Makale Türü: Araştırma Makalesi
Makale Gönderilme Tarihi: 27.11.2021
Makale Kabul Tarihi: 06.03.2022

Bazı Alt Uzaylarda Kriptografik Açıdan Eniyilenmiş Büyük S-kutuları
Cryptographically Optimized Large S-boxes in Some Subspaces

Selçuk Kavut
Bilgisayar Mühendisliği Bölümü, Balıkesir Üniversitesi, Balıkesir, Türkiye
skavut@balikesir.edu.tr

Öz

Arama uzayının büyüklüğünden dolayı sezgisel arama algoritmaları, güçlü kriptografik özelliklere sahip S-kutularını elde etmek için literatürde genellikle sekiz ve daha küçük boyutlardaki uzaylarda uygulanmıştır. Bununla birlikte, boyutun artmasıyla doğrusal olmama, farksal birbiçimlilik ve cebirsel bağışıklık özelliklerinin iyileşebileceği bilinmektedir. Çalışmamızda bu durum ele alınarak, bildiğimiz kadarıyla ilk defa on boyutlu uzay için arama gerçekleştirilmiştir. Özel olarak, kriptografik açıdan zengin olan bazı alt uzaylarda rastgele ve sezgisel aramalar yürütülerek, her iki alt uzay için elde edilen en iyi sonuçlar AES S-kutusunun kriptografik özellikleri ile karşılaştırılmıştır. Bunun sonucunda, cebirsel inşa yöntemlerinin yanı sıra, rastgele veya sezgisel arama algoritmaları ile on boyut için bahsedilen alt uzaylarda bulunan S-kutularının doğrusal, farksal ve cebirsel kriptanalize karşı AES S-kutusundan daha dayanıklı olabileceği deneysel olarak gösterilmiştir. Ayrıca, sezgisel arama algoritmasının ters fonksiyondan başlayarak arama yaptığında, ters fonksiyon ile aynı veya çok yakın kriptografik özelliklere sahip S-kutularını üretebildiği gözlenmiştir.
Anahtar Kelimeler: S-kutusu, sezgisel arama, doğrusal olmama, farksal birbiçimlilik, cebirsel bağışıklık

Abstract

Due to the size of the search space, heuristic search algorithms are applied for the spaces in dimensions less than nine to obtain cryptographically strong S-boxes in literature. However, it is known that increasing dimension can improve nonlinearity, differential uniformity and algebraic immunity properties. We here perform a search in dimension ten for the first time to our knowledge. Specifically, implementing random and heuristic searches within some cryptographically rich subspaces, the best obtained results are compared with cryptographic properties of AES S-box. Consequently, beside algebraic constructions, we show that the S-boxes found by random or heuristic searches in the mentioned subspaces for dimension ten can be more resistant than AES S-box against linear, differential and algebraic cryptanalyses. Further, we observe that when heuristic search is started by the inverse function, S-boxes having the same or almost the same properties as those of the inverse function can be generated.
Key Words: S-box, heuristic search, nonlinearity, differential uniformity, algebraic immunity

1. Giriş

S-kutuları (yer değiştirme kutuları) simetrik kriptosistemlerde genellikle doğrusal olmama uygulayan tek bileşenlerdir ve farksal [1], doğrusal [2], cebirsel [3, 4] ve yüksek mertebeden farksal kriptanaliz [5] gibi saldırı yöntemlerinin başarısı S-kutularının kriptografik dayanıklılığına bağlıdır. Bu nedenle kullanılan S-kutusunun kriptografik özellikleri, tüm kriptosistemin güvenliği açısından kritik bir öneme sahiptir. S-kutusu tasarımı simetrik kriptografide karşılaşılan en zor problemlerden birisidir ve literatürde bulunan güçlü kriptografik özelliklere sahip S-kutusu inşaları [6] azdır. $n\times m$ büyüklüğünde bir S-kutusu, n biti m bite gönderen bir fonksiyon olarak tanımlanır. Çalışmamızda, $n\times n$ büyüklüğünde bijektif S-kutuları, diğer bir ifadeyle n boyutlu $\mathrm{GF}(2)^n$ vektör uzayındaki permütasyonlar ele alınmıştır.

Kriptosistemlerde kullanılan S-kutularının sağlaması gereken ve (bir özelliği iyileştirirken başka bir özelliğin kötüleşmesi anlamında) birbiriyle çelişen birçok kriptografik özellik bulunduğundan, bütün kriptografik özellikler bakımından en iyi S-kutusu tasarlamak mümkün değildir [7]. Bu nedenle, kriptografik özellikler arasında dengeleme yapılması kaçınılmazdır. S-kutuları rastgele üretme, cebirsel inşa ve sezgisel/evrimsel arama yöntemleri ile elde edilebilmektedir. Bunlardan rastgele üretme kolay ve hızlı bir yöntem olmasına rağmen, bulunan S-kutularının kriptografik özellikleri çoğunlukla zayıftır. Günümüzde en popüler S-kutusu büyüklüğü olan 8×8 durumu için, rastgele arama yöntemi doğrusal olmama değeri 98'e kadar [8] (bilinen en iyi değer 112) ve farksal birbiçimlilik değeri 10 ile 18 arasında [9] (bilinen en iyi değer 4) S-kutuları üretebilmektedir. Cebirsel inşalar [6] ise genellikle güçlü temel kriptografik özelliklere sahiptir. Örneğin, AES S-kutusunun [10] kullandığı $\mathrm{GF}(2)^8$ uzayında tanımlı ters fonksiyon [11], doğrusal olmama ve farksal birbiçimlilik gibi kriptografik özellikler bakımından literatürde bilinen en iyi değerlere sahiptir. Bununla birlikte, bu tür inşa yöntemleri literatürde fazla bulunmamaktadır ve etkisi henüz günümüzde sınırlı kalmakla beraber, kullanılan cebirsel yapıların cebirsel saldırılar [3, 4] açısından zayıflığa yol açabileceği bilinmektedir. S-kutusu tasarımında yaygın olarak kullanılan (bahsedildiği gibi, AES S-kutusunun da kullandığı) ters fonksiyon, cebirsel bağışıklık açısından en iyi dayanıklılığı sağlamamaktadır. Ayrıca, ters fonksiyonun yan kanal analizi karşısında dayanıklı olmadığı bilinmektedir [7, 12]. Diğer bir yaklaşım olan sezgisel arama yöntemleri, cebirsel yapısı daha karmaşık S-kutuları üretebilmekte, fakat arama uzayının çok büyük olmasından dolayı (bkz. Tablo 1), genellikle $n \leq 8$ için uygulanmaktadır. Doğrusal olmama ve farksal birbiçimlilik

gibi temel kriptografik özellikler açısından ele alırsak, sezgisel arama yöntemleri ile elde edilen sonuçlar, rastgele arama yöntemlerinin ürettiği sonuçları iyileştirmekte; bununla birlikte, boyutun artmasıyla cebirsel inşa yöntemleri ile ulaşılan en iyi sonuçlara ulaşamamaktadır. Özel olarak, 8 boyutlu durum için doğrusal olmama değeri 104'e kadar [9] ve farksal birbiçimliliği 6'ya kadar [13] olan S-kutuları elde edilebilmektedir. Cebirsel inşa yöntemlerinin bahsedilen kriptografik özellikleri daha iyi olabilmektedir; bununla birlikte, sezgisel arama yöntemleri ile yeni S-kutularının tasarımını gerektiren senaryolar mevcuttur. Bunların başında, (örneğin, daha önce belirtilen yan kanal analizine karşı dayanıklılık veya cebirsel bağışıklık gibi) cebirsel inşa yöntemlerinin sağlayamadığı kriptografik özellikleri, ters düşen diğer temel kriptografik özelliklerle birlikte dengelemek veya eniyilemek gerekliliği düşünülebilir. Temel kriptografik özelliklerin en iyi olmasından çok, tüketilen güç, donanım alanı ve gecikme gibi gerçeklenme açısından en iyi performansı veren S-kutusunun tasarımı bir başka senaryo olabilir. Ayrıca, kriptografik özellikleri bakımından cebirsel inşa yöntemlerine yakın özelliklere sahip (örneğin, belirli bir şirket veya kuruma ait olan) S-kutularının tasarlanması amacıyla sezgisel arama yöntemleri kullanılabilir.

