BİR BLOK ŞİFRELEME ALGORİTMASINA KARŞI SQUARE SALDIRISI

M. Tolga SAKALLI[1] Ercan BULUŞ[2] Andaç ŞAHİN[3] Fatma BÜYÜKSARAÇOĞLU[4]

[1,2,3,4]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: andacs@trakya.edu.tr
[4] e-posta: fbuyuksaracoglu@trakya.edu.tr

Anahtar sözcükler: Kriptanaliz, AES, SPN (Substitution-Permutation Network), Square Saldırısı

ABSTRACT

Cryptanalysis is very important for designing strong encryption algorithms. Because they reveal weaknesses of a cryptosystem. When we think of strength evaluation of a block cipher, cryptanalitic attacks make a big contribution to the evaluation of the strength of block ciphers. In our study, we have examined some important attack methods. One of these methods, referred to as square attack, makes a big contribution to calculating AES' number of rounds. This method has been used against a SPN (*Substitution-Permutation Network)* algorithm in which required S boxes and permutation has been chosen from us and we have obtained 16-bit key from the last round of the cipher using Square attack method.

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) [13], AES (Advanced Encryption Standard) [11,12] 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 algoritmasına saldırılır. 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 [1].

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

Çalışmamızda 4 önemli saldırı tekniği olan lineer kriptanaliz, diferansiyel kriptanaliz, imkansız diferansiyel kriptanaliz, kare (square) saldırı teknikleri kısaca incelenmiş ve 4 döngülük, 16 bit girişi ve 16 bit çıkışı olan bir SPN (Substitution-Permutation Network-Yerdeğiştirme-Permütasyon Ağı) [1,2,8,9] algoritmasına karşı square (kare) saldırısı gerçekleştirilmiştir. Son döngüdeki 16 bit anahtarın 16 biti başarı ile elde edilmiştir.

2. TEMEL SALDIRILAR

Blok uzunluğu n bit olan ve k bit anahtar uzunluğuna sahip bir blok şifresi için en temel saldırılardan biri sözlük saldırısıdır. Bu saldırıda k bitlik anahtarı kullanan saldırgan bir açık metni olası 2^k anahtarla şifreler ve şifreli metinleri sıralı bir sözlükte tutar. Daha sonra gizli anahtarla şifrelenmiş seçilmiş bir açık metni elde eder ve uygun bir eşleşmeyi sözlükten kontrol eder. Sözlükte arama ihmal edilebilir fakat saldırı için 2^k tane n-bit bellek word'ü gerekmektedir. Bu yüzden bu saldırı pahalı bir saldırı olarak nitelenebilir.

Diğer bir saldırı türü olan kodkitabı saldırısında saldırgan 2^n mümkün açık metnin gizli bir anahtar ile şifrelenmiş şifreli metinlerini elde eder ve bunları bir tabloya (kodkitabı) depolar. Bir şifreli metin için bekler ve elde ettiği gibi bu şifreli metni tablodakiler ile karşılaştırarak açık metni elde eder. Saldırı 2^n açık metin ve 2^n bellek word'ü gerektirir. Bu saldırı türü de pahalı bir saldırı türüdür.

Geniş anahtar arama saldırısında ise 2^k olası anahtar denenerek şifreli metinden anlamlı bir açık metin elde edilince saldırı tamamlanır. 2^k olası deneme her ne kadar mümkün görünmese de zaman karmaşıklığı veri ve alan karmaşıklığından daha ucuz olarak düşünülmektedir. Eğer bir kriptanaliz saldırısı geniş anahtar aramadan daha az efor ile blok şifreyi kırarsa bu saldırı başarılı bir saldırı olarak görülebilir.

2.1. Lineer Kriptanaliz

1993 yılında Matsui [6] tarafından teorik bir saldırı olarak keşfedilmiştir. Daha sonra DES algoritmasına karşı başarı ile uygulanmıştır. Lineer kriptanaliz, şifreli metin bitleri ile açık metin bitleri arasındaki yüksek olasılıkta lineer ifadelerin meydana gelme avantajını kullanır. Bunun yolu da S kutularından geçer. Saldırganın algoritmayı bildiği (Kerchoffs kuralı) ve belli sayıda açık metin ve şifreli metinlere sahip olduğu varsayılır. S kutularının büyük olması, aktif S kutularının (lineer ifade içinde olan) sayısının artışı ve lineer sapması (1/2 den + veya -) küçük S kutularının tasarımı lineer kriptanalizin uygulanmasını engelleyici faktörlerdir.

