Rasgele Seçilen S-kutularını Temel Alan Blok Şifrelerin Diferansiyel Kriptanalizi

Fatih ÖZKAYNAK, Ahmet Bedri ÖZER, Sırma YAVUZ

Özet—**Diferansiyel kriptanaliz blok şifreleme sistemlerine uygulanan ilk önemli saldırı tekniklerinden biridir. Birçok şifreleme algoritmasının güvenlik analizi yapılırken bu saldırı tekniği göz önüne alınmaktadır. Ancak birçok kriptanalist şifreleme mimarisinin statik yapısından yararlanarak daha küçük versiyonları üzerine yoğunlaşmakta ve şifreleme sistemi hakkında genel bir ifade elde etmeye çalışmaktadır. Bu çalışmada şifreleme sisteminin statik yapısından kaynaklanan problemleri gidermek için şifreleme mimarisinin her bir adımında rasgele seçilen farklı s-kutusu yapılarını kullanan yeni bir algoritma önerilmiştir. Rasgele yapı içerisinde kullanılmak üzere oluşturulan s-kutusu yapıları kriptolojik olarak benzer özellikler göstermektedir. Bir başka deyişle birbirine eşdeğer şifreleme mimarileri oluşturulmuştur. Oluşturulan s-kutusu yapıları içerisinden seçim işleminin yapılması sürecinde ise kaos teorisinden faydalanılmıştır. Bu işlem ile şifreleme sisteminin analizi daha zorlaştırılmıştır. Teorik analizler ve bilgisayar simülasyonları önerilen yeni algoritmanın diferansiyel kriptanalize karşı daha dirençli olduğunu göstermiştir.**

Abstract—**Differential cryptanalysis is one of the first important attack techniques applied to block encryption systems. This attack technique is taken into consideration while performing security analysis of several encryption algorithms. However, several cryptanalyst in this technique concentrates on the smaller versions by making use of static structure of encryption architectures and tries to obtain a general expression about encryption system. In this study; a new algorithm which uses different s-box structures selected randomly at each step of encryption architecture, is proposed to eliminate the problems arising from static structure of encryption system. S-box structures which are formed to be used within random structure cryptographically exhibit similar features. In other words, encryption architectures equivalent to each other were formed. Chaos theory was used during the period of selection process among the formed s-box structures. The analysis of encryption system was made more difficult with this process. Theoretical analysis and computational simulations showed that the proposed, new algorithm is more resistant to differential cryptanalyses..**

Index Terms—**block ciphers differential cryptanalysis, randomly selected s-boxes, chaos.**

I. GİRİŞ

BLOK şifreleme algoritmaları modern kriptolojinin en temel yapı taşlarından biridir [1, 2]. Gürbüz bir blok şifreleme algoritması Shonnon'un [3] güvenli iletişim için vurguladığı iki temel kriter olan karıştırma ve yayılma özelliklerini sağlamalıdır. Bir blok şifreleme algoritmasında karıştırma özelliğini sağlamak için genellikle yer değiştirme kutuları olarak bilinen ve kısaca s-kutusu olarak adlandırılan kriptolojik yapılar kullanılmaktadır. Birçok modern blok şifreleme algoritmasında doğrusal olmayan tek eleman s-kutusu olduğu için genellikle kriptanaliz çalışmaları da bu eleman üzerine odaklanmaktadır [4]. Genel olarak s-kutuları n-bitlik bir giriş değerini m-bitlik bir çıkış değerine dönüştüren doğrusal olmayan bijektif (bire bir ve örten) bir dönüşümdür [5]. S-kutularının tasarımı için literatürde birçok yöntem önerilmiştir [6-9]. Modern blok şifreleme algoritmalarında genellikle güçlü cebirsel ilişkilere dayanan s-kutusu tasarım teknikleri kullanılmaktadır [10]. Bu tip katı cebirsel tekniklere dayalı yöntemler kullanıldığında mimarinin statik yapısından yola çıkılarak bazı istatistiksel ilişkiler ortaya çıkarılabilir ve şifreleme sistemine çeşitli saldırılar gerçekleştirilebilir. Diferansiyel kriptanaliz çalışmaları bunun en temel örneklerinden biridir [4]. Şifreleme mimarisi statik bir yapıda tasarlandığından kriptanalist şifreleme mimarisinin daha küçük versiyonları üzerinde çalışarak mimarinin geneli hakkında bir bilgiye sahip olabilir. Bu çalışmada bu problemi ortadan kaldırmak için rasgele seçilen s-kutularını temel alan yeni bir blok şifreleme algoritması önerilmiştir. Önerilen yeni yöntemin, diferansiyel kriptanaliz için başarı olasılığını azalttığı basit bir blok şifreleme mimarisi üzerinde gösterilmiştir.