S-kutusu tasarımı sezgisel arama algoritmaları için özellikle boyut arttıkça zorlaşan bir problemdir. Yakın zamanda, Jacobovic vd. [14, 15] tarafından Boole fonksiyonları ve S-kutuları tasarımının neden zor bir problem olduğunu anlamak için maliyet ortamı analizi yapılmıştır. Özel olarak, S-kutuları için gerçekleştirilen çalışmada [14] seçilen maliyet fonksiyonları ve komşuluk türleri için, neredeyse her başlangıç noktasının farklı bir yerel en iyiye gittiği gözlenmiş ve maliyet ortamında verimli bir şekilde gezinmenin zorluğu deneysel olarak gösterilmiştir. S-kutusu tasarımında sezgisel algoritma kullanan ilk çalışma, Milan [8] tarafından yapılan tepe tırmanma yöntemi ile rastgele üretilen 8×8 büyüklüğündeki S-kutularının doğrusal olmama değerlerinin iyileştirilmesidir. Sonrasında Milan vd. [16] genetik algoritma ile birlikte tepe tırmanma yöntemi kullanarak doğrusal olmama ve mutlak gösterge değerlerini iyileştirmişlerdir. Bu iki çalışmada, doğrusal olmama ve mutlak gösterge değerleri doğrudan maliyet fonksiyonu olarak kullanılmıştır. Clark vd. [17], Walsh-Hadamard spektrumundaki tüm değerleri eniyileyen bir maliyet fonksiyonu kullanarak, tepe tırmanmayla takip edilen tavlama benzetimi algoritması ile [16] çalışmasındaki sonuçları iyileştirmişlerdir. Tesař [18], tüm ağaç arama tekniği ile birleştirdiği genetik algoritmayı $n = 6, 7, 8$ için uygulamış ve önceki sonuçlardan daha iyi doğrusal olmama değerleri elde etmiştir. Kazymyrov vd. [19] dereceli azalma yöntemi ile doğrusal olmama, farksal birbiçimlilik, cebirsel derece ve cebirsel bağışıklık özellikleri bakımından en iyi olan 8×8 büyüklüğündeki S-kutuları için arama gerçekleştirmişlerdir. Ayrıca bu çalışmada, başlangıç fonksiyonu olarak ters fonksiyonun seçilmesi durumda, [18] çalışmasından daha yüksek doğrusal olmama değerine sahip S-kutularının bulunduğu belirtilmiştir. Doğrusal olmama ve farksal birbiçimlilik özellikleri güçlü olan fakat permütasyon olmayan bazı kuvvet fonksiyonlarından sezgisel arama ile bijektif S-kutusu elde etme yöntemi Mamadolimov vd. [20] tarafından önerilmiştir. Bu yöntem, Isa vd. [21] tarafından tüm kuvvet fonksiyonlarına genelleştirilmiş ve S-kutusunu bijektif hale getirmek için geliştirdikleri (fazlalık giderme olarak isimlendirilen) algoritma $GF(2)^8$ uzayında uygulanmıştır. Isa vd. [22] daha sonra arıların sallanma dansından esinlenerek tasarladıkları sezgisel arama algoritmasını, başlangıç fonksiyonu olarak seçtikleri ters fonksiyona eşdeğer olan üç terimli bir polinoma uygulayarak önceki sonuçları geliştirmişlerdir. Ivanov vd. [23], ters fonksiyondan elde ettikleri başlangıç popülasyonunu kullanan genetik algoritma ile 8×8 büyüklüğündeki S-kutuları için en yüksek doğrusal olmama değeri olan 112'ye ulaşmışlardır. Aynı çalışmada, benzer yaklaşımla 16×16 büyüklüğündeki S-kutuları için de güçlü kriptografik özellikler elde edilmiştir. Bahsedilen çalışmalardan başlangıç olarak rastgele üretilen S-kutularının kullanıldığı arama algoritmalarının tümü, 8×8 büyüklüğündeki tüm bijektif S-kutularının oluşturduğu (büyüklüğü 2^{1684} olan) arama uzayında koşulmuştur. Bu şekilde yürütülen (ters fonksiyondan başlayarak veya belirli bir matematiksel inşa yöntemini kullanarak arama yapmayan) sezgisel aramaların ürettiği S-kutularının en iyi doğrusal olmama ve farksal birbiçimlilik değerlerinin sırasıyla 104 ve 6 olduğu görülmektedir. Bununla birlikte, Döngüsel Simetrik S-Kutuları (DSSK'lar), DSSK'ların bağlaşımları ve k-DSSK'ların (burada k, $n\times n$ büyüklüğündeki S-kutusu için n'yi bölen ve 1'den büyük sabit bir tamsayıdır) oluşturduğu alt uzaylarda yapılan aramalar sonucunda daha yüksek doğrusal olmama değerleri elde edilebilmektedir [13, 24].

Tablo 1. Bijektif S-kutuları için arama uzaylarının büyüklükleri.

Arama Uzayı	Değişken Sayısı (n)		
	6	8	10
Tüm uzay	2^{296}	2^{1684}	2^{8769}
DSSK uzayı	$2^{47.9}$	$2^{208.3}$	$2^{872.4}$
Bağlaşım uzayı	$2^{61.3}$	$2^{243.7}$	$2^{976.1}$
2-DSSK uzayı	$2^{97.4}$	$2^{412.2}$	$2^{1754.3}$
$(n/2)$-DSSK uzayı	$2^{141.2}$	$2^{824.7}$	$2^{4345.2}$

DSSK'lar ilk olarak 2008'de Rijmen vd. [25] tarafından tanımlanmıştır. Bu tanım tek çıkışlı döngüsel simetrik Boole fonksiyonları (DSBF) tanımının çok çıkışlı Boole fonksiyonları olan S-kutularını kapsayacak şekilde genişletilmesi olarak görülebilir. Bir $n\times n$ S-kutusu, $1 \le i \le n$ olmak üzere, her bir girişi i kere döngüsel olarak kaydırıldığında karşılık gelen çıkışı da i kere döngüsel olarak kayıyorsa döngüsel simetrik olarak isimlendirilir; diğer bir ifadeyle, $n\times n$ DSSK'lar $\pi(x_0, x_1, \ldots, x_{n-1}) = (x_1, x_2, \ldots, x_{n-1}, x_0)$ permütasyonuna göre simetrik S-kutuları olarak düşünülebilir. Benzer şekilde, büyüklüğü $n\times n$ olan k-DSSK'lar ise $\pi(x_0, x_1, \ldots, x_{n-1}) = (x_k, x_{k+1}, \ldots, x_{n-1}, x_0, x_1, \ldots, , x_{k-1})$ permütasyonuna göre simetrik S-kutuları olarak tanımlanır. DSSK'ların kuvvet fonksiyonlarından ve bunların toplamından üretilen S-kutuları ile doğrusal ilişkili olduğu gösterilmiştir [25]. Temel kriptografik özellikler doğrusal dönüşüm altında değişmediğinden, yüksek doğrusal olmama, düşük farksal birbiçimlilik ve yüksek cebirsel derece gibi istenilen kriptografik özellikleri barındıran ters fonksiyon, Dobbertin, Gold, Kasami fonksiyonları ve benzeri inşalar [6], birer DSSK olarak düşünülebilir. Bu yüzden DSSK sınıfı bahsedilen kriptografik özelliklere sahip S-kutuları açısından zengin bir sınıf oluşturmaktadır. İki tane $(n-1)\times(n-1)$ DSSK'nın bağlaşımı olarak tanımlanan [24] $n\times n$ S-kutuları, $\pi(x_0, x_1, \ldots, x_{n-1}) = (x_0, x_2, \ldots, x_{n-1}, x_1)$ permütasyonuna göre simetrik S-kutularıdır. $n = 6$ için DSSK'lar ve bağlaşımlar üzerine daha önce yapılan çalışmalarda [24, 26], verimli bir tüketici arama algoritması gerçekleştirilmiş ve bu alt uzaylarda ters fonksiyonla aynı doğrusal olmama ve farksal birbiçimlilik değerlerine sahip olan, aynı zamanda ters fonksiyonla afin ilişkili olmayan S-kutuları elde edilmiştir. Ayrıca, bağlaşım yöntemi ile oluşturulan 8×8 S-kutuları için gerçekleştirilen arama algoritması ile doğrusal olmama değeri 106 olan S-kutuları üretilmiştir [24]. 8×8 büyüklüğündeki simetrik S-kutuları üzerine yapılan çalışmada [13] ise, DSSK'lar için uygulanan arama algoritması ile 108 doğrusal olmama değerine ulaşılmıştır.