2.2. Diferansiyel Kriptanaliz

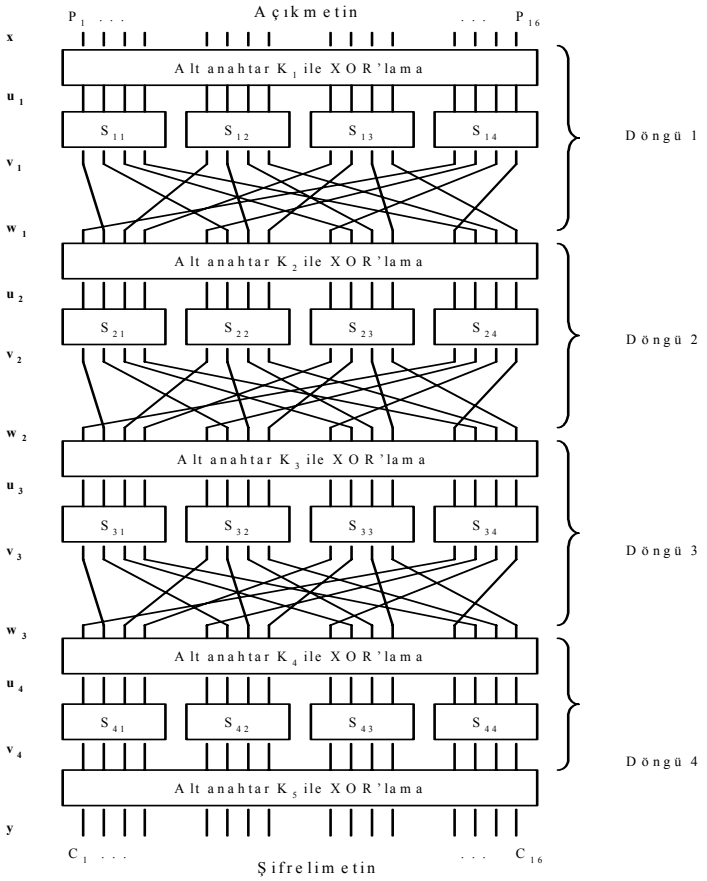
Diferansiyel kriptanaliz [5,7] açıkmetin çiftlerindeki özel farkların sonuçlanan şifrelimetinlerde oluşturduğu farkın etkisini analiz eder. Bu farklar mümkün olan anahtarların olasılıklarını ve en yüksek mümkün anahtarı ortaya koymak için tayin edilir.

2.3. İmkânsız Diferansiyel Kriptanaliz

Kesik diferansiyel kriptanalizin [17] bir çeşididir. Önceden bir diferansiyel öngörülür ve buna göre bazı özel farklar asla meydana gelmeyecektir. Kriptanalizde imkânsız durumların kullanılabileceği gerçeği eski bir fikirdir. *Ortada ıskalama saldırısı (Miss in the middle attacks)* ya da imkânsız diferansiyel saldırısı [18] olarak isimlendirilen bu saldırılar bir blok şifrede imkânsız bir davranışın nasıl belirleneceği ve bunun nasıl anahtarı elde etmek için kullanılacağı ile ilişkili sistematik analizdir.

2.4. Çokluset Saldırıları (Mulltiset Attacks) - Square Saldırısı

Çokluset saldırıları ilk defa J. Daemen, V. Rijmen ve L. Knudsen, Square algoritmasını [3] ortaya koyduklarında öne sürülmüştür. Dolayısıyla diğer ismi Square (Kare) saldırısı olarak bilinir. O zamandan beri diğer birçok algoritmaya uygulanmıştır. (Twofish, IDEA, Camellia, Skipjack gibi) Seçilmiş açıkmetin saldırısıdır ve iyi seçilmiş açıkmetin setleri ile şifrenin ileri doğru incelenmesiyle gerçekleştirilir. Bu saldırı tipinde lineer ve diferansiyel kriptanalizden farklı olarak açıkmetinlerin tüm grubunu düşünerek şifre hakkında bilgi toplarız.