Önerilen algoritma iteratif bir blok şifreleme algoritmasının her bir iterasyon adımında farklı bir s-kutusu kullanılması prensibine dayanmaktadır. Bunun için öncelikle s-kutularının tasarım aşamasında en yaygın kullanılan yöntemlerden biri olan Nyberg'in ters haritalama yöntemi incelenmiştir. Bu yöntem kullanılarak tasarlanabilecek farklı s-kutuları gösterilmiştir.

Çalışmadaki önemli katkılardan biri de her bir iterasyon adımında oluşturulan s-kutuları içerisinden seçim işlemine karar verilmesi sürecinde kaos teorisinden yararlanılmış olunmasıdır. Birçok kriptoloji uzmanı arasındaki yaygın görüşlerden biri; blok şifreleme mimarisinde kullanılan elemanlar ne kadar rasgele ise şifreleme mimarisinin o kadar güçlü olacağı yönündedir. Ancak rasgele oluşturulan

Fatih ÖZKAYNAK, Fırat Üniversitesi Yazılım Mühendisliği Bölümü 23119 Elâzığ, Türkiye (telefon: +904242370000/4227, faks: +904242367064; e-mail: ozkaynak@firat.edu.tr).
Ahmet Bedri ÖZER, Fırat Üniversitesi Bilgisayar Mühendisliği Bölümü, 23119 Elazığ, Türkiye (e-mail: bedriozer@firat.edu.tr).
Sırma YAVUZ, Yıldız Teknik Üniversitesi Bilgisayar Mühendisliği Bölümü 34349 İstanbul, Türkiye (sirma@ce.yildiz.edu.tr).

elemanlar belirli bir yapıya oturtulamadığından bu elemanların kriptolojik olarak test edilmesi aşamasında sıkıntılar ortaya çıkmaktadır. Bu problemin çözümü için kaotik sistemler ideal bir yapıya sahiptir. Çünkü kaotik sistemler gerekirci (deterministtik) bir yapıya sahip olmalarına rağmen rasgele benzeri bir davranış göstermektedir. Başlangıç koşulları ve kontrol parametrelerindeki ufak bir değişiklik ile sistem kısa vadede gerekirci bir yapıya sahip iken uzun vadede tahmin edilemez bir yapı kazanmaktadır.

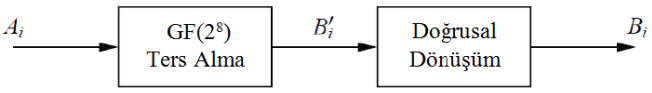
Çalışmanın geri kalan kısmı aşağıdaki gibi organize edilmiştir. İkinci bölümde her bir iterasyon adımında kullanılacak rasgele seçilen s-kutularının nasıl üretileceği gösterilmiştir. Üçüncü bölümde kaos teorisi kısaca tanıtılmış ardından kaotik seçim algoritmasının detayları verilmiştir. Dördüncü bölümde kaotik olarak seçilmiş s-kutularını temel alan basit blok şifreleme mimarisinin diferansiyel kriptanalizi verilmiştir. Elde edilen sonuçlar son bölümde tartışılmıştır.

II. CEBİRSEL TABANLI S-KUTULARI

Gelişkin şifreleme standardı olarak bilinen AES [10] algoritmasının seçim sürecinde en önemli konulardan biri diferansiyel ve lineer kriptanalize karşı dirençli bir yapının araştırılması olmuştur. Bu tasarım sürecinde Galois cisim aritmetiğinden yararlanılarak Nyberg [6] tarafından önerilen yöntem kullanılmıştır. Bu bölümde öncelikle s-kutusu tasarım aşamasında kullanılan Galois aritmetiği hakkında kısa bir bilgi verilmiş ardından Nyberg'in tasarım yöntemi açıklanmıştır. Bölümün sonunda önerilen yeni yapıda kullanılabilecek s-kutularının nasıl üretildiği ve kriptolojik özellikleri verilmiştir.

A. Galois Aritmetiği

Bazen Galois cismi olarak adlandırılan bir sonlu cisim sonlu sayıda eleman içeren bir kümedir. AES'de sonlu cisim 256 eleman içermektedir ve GF(2^8) olarak gösterilmektedir [11]. Burada 2^8=256 polinom vardır.



Şekil. 1. AES S-kutusu oluşturma sürecinde kullanılan matematiksel dönüşümler.