Blok şifreler ağırlıklı olarak 8 ve daha küçük boyutlu uzaylarda tanımlı olan S-kutularını kullanmaktadır. Bununla birlikte, daha büyük boyutlarda S-kutusu kullanan blok şifreler de bulunmaktadır (örneğin, Kasumi [27] 9×9 S-kutusu kullanmaktadır). Bu çalışma, bildiğimiz kadarıyla, 10×10 S-kutuları için rastgele veya sezgisel aramanın gerçekleştirildiği ilk çalışma niteliğindedir. Özel olarak, 10 boyutlu durumda arama uzayı büyüklükleri sırasıyla $2^{872.4}$ ve $2^{976.1}$, $2^{1754.3}$ ve $2^{4345.2}$ olan DSSK'ların, bağlaşımların, 2-DSSK'ların ve 5-DSSK'ların oluşturduğu alt uzaylarda, bijektif S-kutuları rastgele arama yöntemi ve en dik iniş prensibine dayalı arama algoritması [28] ile aranmıştır. AES S-kutusunun giriş ve çıkış bitleri arasındaki en yüksek doğrusal ilişki olasılığının 0.5625 ve en yüksek farksal olasılığının (S-kutusunun girişine uygulanan bir fark ile çıkışında elde edilen farkın aynı kalma olasılığı) 0.015625 olduğu bilinmektedir. Gerçekleştirdiğimiz arama sonucu üretilen 10×10 büyüklüğündeki S-kutuları için hesaplanan en iyi doğrusallık ve farksal olasılıkları ise sırasıyla 0.5546875 ve 0.0078125 olarak bulunmuştur. AES S-kutusundan daha düşük olan olasılık değerleri, arama yöntemi ile bahsedilen alt uzaylarda üretilen S-kutularının doğrusal ve farksal kriptanalize karşı daha dayanıklı olabildiğini göstermektedir. Bunun yanı sıra, AES S-kutusunun cebirsel bağışıklık açısından (8 boyutlu durum için) en iyi özellikleri sağlamadığı bilinmektedir. Çalışmamızda elde edilen S-kutularının ise hem AES S-kutusundan daha iyi cebirsel bağışıklık özelliklerine sahip oldukları hem de 10 boyutlu durum için cebirsel bağışıklık açısından en iyi oldukları bulunmuştur. Ayrıca, büyük S-kutularının yan kanal analizine karşı dayanıklılığı artırabildiği bilinmektedir [29] ve DSSK'lar sadece yörünge temsilcileri ile ifade edilebildiğinden donanım ve yazılım açısından verimli bir şekilde gerçeklenebilirler [25]; bu nedenle, çalışmamızda elde edilen sonuçlar pratik açıdan da önem taşımaktadır. Diğer taraftan, sezgisel arama algoritmasının başlangıç S-kutusu $GF(2)^{10}$ uzayında tanımlı ters fonksiyon olarak alındığında, ters fonksiyon ile aynı veya yakın kriptografik özelliklere sahip S-kutularının da elde edilebildiği gözlenmiştir.

S-kutularının kriptografik özellikleri, arama algoritmasında kullanılan maliyet fonksiyonu ve simetrik S-kutuları üzerine bir sonraki bölümde sunulan temel bilgilerden sonra, Bölüm 3'te kullandığımız arama algoritmasının genel yapısı ile birlikte gerçekleştirme detayları verilmektedir. Bölüm 4'te arama algoritması ile elde edilen kriptografik özellikler sunularak AES S-kutusunun özellikleri ile karşılaştırılmış ve sonuç bölümü ile makalemiz sonlandırılmıştır.

2. Temel bilgiler

Bir Boole fonksiyonu $f : GF(2)^n \to GF(2)$, n biti bir bite gönderen bir fonksiyondur ve tek çıkışlı Boole fonksiyonu olarak da isimlendirilir. f fonksiyonun Hamming ağırlığı, doğruluk tablosundaki birlerin sayısı olarak tanımlanır. Doğruluk tablosunda birlerin sayısı sıfırların sayısına eşit olan Boole fonksiyonuna dengeli denir. Kriptografik açıdan kullanılabilir olması için, Boole fonksiyonun dengeli olması gerekmektedir. İki Boole fonksiyonu arasındaki Hamming uzaklık, doğruluk tablolarında aynı pozisyonlarda bulunan farklı bitlerin sayısı olarak tanımlanır.

$n\times m$ büyüklüğünde bir S-kutusu $S : GF(2)^n \to GF(2)^m$ ise, n biti m bite gönderen çok çıkışlı bir Boole fonksiyon olarak tanımlanır. Herhangi bir S-kutusu S, $x = (x_0, x_1, \ldots, x_{n-1}) \in GF(2)^n$ olmak üzere, n-değişkenli Boole fonksiyonlarının oluşturduğu bir kombinasyon, diğer bir ifadeyle $S(x) = (f_0(x), f_1(x), \ldots, f_{m-1}(x))$ olarak düşünülebilir. Buradaki f_i fonksiyonları ($i = 0, 1, \ldots, m-1$) koordinat fonksiyonları, bu fonksiyonların sıfırdan farklı ($2^m - 1$ tane) lineer kombinasyonları ise bileşen fonksiyonları olarak isimlendirilir. Sıfır vektöründen farklı bir $\omega = (\omega_0, \omega_1, \ldots, \omega_{m-1}) \in GF(2)^m$ için karşılık gelen bileşen fonksiyonu f_ω ile gösterilir ve aşağıdaki eşitlik ile elde edilir:

$$f_\omega(x) = \omega_0 f_0(x) \oplus \omega_1 f_1(x) \oplus \ldots \oplus \omega_{m-1} f_{m-1}(x). \quad (1)$$

Bu bölümde S-kutuları için verilen doğrusal olmama, mutlak gösterge ve cebirsel derece özellikleri, tek çıkışlı Boole fonksiyonları için tanımlanan kriptografik özelliklerin m-bit çıkışlı S-kutularına genişletilmesi olarak görülebilir.

2.1 Cebirsel derece

Herhangi bir Boole fonksiyon $f : GF(2)^n \to GF(2)$, çıkış bitlerinin oluşturduğu 2^n uzunluğundaki doğruluk tablosu ile veya cebirsel normal biçim olarak isimlendirilen, GF(2) üzerinde çok değişkenli bir polinom ile eşsiz şekilde gösterilebilir. Değişken sayısı n için, cebirsel normal biçimin genel ifadesi aşağıdaki gibidir:

$$f(x) = a_0 \oplus a_1 x_0 \oplus \ldots \oplus a_n x_{n-1} \oplus a_{12} x_0 x_1 \oplus a_{13} x_0 x_2 \oplus \ldots \oplus a_{12\ldots n} x_0 x_1 \ldots x_{n-1}, \quad (2)$$

burada $a_0, a_1, \ldots, a_{12}, a_{13}, \ldots, a_{12\ldots n} \in GF(2)$ eşsiz sabitlerdir ve Möbius dönüşümü ile doğruluk tablosundan elde edilebilir. f Boole fonksiyonunun cebirsel derecesi d_f, cebirsel normal biçimindeki terimlerin sahip olduğu en yüksek değişken sayısıdır. Derecesi en fazla bir olan fonksiyonlar afin fonksiyonlar, sabit terimi sıfır ($a_0 = 0$) olan afin fonksiyonlar ise doğrusal fonksiyonlar olarak adlandırılır.

$n\times m$ büyüklüğünde bir S-kutusu S için cebirsel derece (d_S) değeri, bileşen fonksiyonların aldığı kriptografik açıdan en kötü değer olarak tanımlanır. Diğer bir ifadeyle,

$$d_S = \min_{\omega \neq \mathbf{0} \in GF(2)^m} d_{f_\omega}. \quad (3)$$

Bir S-kutusunun yüksek mertebeden farksal kriptanaliz [5] yöntemine karşı dayanıklı olabilmesi için yüksek cebirsel dereceye sahip olması beklenir.