Şekil–1. Saldırıda kullanılacak SPN algoritması

3. 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 dönüşüm (permütasyon) safhasında yerdeğiştirme safhasının çıkışı, tersine çevrilebilir N bit lineer dönüşüm yolu ile işlenir. Bu aşamada bit pozisyonlarının yerleri değiştirilir. Son döngüde lineer dönüşüm işlemi göz ardı edilir. Şekil–1, N = 16, M = n = 4 ve R = 4 için bir SPN algoritmasını göstermektedir. Bu algoritma Square saldırısı için kullanılacaktır. Ayrıca Şekil–1'deki Square saldırısında kullanılacak SPN algoritmasında gösterilen x, u, v, w, y değerleri, ağ üzerinde ilerlerken belli yerlere işaret etmektedir. Bu değerler SPN algoritmasının ve Square saldırısının anlaşılmasını kolaylaştıracaktır. Tablo–1'de ise bu algoritmanın kullandığı S kutusu ve permütasyon özellikleri verilmiştir. S kutusu değerleri DES algoritmasının S kutularından seçilmiştir. (Üçüncü S kutusunun ilk satırıdır.) Permütasyon işlemi, basitçe bitlerin yerlerinin değiştirilmesidir ve bizim tarafımızdan seçilmiştir. Tablo–1'de gösterilen permütasyondaki rakamlar bloktaki bitlerin pozisyonlarını temsil etmektedir. Örnek–2, hexadecimal gösterimde 4 döngülük SPN için adım adım şifreleme işlemini göstermektedir.

Tablo- 1. a) SPN algoritmasında kullanılacak S kutusu gösterilimi
b) SPN algoritmasında kullanılacak permütasyon gösterilimi

a

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

b

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

Örnek–1:

:

Açık metin 1	=	0315
Açık metin 2	=	1315
Açık metin 3	=	2315
Açık metin 4	=	3315
Açık metin 5	=	4315
Açık metin 6	=	5315
Açık metin 7	=	6315
Açık metin 8	=	7315
Açık metin 9	=	8315
Açık metin 10	=	9315
Açık metin 11	=	A315
Açık metin 12	=	B315
Açık metin 13	=	C315
Açık metin 14	=	D315
Açık metin 15	=	E315
Açık metin 16	=	F315
Açık metinlerin XORdeğeri	=	0000

4. BİR SPN ŞİFRESİNE KARŞI SQUARE SALDIRISI

Square saldırısı seçilmiş açıkmetin saldırısıdır [4,16]. Bunun anlamı saldırgan açık metin katarını seçebilir ve bunların şifreli metinlerini oluşturabilir.

SPN algoritmasına Square saldırısı için ilk 4 biti farklı geri kalan 12 biti aynı olan 16 açıkmetin düşünelim ve bu açık metin grubuna delta set ismini verelim. Eğer 16 açıkmetin grubunun XOR değerini hesaplarsak hexadecimal sonucunun 0000 olduğunu görürüz.

Örnek–1, bazı açık metin örneklerini ve bu açık metin örneklerinin XOR sonucunu göstermektedir. Şimdi söyleyebiliriz ki bizim delta setimiz dengelidir. Biz, saldırıyı gerçekleştirebilmek için bu açık metinleri şifreleyerek ağ boyunca ilerlerken delta setimizin nerede bozulduğunu bulmamız gerekmektedir. Delta setimizin denge durumunun bozulduğu yerde saldırıyı gerçekleştirebiliriz.