AES s-kutusu şekil 1'de gösterildiği gibi iki adımlı bir matematiksel dönüşüm kullanılarak oluşturulmuştur. İlk aşamada her bir elemanın GF(2^8) cismi üzerinde tersi alınmıştır. Ters alma işleminde indirgenemez polinom olarak $P(x)=x^8+x^4+x^3+x+1$ polinomu kullanılmıştır. Sıfır elemanının tersi olmadığı için kendisine dönüştürülmüştür. İkinci adımda ise hesaplanan değer sabit bir bit matrisi ile çarpıldıktan sonra yine sabit bir 8-bit vektör ile toplanmıştır. Bu işlem denklem (1)'de gösterilmiştir.

B. GF(2^8)'de Oluşturulabilecek Farklı S-kutuları

Barkan ve Biham [12] AES şifreleme sistemine eşdeğer şifreleme sistemleri yazılıp yazılamayacağını araştırmışlardır. Bunun için şifreleme mimarisinde kullanılan bazı yapıların yerine kullanılabilecek alternatifleri göstermişlerdir. Bu yapılar s-kutularının tasarım sürecindeki indirgenemez polinomlar, kolon karıştırma işleminde kullanılan matrisin katsayıları ve doğrusal dönüşümde kullanılabilecek matrislerdir.

$$\begin{pmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} b'_0 \\ b'_1 \\ b'_2 \\ b'_3 \\ b'_4 \\ b'_5 \\ b'_6 \\ b'_7 \end{pmatrix} + \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} \quad (1)$$

Buradan hareketle çalışmada önerilen algoritmanın her bir adımında kullanacağımız s-kutularını oluşturmak için sadece indirgenemez polinomları değiştirerek AES s-kutusuyla aynı mantıkla tasarlanmış kriptolojik olarak eşdeğer olan farklı s-kutuları üretilmiştir. GF(2^8)'de yazabileceğimiz indirgenemez polinomların listesi tablo 1'de verilmiştir.

C. Oluşturulabilecek S-kutularının Kriptolojik Özellikleri

Tablo 1'de verilen indirgenemez polinomları kullanarak oluşturulacak s-kutularının kriptolojik özelliklerini değerlendirmek için literatürde birçok test kriteri önerilmiştir. Bu kriterlerden en yaygın şekilde kullanılanları s-kutularının bijektif (bire-bir ve örten) olması, doğrusal saldırılara karşı güçlü olması için doğrusal olmama ölçütünün yüksek olması, diferansiyel saldırılara karşı dirençli olması için fark dağılım tablosundaki en büyük değerin küçük olması ve çığ kriterini sağlaması olarak özetlenebilir [13].

Oluşturulan tüm s-kutuları bijektif bir yapıya sahiptir ayrıca izomorfik yapıda olduğu için kriptolojik testlerden diferansiyel ve doğrusal olmama ölçütüne ilişkin test sonuçları benzer çıkacaktır. Oluşturulan tüm s-kutularının diferansiyel düzgünlük değeri 4 iken doğrusal olmama değeri ise 112 olarak hesaplanmıştır.

S-kutularının kriptolojik özelliklerinin değerlendirilmesi aşamasında kullanılan diğer önemli bir test ise çığ kriterinin testidir. Çığ testinde giriş bitlerinde bir bitlik bir değişim meydana geldiği zaman bu değişimin çıkış bitlerini nasıl etkilediği ölçülmektedir. İdealde giriş bitlerinde bir bitlik bir değişim meydana geldiğinde çıkış bitlerinin yarısının değişmesi istenmektedir. Tablo 1'de verilen indirgenemez polinomları kullanarak üretilen tüm s-kutuları ideal değer olan 0.5 değerine çok yakın sonuçlar üretmişlerdir. Üretilen s-kutuları içerisinde en iyi sonuç ise $x^8+x^6+x^5+x+1$ polinomunu kullanarak üretilen 8 numaralı s-kutusu olmuştur.

III. KAOTİK SEÇİM ALGORİTMASI

Kaos ekosistemdeki popülasyon artışından elektrik devrelerine, kimyasal reaksiyonlardan mekanik sistemlere kadar bilimin birçok alanında gözlemlenebilen ilginç bir olgudur. Kaos doğrusal olmayan dinamik sistemlerdeki gerekirci ve rasgele benzeri bir süreçtir. Kaotik sistemler periyodik değillerdir ve sonlu olmalarına rağmen belirli bir

değere yakınsamazlar. Kaotik sistemlerin en önemli özelliği başlangıç koşulları ve kontrol parametrelerine aşırı bağımlı olmalarıdır. Kaos doğası gereği rasgele ve tahmin edilemez görülmesine rağmen iç kısmında bir düzen vardır. Aslında genellikle kaos düzen içerisinde düzensizlik yada düzensizlik içerisinde düzen olarak adlandırılabilir. Matematiksel olarak kaos basit gerekirci dinamik bir sistemin rasgeleliği olarak tanımlanabilir [14, 15].