2.2 Doğrusal olmama

f Boole fonksiyonunun Walsh-Hadamard dönüşümü (veya spektrumu), tüm doğrusal fonksiyonlar ile korelasyonunu görmemizi sağlayan bir dönüşümdür:

$$W_f(w) = \sum_{x \in GF(2)^n} (-1)^{f(x)} (-1)^{w \cdot x}. \quad (4)$$

NL_f doğrusal olmama değerini, spektrumdaki mutlak değerce en büyük değer belirler ve aşağıdaki gibi hesaplanır:

$$NL_f = 2^{n-1} - \frac{1}{2} \max_{w \in GF(2)^n} |W_f(w)|. \quad (5)$$

Diğer bir ifadeyle, bir Boole fonksiyonun doğrusal olmama değeri, tüm afin fonksiyonlara olan Hamming uzaklıklarının en küçüğüdür. Çift değişken sayısı n için, doğrusal olmama değeri açısından en iyi olan Boole fonksiyonları bükük fonksiyonlar olarak isimlendirilir ve (Parseval teoreminden) n-değişkenli bir bükük fonksiyonun tüm spektrum değerleri mutlak değerce $2^{n/2}$'ye eşittir. Fakat bükük fonksiyonlar dengeli değillerdir ve cebirsel dereceleri düşüktür.

Herhangi bir $n\times m$ S-kutusu S için doğrusal olmama (NL_S) değeri, bileşen fonksiyonlarının aldığı en düşük doğrusal olmama değeri olarak tanımlanır. Diğer bir ifadeyle,

$$NL_S = \min_{\omega \neq \mathbf{0} \in \mathrm{GF}(2)^m} NL_{f_\omega}. \quad (6)$$

Bir Boole fonksiyonun doğrusal olmama özelliği, tüm afin fonksiyonlara uzaklıklarının en küçüğü olarak tanımlandığından, doğruluk tablosundaki $2^n - NL_f$ tane bitin afin bir fonksiyonla aynı olduğu ve bu nedenle afin bir fonksiyonla aynı çıktıyı üretme olasılığının (diğer bir ifadeyle doğrusallık olasılığının) $(2^n - NL_f)/2^n$ olduğu görülmektedir. Doğrusal ilişkinin azalması için, bu değerin 0.5'e yaklaşması gerektiğine dikkat edilmelidir. Bir S-kutusu için ise doğrusallık olasılığı, bileşen fonksiyonlarının en kötü (en yüksek) doğrusallık olasılığıdır ve bu değer p_d ile gösterilir. Doğrusal kriptanaliz [2] karşısında dayanıklılık için, S-kutusunun yüksek doğrusal olmama değerine sahip olması beklenir.

Bir S-kutusunun bileşen fonksiyonlarının tüm doğrusal fonksiyonlara yakınlıkları, Doğrusal Yaklaşım Tablosu (DYT) [2, 30, 31] ile ölçülmektedir. $n \times m$ büyüklüğündeki bir S-kutusu S için karşılık gelen DYT, $2^n \times 2^m$ büyüklüğündedir ve bu tablonun her bir elemanı aşağıdaki eşitlik ile bulunur:

$$DYT(u, v) = \#\{x \in \mathrm{GF}(2)^n : u \cdot x = v \cdot S(x)\} - 2^{n-1}, \quad (7)$$

burada $u \in \mathrm{GF}(2)^n$, $v \in \mathrm{GF}(2)^m$ ve "$\cdot$" işlemi iç çarpım işlemidir. Diğer bir ifadeyle, $v \cdot S(x)$ bileşen fonksiyonunun $u \cdot x$ doğrusal fonksiyonuna eşit olma olasılığı $DYT(u, v)/2^n + 0.5$ olur. Ayrıca, S-kutusunun doğrusal olmama değeri, DYT değerleri kullanılarak aşağıdaki eşitlikle bulunabilir:

$$NL_S = 2^{n-1} - \max_{(u,v) \neq (\mathbf{0},\mathbf{0})} |DYT(u, v)|. \quad (8)$$

DYT'deki mutlak değer bakımından en yüksek değer ne kadar küçükse, p_d olasılığının da 0.5'e o kadar yakındır.

2.3 Farksal birbiçimlilik

Herhangi bir $n \times m$ S-kutusu S'nin farksal birbiçimlilik değeri δ_S, $S(x) \oplus S(x \oplus \gamma) = \beta$ eşitliğini sağlayan $x \in \mathrm{GF}(2)^n$ girişlerinin en yüksek sayısıdır ve bu durumda S'ye farksal-δ_S birbiçimlidir denir. Bu tanımdan, S-kutusunun girişine uygulanan bir fark ile karşılık gelen çıkış farkının değişmeme olasılığının $\delta_S/2^n$ olduğu görülmektedir. Bu değer p_f ile gösterilir ve en düşük 2^{n-1} olabilmektedir. Bir S-kutusunun farksal kriptanalize [1] karşı dayanıklı olabilmesi için düşük farksal birbiçimlilik değerine sahip olması beklenir.

Her bir giriş ve çıkış farkı (γ, β) çifti için $S(x) \oplus S(x \oplus \gamma) = \beta$ eşitliğini sağlayan x girişlerinin sayısı Fark Dağılım Tablosu (FDT) ile verilmektedir [1, 30, 31]. S'nin FDT'si $2^n \times 2^m$ büyüklüğündedir ve tablo elemanları aşağıdaki eşitlik ile bulunur:

$$FDT(\gamma, \beta) = \#\{x \in GF(2)^n : S(x) \oplus S(x \oplus \gamma) = \beta\}. \quad (9)$$

Farksal birbiçimlilik değeri, FDT değerleri kullanılarak aşağıdaki gibi bulunabilir:

$$\delta_S = \max_{(\gamma,\beta) \neq (\mathbf{0},\mathbf{0})} FDT(\gamma, \beta). \quad (10)$$

2.4 Cebirsel bağışıklık

S-kutularının giriş ve çıkış bitleri arasında düşük dereceye sahip çok değişkenli polinomlar ile tanımlanan ilişkilerin varlığı, cebirsel saldırılarda kullanılabilmektedir. Büyüklüğü $n \times m$ olan herhangi bir S-kutusu S, $(x_0, x_1, \ldots, x_{n-1}) \in \mathrm{GF}(2)^n$ giriş bitlerini ve $(y_0, y_1, \ldots, y_{m-1}) \in \mathrm{GF}(2)^m$ çıkış bitlerini temsil etmek üzere, aşağıda verilen (r tane) eşitliklerden oluşan bir sistem ile tanımlanabilir:

$$\begin{aligned} &g_0(x_0, x_1, \ldots, x_{n-1}, y_0, y_1, \ldots, y_{m-1}) = 0, \\ &g_1(x_0, x_1, \ldots, x_{n-1}, y_0, y_1, \ldots, y_{m-1}) = 0, \\ &\quad\vdots \\ &g_{r-1}(x_0, x_1, \ldots, x_{n-1}, y_0, y_1, \ldots, y_{m-1}) = 0. \end{aligned} \quad (11)$$

S-kutusunun cebirsel bağışıklığı (I_S) sistemdeki tüm polinomların en düşük derecesi olarak tanımlanır:

$$I_S = \min_{0 \leq i \leq r-1} \deg(g_i). \quad (12)$$

Sistemi oluşturan bağımsız eşitliklerin sayısı N_S parametresi ile verilmektedir. Bir S-kutusunun cebirsel saldırılar karşısında dayanıklı olması için cebirsel bağışıklık değerinin yüksek ve bununla birlikte eşitlik sayısının düşük olması beklenir. Çalışmamızda ele aldığımız 8×8 ve 10×10 S-kutuları için ulaşılabilecek en iyi (I_S, N_S) değerleri sırasıyla (3, 441) ve (3, 327)'dir [32, 33].

2.5 Mutlak gösterge

Özilinti fonksiyonu $r_f(d)$, f Boole fonksiyonu ile girişine $d \in \mathrm{GF}(2)^n$ farkı uygulandığında elde edilen versiyonu arasındaki korelasyonu verir:

$$r_f(d) = \sum_{x \in \mathrm{GF}(2)^n} (-1)^{f(x)} (-1)^{f(x \oplus d)}. \quad (13)$$

Özilinti spektrumuyla ilişkili olan ve global çığ etkisi karakteristiği [34] olarak adlandırılan iki önemli kriptografik özellik, mutlak gösterge ve kareler toplamı göstergesidir. Mutlak gösterge AI_f (özilinti fonksiyonu $d = (0, .., 0)$ için her zaman 2^n'ye eşit olduğundan) $r_f(0, \ldots, 0)$ haricinde özilinti spektrumunda bulunan mutlak değerce en büyük değer olarak tanımlanır:

$$AI_f = \max_{d \neq \mathbf{0} \in \mathrm{GF}(2)^n} |r_f(d)|, \quad (14)$$

burada $\mathbf{0} = (0, \ldots, 0)$.