Örnek–2:

x	=	0534 (açıkmetin)
K_1	=	355F
u_1	=	306B
v_1	=	EAF7
w_1	=	7DF9
K_2	=	4974
u_2	=	348D
v_2	=	E614
w_2	=	4E61
K_3	=	8123
u_3	=	CF42
v_3	=	B869
w_3	=	E15C
K_4	=	9876
u_4	=	792A
v_4	=	5D9C
K_5	=	ABC4
y	=	F658 (şifrelimetin)

Tablo- 2. Hexadecimal notasyonda delta set için şifreleme sonuçları

x Delta Set	w_1 1. Döngü Çıkışı	w_2 2. Döngü Çıkışı	w_3 3. Döngü Çıkışı	v_4 4. Döngü Çıkışı
06B7	6678	F09C	8515	04FE
16B7	623C	433E	6846	8AEA
26B7	2238	C7FE	2F62	7506
36B7	6278	D2BE	3B65	CE0E
46B7	263C	655C	8361	0705
56B7	667C	701C	D110	6DFF
66B7	227C	567E	0E13	DFF3
76B7	2678	F4DC	9426	AB3A
86B7	267C	745C	C123	3D33
96B7	6638	E19C	E575	54AE
A6B7	663C	611C	B170	9DAF
B6B7	223C	477E	6A77	89A0
C6B7	6238	C3BE	3D43	C3E3
D6B7	2278	D6FE	0B46	DEEA
E6B7	2638	E5DC	D664	6209
F6B7	627C	523E	2E20	7F3F
Çıkışların XOR değeri	**0000**	**0000**	**0000**	**5682**

Daha öncede söylediğimiz gibi saldırıyı gerçekleştirebilmek için dengeliliğin algoritmada bozulduğu yeri bulmamız gerekmektedir. Tablo–2, dengeliliğin 4. döngü çıkışı olan v_4'te bozulduğunu göstermektedir. Çünkü 4. döngü çıkışları XOR işlemine tabi tutulduğunda sonucun hexadecimal gösterimde 5682 olduğunu görmekteyiz. Ayrıca w_3, 3. döngünün çıkışı, dengelidir ve çıkışların XOR değeri 0000'dur. Dolayısıyla dengeliliği bozan neden 4. döngüdeki S kutularıdır diyebiliriz.

Böylece bozulan dengeliliği kullanarak şifreye saldırabiliriz. Bu saldırı yöntemini kullanarak son döngüdeki anahtarın ilk 4 bitini, $K_{5,1}$, $K_{5,2}$, $K_{5,3}$, $K_{5,4}$, elde etmeyi düşünelim. Son döngüden elde edilecek bu bitlere hedef kısmi alt anahtar bitleri diyebiliriz. Bu işlem kısmi olarak şifrenin son döngüsünün deşifrelenmesini takip eder. Kısmi alt anahtarın tüm olası değerleri için delta set'in şifreli metinleri (tüm y çıkışları) hedef kısmi alt anahtar bitleri ile XOR'lanır ve takip eden S kutusundan, $S_{4,1}$, geriye doğru gidilir. Sonuçta, u_4 çıkışından tüm alt anahtar değerleri ve delta set için değerler elde ederiz. Biliyoruz ki u_4 çıkışı dengelidir çünkü w_3 çıkışı dengelidir ve w_3'ten u_4'e geçerken gerçekleşen anahtar XOR'lama işlemi dengeliliği bozmaz.

Şekil-1'deki 4 döngülük SPN algoritmasına karşın, kısmi alt anahtar [$K_{5,1}$, $K_{5,2}$, $K_{5,3}$, $K_{5,4}$] değerlerini elde etmek için, Square saldırısı aşağıdaki gibi özetlenebilir:

1- 16 açık metinden oluşan seti, delta seti, seç. Bu set için, P_i, ilk dört bit değişirken diğer açık metin bitleri aynı kalsın.
2- Bu açık metinlere karşı gelen şifreli metinleri, C_i, elde et.
3- İlk dört bit pozisyonu için, aşağıdakileri yap.
   a. $K_{5,1}$, $K_{5,2}$, $K_{5,3}$, $K_{5,4}$ anahtar bitlerinin tüm olası değerler için (0000'dan 1111'e kadar)
      i. $u_4 = \pi_S^{-1}$ o K_5 (C_i) (Mümkün anahtarın ilk dört biti ile 16 şifreli metnin ilk dört bitinin $\oplus$[1] işleminin sonucu) değerini hesapla. Bunun anlamı 16 u_4 çıkışı anlamına gelir.
      ii. 16 u_4 değerinin XOR sonucunu hesapla.
      iii. Eğer XOR = 0 ise 4 bit anahtar değeri doğru alt anahtar değeri olabilir. Değilse, alt anahtar doğru değildir. Dolayısıyla, yanlış anahtar değerlerini kısmi alt anahtar değerlerinden elimine edebiliriz.
   b. Kısmi alt anahtarın [$K_{5,1}$, $K_{5,2}$, $K_{5,3}$, $K_{5,4}$] tüm olası değerlerini deneyerek, bir ya da daha fazla 4 bit alt anahtar değerleri biri doğru olacak şekilde elimizde kalacaktır.
   c. Diğer bir delta seti ya da setlerini doğru anahtar değerini tespit etmek için kullan.