TABLO I
GF(2^8) ÜZERİNDE İNDİRGENEMEZ POLİNOMLAR

Polinom No	İndirgenemez Polinomlar
0	$x^8+x^4+x^3+x+1$
1	$x^8+x^4+x^3+x^2+1$
2	$x^8+x^5+x^3+x+1$
3	$x^8+x^5+x^3+x^2+1$
4	$x^8+x^5+x^4+x^3+1$
5	$x^8+x^5+x^4+x^3+x^2+x+1$
6	$x^8+x^6+x^3+x^2+1$
7	$x^8+x^6+x^4+x^3+x^2+x+1$
8	$x^8+x^6+x^5+x+1$
9	$x^8+x^6+x^5+x^2+1$
10	$x^8+x^6+x^5+x^3+1$
11	$x^8+x^6+x^5+x^4+1$
12	$x^8+x^6+x^5+x^4+x^2+x+1$
13	$x^8+x^6+x^5+x^4+x^3+x+1$
14	$x^8+x^7+x^2+x+1$
15	$x^8+x^7+x^3+x+1$
16	$x^8+x^4+x^3+x^2+1$
17	$x^8+x^7+x^4+x^3+x^2+x+1$
18	$x^8+x^7+x^5+x+1$
19	$x^8+x^7+x^5+x^3+1$
20	$x^8+x^7+x^5+x^4+1$
21	$x^8+x^7+x^5+x^4+x^3+x^2+x+1$
22	$x^8+x^7+x^6+x+1$
23	$x^8+x^7+x^6+x^3+x^2+x+1$
24	$x^8+x^7+x^6+x^4+x^2+x+1$
25	$x^8+x^7+x^6+x^4+x^3+x^2+1$
26	$x^8+x^7+x^6+x^5+x^2+x+1$
27	$x^8+x^7+x^6+x^5+x^4+x+1$
28	$x^8+x^7+x^6+x^5+x^4+x^2+1$
29	$x^8+x^7+x^6+x^5+x^4+x^3+1$

Kaos ve kriptoloji bilimleri arasında doğal bir ilişki bulunmaktadır. Bu ilişki herhangi bir şifreleme sisteminin güvenilir olması için sahip olması gereken özellikler olan karıştırma ve yayılma özellikleri ile kaotik sistemlerin başlangıç koşullarına duyarlı olması ve doğrusal olmaması özellikleriyle örtüşmesinden ortaya çıkmaktadır [16].

Karıştırma ve yayılma özellikleri dinamik sistemlerin sahip olduğu özelliklerdir. Kaotik sistemlerin başlangıç koşulları ve kontrol parametrelerine bağımlılığı bir kaotik sistemden üretilen yörüngeler boyunca yayılma özelliğini sağlar. Başka bir ifade ile herhangi bir yörünge üzerinde alınan her bir değer başlangıç koşulları veya kontrol parametrelerine bağımlıdır. Başlangıç koşulları ve kontrol parametrelerindeki en ufak bir değişiklik ile tamamen farklı yörüngeler oluşacağından bu bağımlılık çok güçlüdür. Sonuç olarak kaotik sistemler başlangıç koşulları ve/veya kontrol parametrelerine bağımlılığı yayılma özelliğine sahiptir [17].

Kaotik sistemlerin ergodiklik özelliği kaotik yörüngenin uzun vadeli davranışının başlangıç koşulları ve kontrol parametrelerine bağımlılığını ortaya koymaktadır. Buradan bir kaotik sistemden üretilen yörüngelerin bir kümesi ile istatistikî olarak başlangıç koşulları ve kontrol parametrelerinin tam değerlerinin çıkarılmasının mümkün olmadığı görülebilir. Sonuç olarak kaotik sistemler karıştırma özelliğini göstermedir [17].

Bu çalışmada kaotik sistem olarak Lojistik harita seçilmiştir. Lojistik haritanın ifadesi denklem (2)'de yörüngesinin davranışı ise şekil 2'de gösterilmiştir [15]. Şifreleme algoritmasında Lojistik haritanın seçilmesindeki en önemli sebeplerden biri kaotik sistemin birinci dereceden bir yapıya sahip olması ve sadece bir başlangıç koşulu, bir kontrol parametresiyle kaotik yörüngenin oluşturulabilmesidir. Bu birçok şifreleme algoritmasının gereksinim duyduğu şifreleme ve şifre çözme sürelerinin azaltılması için önemli bir özelliktir. Ayrıca Lojistik harita düzgün bir dağılıma sahip olması şifreleme mimarisine uygulanacak istatistiksel saldırılara karşı önemli bir etken olacaktır.