$n \times m$ büyüklüğünde bir S-kutusu S için mutlak gösterge (AI_S) değeri, bileşen fonksiyonların mutlak gösterge değerlerinin en düşüğü olarak tanımlanır:

$$AI_S = \min_{\omega \neq \mathbf{0} \in \mathrm{GF}(2)^m} AI_{f_\omega}. \quad (15)$$

Çalışmamızda maliyet fonksiyonu seçiminde kullanılan ve global çığ etkisi karakteristiklerinden diğeri olan kareler toplamı göstergesi, özilinti spektrumundaki değerlerin karelerinin toplamıdır:

$$\sum_{d \in \mathrm{GF}(2)^n} r_f^2(d). \quad (16)$$

Mutlak ve kareler toplamı göstergelerinin düşük olması, S-kutusunun iyi difüzyon özellikleri taşıdığını gösterir.

2.6 Maliyet fonksiyonu

Kareler toplamı göstergesi ile Walsh-Hadamard spektrumu aşağıda verilen teorem ile ilişkilendirilir.

Teorem 1 [35].

$$\sum_{d \neq \mathbf{0} \in \mathrm{GF}(2)^n} r_f^2(d) = 2^{-n} \sum_{w \in \mathrm{GF}(2)^n} \left(W_f^2(w) - 2^n\right)^2. \quad (17)$$

Teorem 1'den, özilinti değerlerindeki (mutlak değerce) minimizasyonun, aynı zamanda Walsh-Hadamard değerlerini (doğrusal olmama yönünden en iyi olan) bir bükük fonksiyon spektrumuna yaklaştıracağı görülmektedir. Bu nedenle, arama algoritmamızda S-kutusunun bileşen fonksiyonlarının kareler

toplamı göstergeleri minimize edilmeye çalışılmış ve maliyet fonksiyonu olarak bu göstergelerin toplamı seçilmiştir.

2.7 Simetrik S-kutuları

Herhangi bir S-kutusu $S : \mathrm{GF}(2)^n \to \mathrm{GF}(2)^n$, $\pi(x_0, x_1, \ldots, x_{n-1})$ bir permütasyon olmak üzere, her $x = (x_0, x_1, \ldots, x_{n-1}) \in \mathrm{GF}(2)^n$ için $S(\pi(x)) = \pi(S(x))$ koşulunu sağlıyorsa π permütasyonu altında simetrik S-kutusu olarak isimlendirilir. π permütasyonuna göre, bir x vektörü tarafından üretilen yörünge

$$G_n(x) = \{\pi^k(x) \mid 1 \le k \le n\} \tag{18}$$

ile tanımlanır ve yörüngede bulunan vektörlerin sözlüksel (leksikografik) sıralanışında ilk sırada yer alan vektör yörünge temsilcisi olarak isimlendirilir. $n \times n$ büyüklüğünde simetrik bir S-kutusu için toplam yörünge sayısı g_n ile gösterilir.

DSSK'lar $\pi(x_0, x_1, \ldots, x_{n-1}) = (x_1, x_2, \ldots, x_{n-1}, x_0)$ permütasyonu altında ve bağlaşımlar $\pi(x_0, x_1, \ldots, x_{n-1}) = (x_0, x_2, \ldots, x_{n-1}, x_1)$ permütasyonu altında simetrik S-kutuları olarak düşünülebilir. Değişken sayısı n çift olmak üzere, 2-DSSK'lar ve $(n/2)$-DSSK'lar ise sırasıyla $\pi(x_0, x_1, \ldots, x_{n-1}) = (x_2, x_3, \ldots, x_{n-1}, x_0, x_1)$ ve $\pi(x_0, x_1, \ldots, x_{n-1}) = (x_{n/2}, x_{n/2+1}, \ldots, x_{n-1}, x_0, x_1, \ldots, x_{n/2-1})$ permütasyonlarına göre simetriktir. $n = 10$ durumunda $\mathrm{GF}(2)^{10}$ vektör uzayı, DSSK'lar için 1, 2, 5 ve 10 büyüklüğünde sırasıyla 2, 1, 6 ve 99 yörüngeye, bağlaşımlar için ise 1, 3 ve 9 büyüklüğünde sırasıyla 4, 4 ve 112 yörüngeye bölüntülenmektedir.

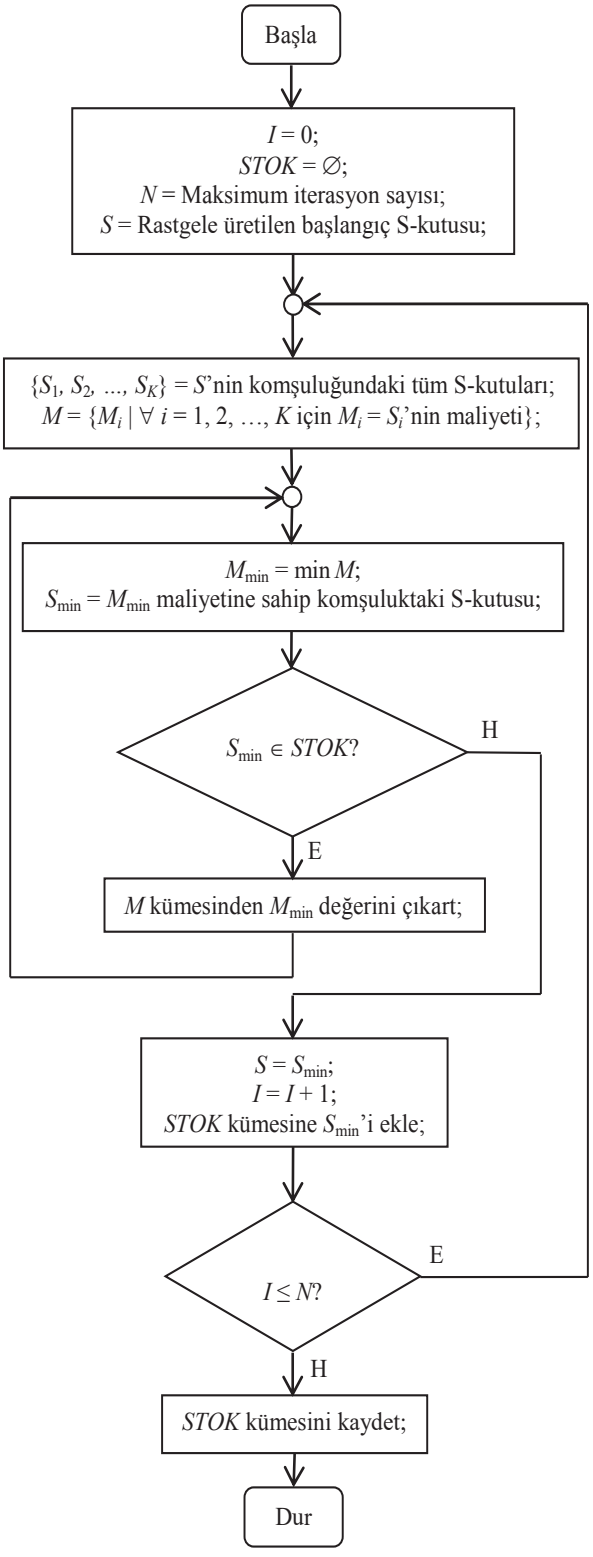
3. Arama algoritması

DSSK'lar ve bağlaşımlar için gerçekleştirilen en dik iniş prensibine dayalı sezgisel arama algoritmasının akış diyagramı Şekil 1'de verilmiştir. Algoritma, DSSK'lar veya bağlaşımların oluşturduğu alt uzayda rastgele üretilen bir S-kutusu (S) ile başlamaktadır ve arama aynı alt uzayda gerçekleşmektedir. İterasyon sayısı (N) denemelerimizde 400 olarak alınmıştır. Aynı iterasyon çıktılarının üretilmesini engellemek için her iterasyon çıktısı *STOK* kümesine kaydedilir. Algoritmanın her bir iterasyonunda, iterasyon girişindeki S-kutusunda aşağıda verilen değişiklikler yapılarak, iterasyon çıktısı için aday S-kutularının bulunduğu ve bunların her biri için maliyet fonksiyonunun hesaplandığı bir komşuluk oluşturulmaktadır.

