Süleyman Demirel Üniversitesi
Fen Bilimleri Enstitüsü Dergisi
Cilt 22, Sayı 2, 803-810, 2018

Süleyman Demirel University
Journal of Natural and Applied Sciences
Volume 22, Issue 2, 803-810, 2018

DOI: 10.19113/sdufbed.64033

Düşük Saydamlık Derecesine Sahip Küçük Büyüklükte S-kutuları

Selçuk KAVUT[*1]

[1]Balıkesir Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 10145, Balıkesir

(Alınış / Received: 01.02.2017, Kabul / Accepted: 09.10.2017, Online Yayınlanma / Published Online: 20.11.2017)

Anahtar Kelimeler
Farksal güç analizi (FGA),
S-kutuları,
Saydamlık derecesi (SD)

Özet: Farksal güç analizine (FGA) kendiliğinden dayanıklı S-kutularının inşası kriptografide önemli bir problemdir. Prouff tarafından 2004'te ortaya konulduğundan itibaren bir S-kutusunun saydamlık derecesi (SD), FGA karşısında önemli bir gösterge olarak yaygın biçimde kullanılmaktadır. Bu çalışmada ilk olarak, bir S-kutusunun SD'sini değiştirmeyen bazı afin dönüşümler sağlanmakta ve bu sonuca dayanarak afin eşdeğer olan bütün S-kutuları arasından en düşük SD'yi başaran S-kutularını elde etmek için verimli bir tüketici arama stratejisi verilmektedir. İyi bilinen yapıların boyutu ≤ 6 olan durumları için arama stratejimiz başarıyla uygulanmış ve sonuçlar sunulmuştur. İkinci olarak, boyutun 6 olduğu durum için en dik iniş prensibine dayalı özyineli arama algoritması gerçekleştirilmiş ve bilinen yapılardan daha iyi SD değerleri sağlarken aynı zamanda yüksek doğrusal olmama ve düşük farksal birbiçimliliğe sahip S-kutuları üretilmiştir.

Small Size S-boxes with Low Transparency Order

Keywords
Differential power analysis (DPA),
S-boxes,
Transparency order (TO)

Abstract: Constructing S-boxes that are inherently resistant against the differential power analysis (DPA) is an important problem in cryptography. Since it was introduced by Prouff in 2004, the transparency order (TO) of an S-box has been commonly used as a significant indicator against the DPA. In this work, we fist provide some affine transformations under which the TO of an S-box remains the same, and based on this result we give an efficient exhaustive search strategy to attain the S-boxes achieving the lowest TO among all the S-boxes which are affine equivalent. For the well-known constructions in dimensions ≤ 6, we apply our search strategy successfully and present the results. Secondly, for dimension 6 we perform the steepest-descent-like iterative search algorithm and generate the S-boxes which, while providing better TOs than those of the known constructions, have high nonlineariy and low differential uniformity.

1. Giriş

Kriptografik cihazlarda gömülü simetrik kriptosistemler güç tüketimi, yürütme zamanlaması, veya elektromanyetik emisyon gibi yan kanal bilgisi sızdırırlar. Bu bilgiden faydalanarak böyle bir kriptosistem tarafından kullanılan gizli anahtarı elde etmek için yan kanal analizi (YKA) gerçekleştirilebilir. Bu tür bir kriptanaliz birçok durumda çok büyük sayıda açık metin ve şifreli metin çifti gerektiren doğrusal veya farksal kriptanalizden çok daha fazla verimlidir. Doğrusal veya farksal kriptanalizin bu gereksinimi uygulanmalarını pratikte elverişsiz kılarken, yan kanallardan elde edilen bilgiye bağlı olarak birkaç bin açık metin ve şifreli metin çifti ile YKA saldırısı yapılabilir. En güçlü YKA tekniklerinden birisi farksal güç analizidir (FGA). FGA karşısında günümüze dek kapı seviyesinde veya algoritmik seviyede maskeleme, rasgele zaman gecikmeleri veya işlevsiz işlemler ekleme ve YKA'ya dayanıklı mantık stilleri tasarlama gibi önlemler geliştirilmiştir. Bununla birlikte, bu önlemler bir taraftan güç tüketimi, donanım alanı, veya işleme zamanında önemli bir artışa neden olurken, diğer taraftan donanım implementasyonlarında oluşan kısa süreli hatalardan dolayı FGA saldırılarına karşı zayıf kalabilmektedirler. [1]'de önerildiği gibi, bir kriptosistemi FGA saldırıları karşısında dayanıklı kılmak için daha verimli bir yöntem uygun S-kutularının tasarlanması ile başarılabilir. [1]'de, bir S-kutusunun FGA dayanıklılığı saydamlık derecesi (SD) kavramı ortaya konularak nicelleştirilmiş ve bu ölçütün geçerliliği SASEBO-GII kartı [2–4] ve ATmega163 akıllı kart [5, 6] gibi kriptografik cihazlar üzerinde uygulanan birçok implementasyon ile doğrulanmıştır.