$$x_{k+1} = Ax_k(1-x_k), \quad x_0 = 0.2, \quad A = 3.8 \tag{2}$$

A. *Önerilen Algoritma*

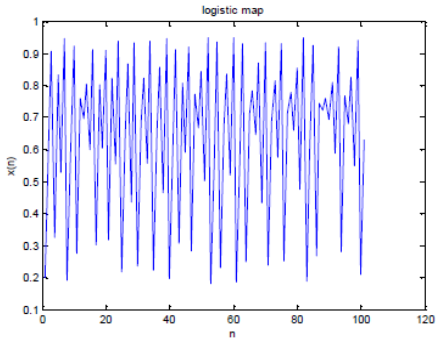
AES şifreleme algoritmasında anahtar uzunluğuna göre iterasyon adım sayısı değişmektedir. Maksimum iterasyon sayısı anahtar uzunluğu 256-bit olduğunda 14 olarak belirlenmiştir. GF(2^8)'de yazılabilecek indirgenemez polinom sayısı tablo 1'de gösterildiği gibi 30 tanedir. Bu indirgenemez polinomlar kullanılarak oluşturulan her bir s-kutusuna 0'dan 29'a kadar numara verilir. Bu durumda her bir iterasyon adımında hangi s-kutusunun seçileceğine karar verilmelidir. Kriptolojik uygulamalarda bu tip bir seçim yapılırken sürecin rasgele olması istenmektedir. Ancak rasgele yapılan bir sürecin kriptolojik özelliklerin değerlendirilmesi aşamasında çeşitli sıkıntılar ortaya çıkmaktadır. Çünkü rasgele bir işlem belirli bir yapıya oturtulamadığından nasıl test edileceği önemli bir soru olarak karşımıza çıkmaktadır. Bu problemi çözmek için seçim sürecinde kaotik sistemlerden yararlanılabilir. Kaos rasgele benzeri bir davranış göstermesine rağmen gerekirci bir yapıya sahiptir. Kaotik sistemin belirlenen başlangıç koşulları ve kontrol parametrelerini kullanarak kaç defa iterasyona sokulacağını şifreleme sisteminin anahtarı belirlemektedir. Dolayısıyla kaotik sistemin kullanılması sisteme ek bir maliyet getirmeyecektir. Kaotik sistem yardımıyla hangi s-kutusunun seçileceğini belirleyen algoritmanın adımları aşağıda adım adım açıklanmıştır. Algoritmanın sözde kodu ise tablo 2'de verilmiştir.

Adım 1) Anahtar planlama algoritmasından gelen 128-bitlik iterasyon adım anahtarı 8-bitlik bloklara bölünür.

Adım 2) Kaotik haritanın kaç sefer iterasyona sokulacağını 8-bit uzunluğunda bloklara bölünen yapı içerisinden seçilen i. blok belirlemektedir. i değeri başlangıçta sıfırdır.

Adım 3) Kaotik haritanın adım 2'de bulunan değer kadar iterasyonu sonucunda hesaplanan çıkış değerinin virgülden sonraki iki basamağına mod 30 işlemi uygulanarak hangi s-kutusunun seçileceğine karar verilir.

Adım 4) Eğer belirlenen s-kutusu daha önce seçilmişse i değeri artırılır ve yeni i. blok için adım 2'den devam edilir. S-kutusu daha önce kullanılmamışsa algoritma sonlandırılır.



Şekil. 2. Lojistik haritanın yörüngesinin davranışı.

IV. Önerilen Kaotik Seçim Algoritmanın Kriptanalizi

Diferansiyel kriptanaliz Biham ve Shamir [4] tarafından blok şifrelerin kriptanalizi için geliştirilen bir seçilmiş açık metin saldırısıdır. Bu saldırı tekniğinde farkları özel olarak seçilmiş açık metinlerin şifreli metinler üzerine etkilerinin incelenmesine bağımlıdır. Diferansiyel kriptanalizde yüksek olasılıklı fark çiftlerinin bulunması amaçlanmaktadır. Bunun için fark dağılım tablosu kullanılmaktadır. XOR tablosu olarak da adlandırılan bu tablo s-kutusunun olası tüm giriş çıkış çiftlerinin her birinin tüm giriş çıkış farklarını göstermektedir.