- Büyüklüğü birden fazla olan çıkış yörüngelerinin olası tüm permütasyonları ile yer değiştirmesi. Diğer bir ifadeyle, her $1 \le k < t$ değeri için çıkış yörüngesinde bulunan tüm $S(x)$ vektörleri $\pi^k(S(x))$ olarak değiştirilir, burada t değeri $\pi^t(x) = x$ eşitliğini sağlayan en küçük değerdir. Örneğin, DSSK'lar için 10 büyüklüğünde 99 yörünge bulunmaktadır; buna göre, böyle bir yörüngedeki vektörler en fazla 9 kere kaydırılabilir ve böylelikle $9 \times 99 = 891$ komşu elde edilir. Bu adımda DSSK'lar için 916 ve bağlaşımlar için 904 komşu üretilir.

- Aynı büyüklükte iki farklı çıkış yörüngesinin permütasyonları göz önüne alınmadan birbiri ile değiştirilmesi. Örneğin bu şekilde, DSSK'lar için 10 büyüklüğündeki 99 yörüngeden $99 \times 98/2 = 4851$ komşu elde edilir. Böylelikle DSSK'lar için 4867, bağlaşımlar için 6228 komşu bulunur.

Bu iki adımın sonunda komşulukta bulunan S-kutularının toplam sayısı (Şekil 1'deki K parametresi) DSSK'lar için 5783 ve bağlaşımlar için 7132 bulunmaktadır. Her iterasyonda, iterasyon girdisi S'nin komşuluğunda bulunan S-kutularının



Şekil 1. En Dik İniş Prensibine Dayalı Arama Algoritması.

maliyetleri hesaplanır ve *STOK* kümesinde bulunmayan en düşük maliyetli S-kutusu, iterasyon çıktısı olarak *STOK* kümesine eklenir.

Komşuluktaki herhangi bir S-kutusu için algoritmada kullanılan maliyet fonksiyonu, (6×6 ve 8×8 S-kutuları için yapılan çalışmalarda [13, 26] iyi sonuçlar veren) bileşen fonksiyonlarının kareler toplamı göstergelerinin toplamıdır:

$$\sum_{\omega \neq \mathbf{0} \in \mathrm{GF}(2)^n} \sum_{d \neq \mathbf{0} \in \mathrm{GF}(2)^n} r_{f_\omega}^2(d), \tag{19}$$

burada $d = \mathbf{0}$ için özilinti değeri sabit olduğundan hesaplamaya katılmamaktadır.

Algoritma C dilinde gerçeklenmiş ve Windows 8.1 Pro işletim sistemi, Intel(R) Xeon(R) CPU E5-1650 v3 @ 3.50GHz işlemci ve 16 GB RAM'e sahip bir bilgisayarda bütün çekirdekler kullanılarak iki hafta çalıştırılmıştır. N = 400 için algoritmanın tek çekirdek üzerinde bir kere koşulması DSSK'larda 2 saat sürerken, bağlaşımlarda 2.5 saat, 2-RSSB'lerde 9 saat ve 5-RSSB'lerde ise yaklaşık 6 gün sürmektedir. Algoritmanın kodları [36]'da verilen bağlantıdan indirilebilmektedir.

3.1 Zaman ve bellek karmaşıklığı

Algoritma kısır döngüye girmemek için, her iterasyon sonucunu önceki iterasyon sonuçları ile karşılaştırmaktadır. Bu nedenle, genel olarak $n \times n$ büyüklüğündeki S-kutuları için algoritmanın koşulduğu düşünülürse, N iterasyon için $2^n N(N-1)/2$ karşılaştırma işlemi yapılmaktadır. Herhangi bir iterasyonda, önceki iterasyon sonuçlarından birisi üretilirse karşılaştırma işlemi tekrar etmektedir; bununla birlikte, yapılan tekrarın işlem yükü açısından etkisi sınırlıdır. Ayrıca, her iterasyonda her bir komşuluk için (19) ile verilen maliyet fonksiyonu hesaplanmaktadır. Maliyet fonksiyonunu bileşen fonksiyonlarının kareler toplamı göstergelerini kullanarak hesaplamak, özilinti değerlerini elde etmek için iki kere Walsh-Hadamard dönüşümü almayı gerektirir. Bunun yerine, ((17) eşitliğinden) doğrudan Walsh-Hadamard spektrumlarını kullanarak hesaplamak daha verimlidir. n değişkenli bir Boole fonksiyonun Walsh-Hadamard dönüşümünün $n2^n$ toplama ve çıkarma işlemi ile elde edilebildiği bilinmektedir. Mutlak Walsh-Hadamard değerlerinin dağılımı afin dönüşüm altında değişmez olduğundan, simetrik bir S-kutusunun maliyet fonksiyonunu hesaplamak için bütün bileşen fonksiyonlar yerine sadece birbiri ile afin ilişkili olmayan ($g_n - 1$ tane) bileşen fonksiyonların Walsh-Hadamard spektrumlarını elde etmek yeterlidir. Bu spektrumların tümü elde edildikten sonra, (17) eşitliğini kullanarak maliyet fonksiyonunun hesaplanması için, kare alma işlemlerinin yapılması gerektiği görülmektedir. Buna karşın, olası tüm Walsh-Hadamard dönüşümü değerleri için $\left(W_f^2(w) - 2^n\right)^2$ işleminin karşılık gelen sonuçları önceden bir diziye atılarak, çarpma işlemi yapılmadan $2^n(g_n - 1)$ toplama işlemi ile maliyet fonksiyonu hesaplanabilir. Bunun sonucunda, N iterasyon ve K komşu için $(n+1)2^n(g_n - 1)NK$ toplama ve çıkarma işleminin yapılması gerektiği görülmektedir. Bu nedenle, simetrik S-kutuları için komşu sayısı $K \approx \binom{g_n}{2} + ng_n$ olduğundan, sabit iterasyon sayısı için asimptotik zaman karmaşıklığı $O(n2^n g_n^3)$ olarak elde edilir.

Kriptografik elemanların tasarımında yaygın olarak kullanılan tavlama benzetimi ve tepe tırmanma gibi diğer benzer arama yöntemleri ile karşılaştırıldığında, en dik iniş prensibine dayalı arama algoritmasında olduğu gibi tüm komşulukta arama yapmadıkları için, bu yöntemlerin daha verimli oldukları düşünülebilir. Bununla birlikte, tepe tırmanma algoritmasının zayıf yönü yerel minimumdan kaçamamasıdır. Tavlama benzetimi algoritması ise tüm komşulukta arama yapmamaktadır ve bu nedenle daha iyi sonuçları kaçırma olasılığı bulunmaktadır. Ayrıca, başlangıç sıcaklığı, soğutma çarpanı, (bir iterasyonda rastgele üretilen) komşu sayısı gibi parametrelerinin ayarlanmasına ihtiyaç duymaktadır. Gerek tavlama benzetimi gerek tepe tırmanma yöntemlerinde, belirli bir komşu üretme operatörü ile elde edilebilen tüm komşuluğa bakıldığı varsayıldığında, asimptotik karmaşıklıklarının en dik iniş prensibine dayalı arama algoritmasınınki ile aynı olduğu görülmektedir. Burada elde edilen avantaj, yerel minimuma takılmadan her zaman komşuluk içerisindeki en iyi çözümün üretilmesidir. Bellek açısından değerlendirdiğimizde, en dik iniş prensibine dayalı arama algoritması her iterasyon çıktısını kaydetmektedir ve bu yüzden belirlenebilecek en yüksek iterasyon sayısı kullanılan bellek kapasitesi ile sınırlıdır. İterasyon çıktılarını kaydetmek için ihtiyaç duyulan bellek miktarının $n2^n N$ bit olduğu kolaylıkla görülebilir. Bunun yanı sıra, simetrik S-kutuları yörünge temsilcileri ile temsil edilebildiğinden, sadece $ng_n N$ bit, tüm iterasyon çıktılarını kaydetmek için yeterlidir. Örneğin, döngüsel simetrik S-kutuları için $g_n \approx \frac{2^n}{n}$ olduğundan, gerek duyulan belleğin $2^n N$ bit olduğu görülür. Bu gereksinim, genellikle makul büyüklükteki S-kutuları ve iterasyon sayıları için karşılanabilir niteliktedir.

4. Bulgular

En dik iniş prensibine dayalı sezgisel arama ve rastgele arama algoritmalarından elde edilen en iyi sonuçlar ile birlikte AES S-kutusunun kriptografik özellikleri Tablo 2'de sunulmuştur. Tablo 2'den, bağlaşımlar için elde edilen sonuçların, DSSK'lar için elde edilen sonuçlara yakın olduğu gözlenmektedir. Sezgisel aramanın rastgele aramadan daha iyi sonuçlar verdiği, her iki alt uzayda da en yüksek olmama değerinin 456, en düşük farksal birbiçimliliğin 8 ve en düşük mutlak göstergenin 168 bulunduğu görülmektedir; bununla birlikte DSSK alt uzayında bulunan 456 doğrusal olmama değerine sahip sonucun farksal birbiçimlilik değeri (δ_S = 10) daha iyi çıkmıştır.