5. DENEYSEL SONUÇLAR

Şifremize saldırıyı 3 delta set kullanarak gerçekleştirdik. Kullandığımız ilk delta set (06B7, 16B7,…., F6B7) ikinci delta set (0315, 1315,…, F315) üçüncü delta set ise (0FA2, 1FA2,…., FFA2)'dir. Üçüncü delta set, üçüncü 4 bitlik anahtar değerini, [$K_{5,9}$…,$K_{5,12}$], kırarken 2 delta set yeterli olmayınca zorunlu olarak kullanılmıştır. Kırılma işlemi açıklanırken ileriki tablolarda hexadecimal değerler kullanılmıştır.

[1] XOR işlemi

Tablo- 3. Üç delta set ve şifrelimetin sonuçları

1. Delta Set		2. Delta Set		3. Delta Set	
x Delta Set	y Şifreli metinler	x Delta Set	y Şifreli metinler	x Delta Set	y Şifreli metinler
06B7	120A	0315	54CD	0FA2	0B15
16B7	15DA	1315	47CF	1FA2	94E6
26B7	18C5	2315	9832	2FA2	5196
36B7	A817	3315	CBF2	3FA2	1476
46B7	59D6	4315	E23A	4FA2	0F75
56B7	E668	5315	E4F1	5FA2	9771
66B7	E9F7	6315	DB35	6FA2	6470
76B7	1B23	7315	6FC4	7FA2	9211
86B7	1D26	8315	41C9	8FA2	5180
96B7	76F8	9315	8F31	9FA2	F271
A6B7	94D8	A315	FFF3	AFA2	F275
B6B7	A92A	B315	24CC	BFA2	1B11
C6B7	922B	C315	A1C8	CFA2	AF10
D6B7	AB06	D315	C1CB	DFA2	C186
E6B7	986C	E315	FE33	EFA2	1B75
F6B7	7967	F315	BB55	FFA2	ABD0

Tablo–3, kullanılan delta setleri ve onların şifreli metin sonuçlarını göstermektedir.

Örnek–3:
Delta set 1'in ilk sütununu kullanarak [$K_{5,1}$, $K_{5,2}$, $K_{5,3}$, $K_{5,4}$] kısmi anahtar parçasının 0000 olduğu durum için u_4'ün XOR değerini bulalım. Tablo–4, bu işlemleri göstermektedir.

Tablo–4, sırasıyla bir olası anahtar için u_4 çıkışlarının XOR sonucunu hexadecimal D olarak göstermektedir. Bu değer bulunurken tüm şifreli metinlerin 1. sütunu 0000 anahtar değeri ile XOR işlemine girmiş, daha sonra bulunan değerler ters S kutusundan geçirilmiş ve u_4 değerlerinin hepsi XOR işlemine sokulmuştur. Diğer tablolarda bulunan değerler bu yöntemle elde edilmiştir.

Tablo- 4. [$K_{5,1}$, $K_{5,2}$, $K_{5,3}$, $K_{5,4}$] kısmi anahtarın olası 0000 anahtar değeri için kısmi deşifreleme

y 1. Delta setin şifreli metinlerinin 1. sütunu	Kısmi alt-anahtar (Hex.) [$K_{5,1}$,...$K_{5,4}$]	v_4 (Hex.)	u_4 (Hex.)
1	0	1	8
1	0	1	8
1	0	1	8
A	0	A	0
5	0	5	7
E	0	E	3
E	0	E	3
1	0	1	8
1	0	1	8
7	0	7	B
9	0	9	2
A	0	A	0
9	0	9	2
A	0	A	0
9	0	9	2
7	0	7	B
u_4 çıkışlarının XOR işlemi sonucu			D