TABLO 2 KAOS TABANLI S-KUTU SEÇİM ALGORİTMANIN SÖZDE KODU

```
KaotikSkutuSecim(K0||K1||...||K15)
    i, n:=0
    kontrol:=true
    while(kontrol)
      n:= Σ_{j=0}^{i} Decimal(K_j)
      x=KaotikHarita(n) mod 30
      if(x seçilmedi ise) then kontrol:=false
      else i++
    end
end

KaotikHarita(n)
   xEski:=0.2
   for i:=1 to n do
      xYeni:=3.8*xEski*(1-xEski)
      xEski:=xYeni
   end
   xYeni:=0,b1b2b3...bk
   return b1b2
end
```

Önerilen kaotik olarak seçilmiş s-kutularını temel alan blok şifreleme mimarisinin diferansiyel kriptanalizini göstermek için Knudsen ve Robshaw [18] tarafından eğitim amaçlı olarak tanıtılmış basit bir blok şifreleme mimarisi incelenmiştir. Bu blok şifreleme mimarisi 16-bitlik bloklar üzerinde işlem yapan r adımlı iteratif bir blok şifreleme algoritmasıdır. Algoritmanın yapısı tablo 3'de verilmiştir. Blok şifreleme algoritmasında kullanılan s-kutusunun fark dağılım tablosu ise tablo 4'de gösterilmiştir.

Tablo 4'den kolayca görülebileceği gibi giriş çiftleri arasında fark olmadığında çıkış çiftleri arasında da fark olmayacağı 16/16=1 olasılıkla tahmin edilebilir. Tablodan çıkarılabilecek bir diğer önemli ilişkide giriş çiftleri arasında f-bitlik fark olduğunda çıkış çiftleri arasında d-bitlik fark olma olasılığının 10/16 olmasıdır. Bu değer fark dağılım tablosundan çıkarılabilecek maksimum olasılık ilişkisidir. Ancak analiz amacına göre farklı ilişkilerde kullanılabilir. Bu çalışmada giriş çiftleri arasında 2-bitlik fark olduğunda çıkış bitleri arasında 1-bitlik fark olma olasılığının 6/16 ve 2-bitlik fark olma olasılığının 6/16 olması ilişkisi kullanılmıştır.

Yani basit bir örnek üzerinde bu ilişki incelenirse blok şifreleme mimarisine giriş olarak seçilen iki açık metin arasında (0,0,2,0) fark olduğu varsayılmıştır. Yani 16-bitlik giriş 4-bitlik 4 bloğa bölündükten sonra seçilmiş açık metin saldırısına göre 1, 2 ve 4 bloklarda değişim yoktur sadece 3. blokta iki bitlik bir değişim bulunmaktadır. Bu giriş ile 4 iterasyon ilerlendikten sonra 5. adım alt anahtarı olan k_5 $(6/16)^4$ olasılıkla tahmin edilebileceği görülür.

Eğer statik s-kutuları yerine her bir adımda rasgele seçilen s-kutularını kullanan bir yapı kullanılsaydı her bir iterasyon adımda s-kutusu değişeceğinden bu s-kutularına ilişkin fark dağılım tabloları da değişecektir. Bu durumda 5. adım alt anahtarı olan k_5 $(1/16)^4$ olasılıkla hesaplanabilecektir. Sonuç olarak istatistiki ilişki çıkarmak zorlaşacaktır.

İncelenen blok şifreleme mimarisinin kaotik olarak seçilen s-kutularıyla nasıl kullanılacağını göstermek için 4x4 boyutunda s-kutuları $GF(2^4)$ üzerinde tasarlanmıştır. $GF(2^4)$ cismi üzerinde yazabileceğimiz indirgenemez polinomlar denklem (3)'de verilmiştir. Bu indirgenemez polinomları kullanarak AES s-kutusuna benzer mantıkla tasarlanmış s-kutuları tablo 5'de gösterilmiştir. Tablo 5'de verilen s-ilk iki s-kutusu için fark dağılım tabloları ise sırasıyla tablo 6 ve 7'de verilmiştir. Her bir adımda farklı bir s-kutusu kullanıldığında fark dağılım tablolarından istatistiksel ilişki çıkarmanın zorluğu kolayca görülebilir.

$$P_1(x) = x^4 + x + 1$$
$$P_2(x) = x^4 + x^3 + 1 \quad (3)$$
$$P_3(x) = x^4 + x^3 + x^2 + x + 1$$

V. Sonuçlar

Bu çalışmada statik s-kutularını kullanan blok şifreleme mimarisi yerine rasgele seçilen s-kutularını kullanan bir mimari seçildiği zaman diferansiyel kriptananliz başarı olasılığının azaltılabileceği gösterilmiştir.

Blok şifreleme mimarisinin her bir adımında rasgele seçilen s-kutuları $GF(2^8)$ üzerinde yazılabilen indirgenemez

polinomlar kullanılarak AES s-kutusu tasarım mantığına benzer olarak oluşturulmuştur.