Tablo 2. (NL_S, AI_S, δ_S, d_S), (p_d, p_f) ve (I_S, N_S) sonuçlarının karşılaştırılması.

	DSSK'lar	Bağlaşımlar
Rastgele arama	(450, 200, 12, 9) (448, 200, 10, 9) (440, 176, 14, 9)	(450, 304, 12, 9) (448, 334, 10, 9) (440, 176, 12, 9)
En iyi (p_d, p_f)	(0.560546875, 0.009765625)	
En iyi (I_S, N_S)	(3, 327)	
Sezgisel arama	(456, 192, 10, 9) (454, 184, 8, 9) (448, 168, 10, 9)	(456, 192, 12, 9) (454, 184, 8, 9) (448, 168, 10, 9)
En iyi (p_d, p_f)	(0.5546875, 0.0078125)	
En iyi (I_S, N_S)	(3, 327)	
	2-DSSK'lar	5-DSSK'lar
Rastgele arama	(448, 224, 10, 9) (444, 184, 10, 9) (442, 176, 12, 9)	(442, 232, 14, 9) (440, 216, 12, 9) (432, 200, 12, 9)
En iyi (p_d, p_f)	(0.5625, 0.009765625)	
En iyi (I_S, N_S)	(3, 327)	
Sezgisel arama	(454, 208, 8, 9) (454, 176, 10, 9) (444, 176, 8, 9)	(450, 200, 10, 9)
En iyi (p_d, p_f)	(0.556640625, 0.0078125)	
En iyi (I_S, N_S)	(3, 327)	
AES S-kutusu	(112, 32, 4, 7)	
(p_d, p_f)	(0.5625, 0.015625)	
(I_S, N_S)	(2, 39)	

Rastgele üretme yöntemi ile elde edilen sonuçlardan mutlak göstergesi en düşük (AI_S = 176) olanların doğrusal olmama değerleri düşük (NL_S = 440) olduğundan, AES S-

kutusundan daha kötü doğrusallık olasılığına (p_d = (1024−440)/1024 = 0.5703125) sahip oldukları gözlenmektedir. 448 doğrusal olmama değeri AES S-kutusu ile aynı (p_d = 0.5625) ve 450 doğrusal olmama değeri ise AES S-kutusundan daha iyi (p_d = 0.560546875) doğrusallık olasılığı vermektedir. Farksal birbiçimlilik açısından bakıldığında ise rastgele üretme ile bulunan 10, 12 ve 14 değerlerinin tümü AES S-kutusundan daha düşük p_f olasılığı üretmektedir. Sezgisel arama algoritmasının her iki alt uzay için de kriptografik özellikleri iyileştirerek, AES S-kutusundan daha iyi doğrusallık ve farksal olasılıkları bulduğu görülmektedir.

Diğer taraftan, n çift olmak üzere, GF(2)^n uzayında tanımlı ters fonksiyonun $2^{n-1}-2^{n/2}$ doğrusal olmama değerine sahip farksal-4 birbiçimli olduğu bilinmektedir [11]. Sezgisel arama algoritmasında, başlangıç S-kutusu olarak rastgele üretilen bir S-kutusu (DSSK veya bağlaşım) yerine ters fonksiyon kullanıldığında, ters fonksiyon ile aynı veya yakın kriptografik özelliklere sahip S-kutuları üretilmiştir. Özel olarak, arama algoritması 400 iterasyon için koşulduğunda, bulunan doğrusal olmama değerleri 470, 472, 474, 476, 478, 480 ve farksal birbiçimlilik değerleri 4, 6, 8, 10, 14 olarak elde edilmiştir.

Karşılaştırma amaçlı olarak 2-DSSK'ların ve 5-DSSK'ların oluşturduğu alt uzaylarda yürüttüğümüz arama sonuçlarına bakıldığında, (Tablo 1'de sunulan) özellikle 5-DSSK'lar için arama uzayının büyüklüğünden dolayı diğer alt uzaylarda elde edilen sonuçlara ulaşılamadığı; bununla birlikte her iki alt uzay için de sezgisel arama algoritmasının, rastgele üretme yöntemi ile elde edilen sonuçları iyileştirdiği gözlenmektedir. Tablo 2'de sunulan sonuçlar cebirsel bağışıklık açısından ele alındığında, 10 boyutlu alt uzayların tümü için elde edilen S-kutularının cebirsel bağışıklıklarının en iyi olduğu ve AES S-kutusundan daha iyi cebirsel bağışıklık sağladıkları görülmektedir.

Tablo 2'de verilen sonuçlardan DSSK'lar için elde edilen (en iyi) 456 ve 454 doğrusal olmama değerlerine sahip S-kutularını sırasıyla S_1 ve S_2 ile, bağlaşımlar için elde edilen aynı doğrusal olmama değerlerine sahip S-kutularını sırasıyla S_3 ve S_4 ile, ve AES S-kutusunu *AES* ile gösterelim. Bu S-kutularının FDT ve DYT'leri, S-kutuları ile birlikte [36]'da verilen bağlantıdan indirilebilmektedir. Bu tablolar çok büyük olduğundan, burada (10 boyutlu durum için her biri 64×1024, 8 boyutlu durum için ise her biri 16×256 büyüklüğünde) 16 parçaya bölüntülenerek, her bir bölüntüdeki mutlak değerce en büyük değer FDT için Tablo 3'te ve her bir bölüntüdeki en büyük değer DYT için Tablo 4'te sunulmuştur.

Tablo 3. Elde edilen en iyi sonuçların ve AES S-kutusunun FDT'lerinin karşılaştırılması.

Bölüm #	S_1	S_2	S_3	S_4	*AES*
1	8	8	10	8	4
2	10	8	10	8	4
3	10	8	10	8	4
4	8	8	10	8	4
5	10	8	10	8	4
6	10	8	10	8	4
7	8	8	10	8	4
8	8	8	10	8	4
9	10	8	12	8	4
10	8	8	8	8	4
11	10	8	8	8	4
12	8	8	8	8	4
13	8	8	8	8	4
14	8	8	8	8	4
15	8	8	8	8	4
16	8	8	12	8	4

Tablo 4. Elde edilen en iyi sonuçların ve AES S-kutusunun DYT'lerinin karşılaştırılması.

Bölüm #	S_1	S_2	S_3	S_4	*AES*
1	56	58	56	58	−16
2	−56	−58	−56	58	−16
3	−56	−58	56	58	−16
4	56	58	56	−58	−16
5	56	−58	56	58	16
6	56	−58	56	−58	16
7	56	−56	56	−58	−16
8	−56	58	−56	−58	−16
9	56	58	56	56	16
10	−56	−58	56	58	16
11	56	−58	−56	56	−16
12	56	−56	56	58	−16
13	56	58	56	58	16
14	−56	56	−56	56	−16
15	−56	58	56	58	−16
16	−56	58	−56	58	16

FDT ve DYT dağılımları incelendiğinde, farksal birbiçimlilik değeri 8 olan S-kutularının, farksal birbiçimlilik değeri 10 ve 12 olan S-kutularına göre daha tekdüze FDT'lere sahip oldukları; benzer şekilde, doğrusal olmama değeri 456 olan S-kutularının, doğrusal olmama değeri 454 olan S-kutularına göre daha tekdüze DYT'lere sahip oldukları oldukları görülmektedir. AES S-kutusunun doğrusal olmama ve farksal birbiçimlilik değerlerinin en iyiye yakın olmasından dolayı, tabloların bütününe [36] bakıldığında hem FDT hem de DYT'sinin arama algoritması ile elde edilen S-kutularına göre daha tekdüze olduğu gözlenmektedir.

5. Sonuç

10×10 büyüklüğündeki S-kutuları için DSSK'lar ve bağlaşımların sırasıyla $2^{872.4}$ ve $2^{976.1}$ olan arama uzaylarında uyguladığımız rastgele veya sezgisel arama yöntemleri ile bulunan S-kutularının, doğrusal, farksal ve cebirsel kriptanalize karşı AES S-kutusundan daha dayanıklı olabileceği gösterilmiştir. Bu çalışmada elde edilen kriptografik özelliklerin ve kullanılan metodun, büyük S-kutularının aranmasında farklı sezgisel arama yöntemlerinin geliştirilmesini motive edebilecek nitelikte olduğu düşünülmektedir. Gözlemlerimiz, elde edilen S-kutularının AES S-kutusuna göre üstünlüğünü yansıtmaktan çok, S-kutusu büyüklüğünün doğrusal olmama, farksal birbiçimlilik ve cebirsel bağışıklık gibi kriptografik özelliklerin sağladığı kriptanaliz karşısında dayanıklılığa etkisinin bağımsız biçimde onaylanması olarak yorumlanmalıdır.