Tablo- 5. [$K_{5,1}$, $K_{5,2}$, $K_{5,3}$, $K_{5,4}$] alt anahtarı için doğru anahtarın bulunması için deneysel sonuçlar

1. Delta set'in şifreli metinlerinin 1. sütunu	2. Delta set'in şifreli metinlerinin 1. sütunu	Kısmi alt-anahtar (Hex.) [$K_{5,1}$, ... , $K_{5,4}$]	1. Delta setin u_4 çıkışlarının XOR işlemi sonucu	2. Delta setin u_4 çıkışlarının XOR işlemi sonucu
1	5	0	D	5
1	4	1	F	8
1	9	2	D	0
A	C	3	8	9
5	E	4	5	6
E	E	5	0	6
E	D	6	2	3
1	6	7	0	7
1	4	8	D	F
7	8	9	1	F
9	F	A	E	A
A	2	B	5	E
9	A	C	8	C
A	C	D	3	1
9	F	E	C	9
7	B	**F**	**0**	**0**

Tablo- 6. [$K_{5,5}$, $K_{5,6}$, $K_{5,7}$, $K_{5,8}$] alt anahtarı için doğru anahtarın bulunması için deneysel sonuçlar

1. Delta set'in şifreli metinlerinin 2. sütunu	2. Delta set'in şifreli metinlerinin 2. sütunu	Kısmi alt-anahtar (Hex.) [$K_{5,5}$, ... , $K_{5,8}$]	1. Delta setin u_4 çıkışlarının XOR işlemi sonucu	2. Delta setin u_4 çıkışlarının XOR işlemi sonucu
2	4	0	C	6
5	7	1	2	0
8	8	2	9	6
8	B	**3**	**0**	**0**
9	2	4	1	7
6	4	5	F	6
9	B	6	4	7
B	F	7	D	6
D	1	8	5	5
6	F	9	6	0
4	F	A	0	5
9	4	B	4	0
2	1	C	8	4
B	1	D	B	6
8	E	E	D	4
9	B	F	9	6

Tablo- 7. [$K_{5,9}$, $K_{5,10}$, $K_{5,11}$, $K_{5,12}$] alt anahtarı için doğru anahtarın bulunması için deneysel sonuçlar

1. Delta set'in şifreli metinlerinin 3. sütunu	2. Delta set'in şifreli metinlerinin 3. sütunu	3. Delta set'in şifreli metinlerinin 3. sütunu	Kısmi alt-anahtar (Hex.) [$K_{5,9}$, ... , $K_{5,12}$]	1. Delta setin u_4 çıkışlarının XOR işlemi sonucu	2. Delta setin u_4 çıkışlarının XOR işlemi sonucu	3. Delta setin u_4 çıkışlarının XOR işlemi sonucu
0	C	1	0	F	E	3
D	C	E	1	9	9	7
C	3	9	2	D	9	7
1	F	7	3	C	9	7
D	3	7	4	4	0	E
6	F	7	5	5	7	7
F	3	7	6	6	0	D
2	C	1	**7**	**0**	**0**	**0**
2	C	8	8	B	3	D
F	3	7	9	3	9	4
D	F	7	A	9	7	A
2	C	1	B	6	A	7
2	C	1	C	0	0	D
0	C	7	D	F	A	9
6	3	7	E	2	3	D
6	5	D	F	A	E	D

Tablo- 8. [$K_{5,13}$, $K_{5,14}$, $K_{5,15}$, $K_{5,116}$] alt anahtarı için doğru anahtarın bulunması için deneysel sonuçlar

1. Delta set'in şifreli metinlerinin 4. sütunu	2. Delta set'in şifreli metinlerinin 4. sütunu	Kısmi alt-anahtar (Hex.) [$K_{5,13}$, ... , $K_{5,16}$]	1. Delta setin u_4 çıkışlarının XOR işlemi sonucu	2. Delta setin u_4 çıkışlarının XOR işlemi sonucu
A	D	0	4	9
A	F	1	B	6
5	2	2	7	9
7	2	3	8	5
6	A	4	8	6
8	1	5	0	3
7	5	6	B	6
3	4	7	3	0
6	9	8	7	9
8	1	9	B	5
8	3	A	4	9
A	C	B	8	6
B	8	C	B	6
6	B	**D**	**0**	**0**
C	3	E	8	6
7	5	F	3	3