Oluşturulan s-kutuları içerisinden seçim işlemi aşamasında ise kaos teorisinden faydalanılmıştır. Kaotik sistemler gerekirci bir yapıya sahip olmasına rağmen rasgele benzeri bir davranış göstermektedir. Kaotik sistemlerin bu özelliği hem sözde rasgele bir seçim yapma imkânı hem de rasgele seçimlerde mümkün olmayan seçimin nasıl yapıldığına dair ifadenin ortaya koyulması probleminin aşılmasını sağlamaktadır. İleride kaotik sistemlerin bu özelliğinden yararlanılarak kriptolojik sistemlerin güçlendirilebileceği düşünülmektedir.

KAYNAKLAR

[1] J. Katz, Y. Lindell, Introduction to modern cryptography: principles and protocols, Chapman & Hall, 2008.
[2] C. Paar, J. Pelzl, Understanding Cryptography A Textbook for Student and Practitioners, Springer, 2010.
[3] CE. Shanon, Communication theory of secrecy systems, Bell Syst Tech J, 28/4 (1949) 656–715.
[4] E. Biham, A. Shamir, Differential Cryptanalysis of DES-like Cryptosystems, Journal of Cryptology 4 (1991) 3-72.
[5] T. Cusick, P. Stanica, Cryptographic Boolean Functions and Applications, Academic Press, 2008.
[6] K. Nyberg, Differentially uniform mappings for cryptography, Proceedings of Eurocrypt'93 Lecture Notes in Computer Science 765 (1994) 55-64.
[7] C. Adams, S. Tavares, The Structured Design of Cryptographically Good S-Boxes, Journal of Cryptography, 3 (1990) 27-41.
[8] K. Nyberg, S-Boxes and Round Functions with Controllable Linearity and Differential Uniformity, Fast Software Encryption, Lecture Notes in Computer Science 1008 (1995) 111-130.
[9] C. Adams, S. Tavares, Good S-Boxes Are Easy To Find, Advances in Cryptography, Lecture Notes in Computer Science 435 (1990) 612-615
[10] J. Daemen, V. Rijmen, AES Proposal: Rijndael, First Advanced Encryption Conference, California, 1998.
[11] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, Revised edition. 1994.
[12] E. Barkan, E. Biham, In How Many Ways Can You Write Rijndael?, Advances in Cryptology - Asiacrypt2002 Lecture Notes in Computer Science 2501 (2002) 160-175.
[13] F. Özkaynak, A. B. Özer, A Method for Designing Strong S-Boxes Based on Chaotic Lorenz System, Physics Letters A, Vol.374, issue.36, 3733-3738, 2010.
[14] O. Edward, Chaos in Dynamical Systems, Cambridge University Press, New York, 2002.
[15] J. Sprott, Elegant Chaos Algebraically Simple Chaotic Flows. World Scientific, 2010.
[16] L. Kocarev, S. Lian, Chaos Based Cryptography Theory Algorithms and Applications, Springer-Verlag, 2011.
[17] F. Özkaynak, A.B. Özer, S. Yavuz, Kaos Tabanlı Yeni Bir Blok Şifreleme Algoritması, IV. Ağ ve Bilgi Güvenliği Sempozyumu, Ankara, 2011.
[18] L. Knudsen, M. Robshaw, The Block Cipher Companion, Springer, 2011.

TABLO 3 KNUDSEN-ROBSHAW [18] BLOK ŞİFRELEME ALGORİTMASI

x	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
S[x]	6	4	C	5	0	7	2	E	1	F	3	D	8	A	9	B

i	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
P[i]	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11	15

1. $u_0=m$
2. for i:=1 to r-1 do
   a) $a_i=u_{i-1} \oplus k_{i-1}$
   b) a_i dört parçaya bölünür. $a_i=A_0||A_1||A_2||A_3$
   c) $S[A_0] || S[A_1] || S[A_2] || S[A_3]$ hesaplanır.
   d) $y_{15},\ldots,y_0= S[A_0] || S[A_1] || S[A_2] || S[A_3]$ şeklinde .
   e) y_i değeri permute edilir.
   f) u_i değeri $y_{15} || y_{11} || \ldots y_4 || y_0$.
3. Son iterasyon adımı
   a) $a_r=u_{r-1} \oplus k_{r-1}$
   b) a_r dört parçaya bölünür. $a_r=A_0||A_1||A_2||A_3$
   c) $S[A_0] || S[A_1] || S[A_2] || S[A_3]$ hesaplanır.
   d) $y_{15},\ldots,y_0= S[A_0] || S[A_1] || S[A_2] || S[A_3]$ şeklinde yazılır .
   e) Çıkış $y \oplus k$