AES algoritmasında S-kutusu olarak kullanılan (sonlu cisim $\mathbb{F}_{2^8}$ üzerinde) ters fonksiyon dahil olmak üzere yüksek doğrusal olmama değerine sahip bazı S-kutularının SD'lerinin kriptografik açıdan oldukça kötü oldukları gösterilmiştir [7]. [3]'te, AES S-kutusu ile karşılaştırıldığında doğrusal olmama ve farksal birbiçimlilik değerleri daha

* İlgili yazar: skavut@balikesir.edu.tr

kötü olmasına karşın SD'si daha iyi olan S-kutuları kısıtlı bir rasgele arama gerçekleştirilerek bulunmuştur. Döngüsel simetrik S-kutuları (DSSK) sınıfına bakıldığında ise doğrusal olmama, farksal birbiçimlilik ve SD arasında daha iyi bir denge elde edilmiştir [4]. Bahsedilen bu sonuçlar, en dik iniş prensibine dayalı özyineli arama [8] ve genetik [5] algoritmalar gibi sezgisel arama yöntemleri kullanılarak dikkate değer bir şekilde geliştirilmiştir. Bu aramaların tümü boyutu 8 olan S-kutuları için yürütüldüğünden karşılık gelen arama uzayları çok büyüktür (bütün arama uzayının büyüklüğü $\approx 2^{1684}$, DSSK sınıfı için arama uzayının büyüklüğü $\approx 2^{208.3}$). Bu nedenle, elde edilen S-kutularının doğrusal olmama ve farksal birbiçimlilik özellikleri AES S-kutusununki kadar iyi değildir.

Yakın zamanda gerçekleştirilen bazı çalışmalarda [6, 8, 9], bir S-kutusunun FGA dayanıklılığının doğrusal olmama, farksal birbiçimlilik ve cebirsel gibi kriptografik özellikleri değişmeden afin dönüşümlerle iyileştirilebileceği tespit edilmiştir. Bir S-kutusunun uzaklık profili FGA dayanıklılığının göstergesi olarak tanımlandığında, bütün (genişletilmiş) afin eşdeğer S-kutuları arasında ikinci en düşük uzaklığa sahip (mutlak gösterge değeri 8 ve boyutu 4 olan) optimal S-kutularının [10], blok şifre PRINCE [11] için öngörülen 8 S-kutusu yerine kullanılmaları önerilmiştir [9]. Bununla birlikte, bu S-kutuları SD değerleri bakımından en iyi değillerdir; rasgele arama ve genetik algoritmalar kullanılarak, optimal S-kutularının SD'lerinin bazı afin dönüşümler altında 3.2 ile 3.73 arasında değiştiği gözlenmiştir [6].

