryptanalysis, CRYPTOLOGIA, Vol 26, No 3 pp 189-221, 2002.

[5] Heys H., Tavares S., Substitution Permutation Networks Resistant to Differential and Linear Cryptanalysis, JOURNAL OF CRYPTOLOGY ,Vol 9, No 1, pp 1-19, 1996

[6] Schneier B., 1996. Applied Cryptography, Second Edition, John Wiley & Sons, Inc., New York, Ny

[7] Keliher L., Linear Cryptanalysis of Substitution- Permutation Networks, Ph.D. Thesis, 2002.

[8] FIPS 46-3, Data Encryption Standard, Federal Information Processing Standard (FIPS), Publication 46-3, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., October 25, 1999.

[9] FIPS 197, Advanced Encryption Standard, Federal Information Processing Standard (FIPS), Publication 197, National Bureau of Standards, U.S. Department of Commerce, Washington D.C., November 26, 2001.