TABLO 4 KNUDSEN-ROBSHAW S-KUTUSU İÇİN FARK DAĞILIM TABLOSU

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	0	6	0	0	0	0	2	0	2	0	0	2	0	4	0
2	0	6	6	0	0	0	0	0	0	2	2	0	0	0	0	0
3	0	0	0	6	0	2	0	0	2	0	0	0	4	0	2	0
4	0	0	0	2	0	2	4	0	0	2	2	2	0	0	2	0
5	0	2	2	0	4	0	0	4	2	0	0	2	0	0	0	0
6	0	0	2	0	4	0	0	2	2	0	2	2	2	0	0	0
7	0	0	0	0	0	4	4	0	2	2	2	2	0	0	0	0
8	0	0	0	0	0	2	0	2	4	0	0	4	0	2	0	2
9	0	0	0	0	0	2	2	2	0	4	2	0	0	0	0	2
A	0	0	0	0	2	2	0	0	0	4	4	0	2	2	0	0
B	0	0	0	2	2	0	2	2	2	0	0	4	0	0	2	0
C	0	4	0	2	0	2	0	0	2	0	0	0	0	0	6	0
D	0	0	0	0	0	0	2	2	0	0	0	0	6	2	0	4
E	0	2	0	4	2	0	0	0	0	0	2	0	0	0	0	6
F	0	0	0	0	2	0	2	0	0	0	0	0	0	10	0	2

TABLO 5 DENKLEM (3)'DE VERİLEN POLİNOMLARI KULLANARAK OLUŞTURULABİLECEK S-KUTULARI

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
SKUTU1	0	1	9	E	D	B	7	6	F	2	C	5	A	4	3	8
SKUTU2	0	1	C	8	6	F	4	E	3	D	B	A	2	9	7	5
SKUTU3	0	1	F	A	8	6	5	9	4	7	3	E	D	C	B	2

TABLO 6 S-KUTUSU 1 İÇİN FARK DAĞILIM TABLOSU

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	2	0	2	0	2	0	2	2	0	0	0	0	4	0
2	0	0	0	0	4	0	2	2	0	2	0	2	2	0	0	2
3	0	2	4	0	0	2	2	2	0	0	2	0	0	0	0	2
4	0	0	2	2	0	0	0	0	2	4	2	0	2	0	0	2
5	0	4	0	0	2	0	0	2	2	0	2	0	2	2	0	0
6	0	0	0	2	0	0	4	2	2	0	0	0	0	2	2	2
7	0	0	0	0	0	2	2	0	4	0	2	2	2	0	2	0
8	0	2	2	2	0	0	2	0	0	0	0	2	4	2	0	0
9	0	0	2	2	2	4	0	2	0	0	0	0	2	0	2	0
A	0	0	2	0	0	2	0	4	2	2	0	2	0	2	0	0
B	0	2	0	4	0	0	0	2	0	2	2	2	0	0	2	0
C	0	2	0	2	2	2	0	0	2	0	0	2	0	0	0	4
D	0	2	0	0	0	2	0	0	0	2	0	0	2	4	2	2
E	0	0	2	0	2	0	0	0	0	0	2	4	0	2	2	2
F	0	0	0	2	2	2	2	0	0	2	4	0	0	2	0	0

TABLO 7 S-KUTUSU 2 İÇİN FARK DAĞILIM TABLOSU

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	2	0	0	2	0	0	0	0	2	2	2	0	2	4	0
2	0	2	2	2	0	2	0	0	4	0	0	2	0	0	2	0
3	0	0	2	0	0	4	2	0	0	2	2	2	2	0	0	0
4	0	0	0	0	0	2	0	2	2	2	0	0	4	2	2	0
5	0	2	2	0	2	0	2	4	2	2	0	0	0	0	0	0
6	0	0	2	0	2	2	0	2	0	0	0	2	0	4	0	2
7	0	2	0	2	2	2	0	0	0	4	0	0	2	0	0	2
8	0	2	2	0	0	0	0	0	2	0	2	0	2	2	0	4
9	0	2	0	0	0	0	4	2	0	0	0	2	2	0	2	2
A	0	0	2	2	2	0	0	2	0	0	4	0	2	0	2	0
B	0	0	0	0	4	2	2	0	2	0	2	0	0	0	2	2
C	0	4	0	2	0	2	2	2	0	0	2	0	0	2	0	0
D	0	0	0	2	0	0	0	2	2	2	2	4	0	0	0	2
E	0	0	4	2	0	0	2	0	0	2	0	0	0	2	2	2
F	0	0	0	4	2	0	2	0	2	0	0	2	2	2	0	0