Bu makalede, öncelikle SD'nin değişebileceği afin dönüşümler tespit edilmiş ve sonrasında verilen bir S-kutusu için bu dönüşümler uygulanarak iyi SD değerlerine sahip S-kutuları elde edilmiştir. Bu arama stratejisi kullanılarak, sırasıyla boyut 4'te optimal S-kutuları ve boyut 5'te AB (Almost Bent - Hemen Hemen Bükük) permütasyonlar için en iyi SD değerleri 3.2 ve 4.597 olarak bulunmuştur. Boyut 6 durumu için, tespit edildiği 2009 yılından itibaren tek karşı örnek olarak bilinen APN (Almost Perfect Nonlinear - Hemen Hemen Kusursuz Doğrusal Olmayan) S-kutusu [12] ile birlikte Tablo 4'te verilen (n'nin çift değerleri için) literatürde bulunan en yüksek doğrusal olmama değerine ($2^{n-1}-2^{\frac{n}{2}}$) sahip ve farksal birbiçimliliği 4 olan yapılar ele alınmış ve karşılık gelen SD değer aralıkları arama yöntemimiz vasıtasıyla elde edilmiştir. Ayrıca, 6×6 bijektif DSSK'lar arasında en iyi doğrusal olmama ve farksal birbiçimlilik değerlerine sahip olan S-kutularına [13] afin eşdeğer olanların SD değerleri belirlenmiştir. Son olarak, boyut 6'da literatürdeki yapılar kullanılarak elde edilen SD değerlerini iyileştirmek için bütün arama uzayında ($\approx 2^{296}$) hem rasgele hem de sezgisel arama algoritmaları gerçekleştirilmiş ve hem doğrusal olmama, farksal birbiçimlilik ve cebirsel derece gibi kriptografik özellikler bakımından güçlü hem de SD değeri düşük olan S-kutuları bulunmuştur. Bu çalışmada, daha önce [14]'de sunduğumuz sonuçlar gözden geçirilerek boyut 6'da bulunan en iyi SD değerine sahip bir (döngüsel simetrik) S-kutusu sunulmuş ve *Sezgisel ve Rasgele Arama* başlığı altında yeni sonuçlar eklenmiştir. Elde edilen yeni sonuçlar, doğrusal olmama ve farksal birbiçimlilik ile SD değerleri arasında bir ödünleşim olduğunu ve uygun bir maliyet fonksiyonu seçimi ile en dik iniş prensibine dayalı özyineli arama algoritmasının [14]'te başarılan (doğrusal olmama ve farksal birbiçimlilik değerlerine göreli olarak yakın olmakla birlikte) SD değerlerinden daha iyi SD değerlerine sahip S-kutularını üretebildiğini göstermiştir.

Boyutu n olan bir S-kutusunun SD'sini τ ile gösterelim. Çalışmamızda, normalize edilmiş SD, $\overline{\tau}=\frac{\tau}{n}$ ile gösterilmektedir. SD'nin özgün tanımda [1], S-kutusunun dengeli koordinat fonksiyonlarından oluştuğu varsayılmaktadır. Ayrıca, bükük bir fonksiyonun [15] SD'sini ölçmenin mümkün olmadığı gösterilmiştir [16]. Bu nedenle, τ için üst sınır n'nin bükük fonksiyonlar tarafından sağlandığını düşünmek doğru değildir. S-kutuları ve DSSK'ların kriptografik özellikleri ile ilgili temel tanımlar örneğin [8]'de bulunabilir.

2. Afin Eşdeğer S-kutularının Saydamlık Dereceleri

U,V singüler olmayan ikili matrisler ve $u,v\in\{0,1\}^n$ olmak üzere, $S(x)$ ve $T(x)$ afin eşdeğer olan iki S-kutusu olsun:

$$S(x)=T(xU\oplus u)V\oplus v,\quad \forall\, x\in\{0,1\}^n.$$

[6]'da $S(x)$ ve $T(x)$'in farklı SD'lere sahip olabileceği gösterilmiştir. Daha sonra [6]'dan bağımsız olarak, eğer V birim matris ise $S(x)$ ve $T(x)$'in aynı SD'ye sahip oldukları bulunmuştur [8]. Bu sonuç vasıtasıyla, boyutu 6 olan DSSK'lar arasında doğrusal olmama değeri 24 ve farksal birbiçimliliği 4 olanların SD değerlerinin 5.238 ile 5.905 arasında değiştiği belirlenmiştir [8]. $S(x)$'in özilinti fonksiyonunu aşağıdaki gibi tanımlayalım:

$$r_S(a,v)=\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot(S(x)\oplus S(x\oplus a))}.$$