Kaynakça

[1] E. Biham, A. Shamir. Differential cryptanalysis of DES-like cryptosystems. Journal of Cryptology, 4(1):3-72, 1991.

[2] M. Matsui. M. Linear cryptanalysis method for DES cipher. In: EUROCRYPT'93, LNCS, vol. 765, pp. 386-397, Springer, 1994.

[3] N.T. Courtois, J. Pieprzyk. Cryptanalysis of block ciphers with overdefined systems of equations. In: Advances in Cryptology - ASIACRYPT 2002, LNCS, vol. 2501, pp. 267-287, Springer, 2002.

[4] N.T. Courtois. General principles of algebraic attacks and new design criteria for cipher components. In: Advanced Encryption Standard - AES 2004, LNCS, vol. 3373, pp. 67-83, Springer, 2005.

[5] X. Lai. Higher order derivatives and differential cryptanalysis. In: "Symposium on Communication, Coding and Cryptography", in honor of J. L. Massey on the occasion of his 60'th birthday, The Springer International Series in Engineering and Computer Science, vol. 276, pp. 27-233, Springer, 1994.

[6] C. Carlet. Vectorial Boolean functions for cryptography. In: Yves Crama, Peter L. Hammer (Eds.), Chapter of the Monography "Boolean Models and Methods in Mathematics, Computer Science, and Engineering", Cambridge University Press, pp. 398-469, 2010.

[7] C. Carlet. On highly nonlinear S-boxes and their inability to thwart DPA attacks. In: Proceedings of INDOCRYPT'05, LNCS, vol. 3797, pp. 49-62, Springer, 2005.

[8] W. Millan. How to improve the nonlinearity of bijective S-boxes. In: Australasian Conference on Information Security and Privacy, vol. 1438, pp 181-192, Springer, 1998.

[9] S. Picek, M. Cupici L. Rotim. A New Cost Function for Evolution of S-Boxes. Evolutionary Computation, 24(4):695-718, 2016.

[10] J. Daemen, V. Rijmen. AES Proposal: Rijndael. NIST Publication, 1999.

[11] K. Nyberg. Differentially uniform mappings for cryptography. In: Proceedings of EUROCRYPT'93, LNCS, vol. 765, pp. 55-64, Springer, 1994.

[12] M. A. Evci, S. Kavut. DPA resilience of rotation-symmetric S-boxes. In: Proceedings of IWSEC 2014, LNCS, vol. 8639, pp. 146-157, Springer, 2014.

[13] S. Kavut, S. Tutdere. Highly nonlinear (vectorial) Boolean functions that are symmetric under some permutations. Advances in Mathematics of Communications, 14 (1):127-136, 2020.

[14] D. Jakobovic, S. Picek, M. S. R. Martins, M. Wagner. A characterisation of S-box fitness landscapes in cryptography. In: Proceedings of Genetic and Evolutionary Computation Conference – GECCO'19, pp. 285-293, 2019.

[15] D. Jakobovic, S. Picek, M. S. R. Martins, M. Wagner. Toward more efficient heuristic construction of Boolean functions. Applied Soft Computing, vol. 107, 107327, 2021.

[16] W. Millan, L. Burnett, G. Carter, A. Clark, E. Dawson. Evolutionary heuristics for finding cryptographically strong S-boxes. In: International Conference on Information and Communications Security, LNCS, vol. 1726, pp 263-274, Springer, 1999.

[17] J. A. Clark, J. L. Jacob, S. Stepney. The design of S-boxes by simulated annealing. New Generation Computing, 23(3):219-231, 2005.

[18] P. Tesař. A new method for generating high non-linearity s-boxes. Radio Engineerng, 19(1):23-26, 2010.

[19] O. V. Kazymyrov, V. N. Kazymyrova, R. V. Oliynykov. A method for generation of high-nonlinear S-Boxes based on gradient descent. Mat. Vopr. Kriptogr., 5(2):71-78, 2014.

[20] A. Mamadolimov, H. Isa, M. S. Mohamad. Practical Bijective S-box Design, arXiv:1301.4723v1, 2013.

[21] H. Isa, N. Jamil, M. R. Z'aba. S-box construction from non-permutation power functions. In: Proceedings of the 6th International Conference on Security of Information and Networks, pp. 46-53, 2013.

[22] H. Isa, N. Jamil, M. R. Z'aba. Construction of cryptographically strong S-boxes inspired by bee waggle dance. New Generation Computing, 34(3):221-38, 2016.

[23] G. Ivanov, N. Nikolov, S. Nikova. Reversed genetic algorithms for generation of bijective s-boxes with good cryptographic properties. Cryptography and Communications, 8:247-276, 2016.

[24] S. Kavut, S. Baloğlu. Results on symmetric S-boxes constructed by concatenation of RSSBs. Cryptography and Communications, 11:641-660, 2019.

[25] V. Rijmen, P. S. L. M. Barreto, D. L. G. Filho. Rotation symmetry in algebraically generated cryptographic substitution tables. Information Processing Letters, 106:246-250, 2008.

[26] S. Kavut. Results on rotation-symmetric S-boxes. Information Sciences, 201:93-113, 2012.

[27] 3rd Generation Partnership Project, Technical Specification Group Services and System Aspects, 3G Security, Specification of the 3GPP Confidentiality and Integrity Algorithms; Document 2: KASUMI Specification, V.3.1.1, 2001.

[28] M. Bartholomew-Biggs. Chapter 5: The steepest descent method, nonlinear optimization with financial applications. pp. 51-64. Springer, 2005.

[29] L. Goubin, A. Martinelli, M. Walle. Impact of sboxes size upon side channel resistance and block cipher design. In AFRICACRYPT'13, LNCS, vol. 7918, pp. 240-259, Springer, 2013.

[30] B. Aslan, M. T. Sakalli, E. Bulus. Classifying 8-bit to 8-bit S-Boxes based on power mappings from the point of DDT and LAT Distributions. In: Proceedings of Arithmetic of Finite Fields – WAIFI 2008, LNCS, vol. 5130, pp. 123-133, Springer, 2008.

[31] H. Heys, C. M. Adams. A tutorial on linear and differential cryptanalysis. Cryptologia, 26(3):189-221, 2002.

[32] O. Kazymyrov. Methods and tools for analysis of symm etric cryptographic primitives. PhD thesis, The Selmer Center, Department of Informatics, University of Bergen, Norway, 2014.

[33] A. M. Eilertsen, O. Kazymyrov, V. Kazymyrova, M. Storetvedt. A Sage library for analysis of nonlinear binary mapping. In: Pre-proceedings of Central European Conference on Cryptology – CECC'14, pp. 69-78, 2014.

[34] X. M. Zhang and Z. Yheng. GAC – the criterion for global avalanche characteristics of cryptographic functions, Journal for Universal Computer Science, 1(5):316-333, 1995.

[35] M. D. Yücel. Alternative nonlinearity criteria for Boolean functions. Electrical and Electronics Engineering Department, Middle East Technical University, Memorandum No. 2001-1, 2001.

[36] GitHub, URL: https://github.com/Selcuk-kripto/sbox10, (Erişim tarihi: 27, 02, 2022).

Özgeçmişler

Selçuk Kavut, Ankara Üniversitesi Elektronik Mühendisliği Bölümü'nden lisans derecesini 1998 yılında, Orta Doğu Teknik Üniversitesi Fen Bilimleri Enstitüsü Elektrik ve Elektronik Mühendisliği Anabilim Dalı'ndan yüksek lisans ve doktora derecelerini sırasıyla 2002 ve 2008 yıllarında almıştır. 2009-2014 yılları arasında Gebze Yüksek Teknoloji Enstitüsü'nde Öğr. Gör. Dr. olarak çalıştıktan sonra Balıkesir Üniversitesi'ne geçmiş olup, halen Bilgisayar Mühendisliği Bölümü'nde Doç. Dr. olarak çalışmaktadır. Çalışma alanları kriptoloji ve kodlama teorisi üzerinedir.