Tablo–5, tablo–6, tablo-7 ve tablo-8 son döngüdeki 16 bit K_5 alt anahtarının kırılmasındaki sonuçları göstermektedir. K_5 alt anahtarının ilk 4 biti, ikinci 4 biti ve son 4 biti elde edilirken 2 delta set yeterli olmuştur. Doğru anahtar değeri için delta setlerin u_4 çıkışlarının XOR işlem sonucunun kullanılan tüm delta setler için hexadecimal 0 olması gerekmektedir. Buna göre K_5 anahtarının ilk 4 biti hexadecimal F, ikinci dört biti hexadecimal 3 ve son dört biti hexadecimal D bulunmuştur. Tablo 7'de üçüncü 4 bit anahtar değeri elde edilirken 2 delta set yeterli olmadığından üçüncü delta set kullanılmış ve üçüncü 4 bit alt anahtar değeri hexadecimal 7 bulunmuştur.

6. SONUÇ

Çalışmamızda bir SPN algoritmasını Square saldırısı kullanarak kırdık ve son döngüdeki anahtarı [1111001101111101] olarak elde ettik. Çalışmamızın kriptanaliz ile ilgilenenlere bu saldırının ana fikrinin anlaşılmasında faydalı olacağı kanısındayız. Ayrıca bu çalışma daha önce bu konu ile ilgili çalışmaları pekiştirmekte ve bir SPN algoritmasına bu saldırının uygulanabileceğini göstermektedir.

KAYNAKLAR

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

[2] D. R. Stinson, *Cryptography: Theory and Practice*, Second Edition, CRC Press, 2002.

[3] J. Daemen, L. R. Knudsen, and V. Rijmen, *The Block cipher Square*, Proceedings of Fast Software Encryption, New York: Springer Verlag, pp. 149-165, 1997.

[4] E. Biham, N. Keller, *Cryptanalysis of Reduced Variants of Rijndael*, 2000.

[5] E. Biham and A. Shamir, *Differential Cryptanalysis of DES-like Cryptosystems*, Journal of Cryptology, Vol 4, No 1, pp. 3-72, 1991.

[6] M. Matsui, *Linear Cryptanalysis Method for DES Cipher*, Advances in Cryptology - Eurocrypt '93, Springer-Verlag, pp. 386-397, 1994.

[7] E. Biham, A. Shamir, *Differential Cryptanalysis of the Data Encryption Standard*, Springer-Verlag, 1993.

[8] L. Keliher, *Linear Cryptanalysis of Substitution-Permutation Networks*, PHd Thesis, 2003.

[9] H. M. Heys, S. E. Tavares, *Substitution-Permutation Networks Resistant to Differential and Linear Cryptanalysis*, Journal of Cryptology, Vol 9, No 1, pp. 1-19, 1996.

[10] K. Nyberg, *Differentially Uniform Mappings for Cryptography*, Advances in Cryptology - Eurocrypt' 93, Springer- Verlag, pp 55-64, 1994.

[11] J. Daemen, V. Rijmen, *AES Proposal: Rijndael*, First Advanced Encryption Conference, California, 1998.

[12] 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.

[13] 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.

[14] S. Lucks, *Attacking Seven Rounds of Rijndael under 192-bit and 256-bit keys*, Proceedings of 3rd AES Conference, 2000.

[15] R. C. - W. Phan, *Mini Advanced Encryption Standard (Mini-AES): A Testbed for cryptanalysis students*, Cryptologia, Vol 26, No 4, pp. 283-306, 2002.

[16] R. C. - W. Phan, *Impossible Differential Cryptanalysis of Mini-AES*, Cryptologia, Vol 27, No 4, 2003.

[17] L. R. Knudsen, *Truncated and Higher Order Differentials, Fast Software Encryption*, Springer-Verlag, pp. 196-211, 1995.

[18] E. Biham, A. Biryukov, and A. Shamir, *Cryptanalysis of Skipjack reduced to 31 rounds using Impossible Differentials*, Advances in Cryptology - Eurocrypt'99, Springer-Verlag, pp. 55-64, 1996.