SD'nin değişmezliği

$$\left|\sum_{\substack{v\in\mathbb{F}_2^n,\\ wt(v)=1}} r_S(a,v)\right|\leq 2^{n+1},\quad \forall\, a\in\mathbb{F}_2^{n*}.$$

eşitsizliğini sağlayan S-kutuları için [17]'de çalışılmış ve bu koşul altında eğer U ve V birer permütasyon matrisi ise $S(x)$ ve $T(x)$'in SD'lerinin aynı olduğu gösterilmiştir.

$n\times n$ büyüklüğünde bir S-kutusu $S(x)$ için afin dönüşümlerin sayısı aşağıda verilen formül ile bulunabilir ve bu sayı küçük büyüklükteki S-kutuları için bile oldukça yüksektir:

$$2^{2n}\times\left(\prod_{i=0}^{n-1}(2^n-2^i)\right)^2.$$

A,B singüler olmayan ikili matrisler ve $d,e\in\{0,1\}^n$ olmak üzere $T(x)=S(xA\oplus d)B\oplus e$ S-kutusu ele alındığında, $T(x)$'in SD'sinin $S(xA\oplus d)\oplus e$ ile verilen S-kutusunun

Tablo 1. $n\times n$ büyüklüğünde bir S-kutusunun SD'sini değiştirmeyen afin dönüşümlerin n=4,...,8 için sayıları.

n	4	5	6	7	8
#	840 $\approx 2^{9.71}$	83328 $\approx 2^{16.35}$	27998208 $\approx 2^{24.74}$	32509919232 $\approx 2^{34.92}$	132640470466560 $\approx 2^{46.91}$

Tablo 2. Boyut 4'te optimal S-kutularının SD'leri.

Optimal S-kutularının [10] Temsilcileri	Mutlak Gösterge	Derece	$\tau_{\min}(\overline{\tau}_{\min})$	$\tau_{\max}(\overline{\tau}_{\max})$
G_{12}	8	3	3.400 (0.850)	3.667 (0.917)
G_4, G_5, G_7				3.733 (0.933)
G_3 (ters fonksiyon)			3.467 (0.867)	
G_6, G_{11}, G_{13}			3.333 (0.833)	
$G_2, G_9, G_{10}, G_{14}, G_{15}$	16		3.267 (0.817)	
G_0, G_1, G_8			3.200 (0.800)	

SD'si ile aynı olduğu gösterilmiştir [8]. Bu nedenle, herhangi bir S-kutusu için bütün afin eşdeğer S-kutuları arasında en düşük SD'ye sahip S-kutularını elde etmek için gerekli olan afin dönüşümlerin sayısı $\prod_{i=0}^{n-1}(2^n-2^i)$ ile bulunan sayıya indirgenmiş olur. Bununla birlikte, aşağıda verilen önerme ile gösterildiği gibi, bir S-kutusunun SD'si B matrisinin herhangi bir sütun permütasyonu ile de değişmez. Bu sonuç, bahsedilen afin dönüşümlerin sayısını ayrıca $\frac{1}{n!}$ çarpanı ile azaltır.

Önerme 2.1. *B ve C singüler olmayan matrisler olmak üzere, τ_B ve τ_C sırasıyla $S(x)B$ ve $S(x)C$ ile verilen S-kutularının SD'leri olsun. Eğer C matrisi B'nin bir sütün permütasyonu ise, o zaman τ_B=τ_C olur.*

İspat. $b_i \in \mathbb{F}_2^n$, B'nin i'inci sütun vektörü olmak üzere, B=$[b_0,\ldots,b_{n-1}]$ ve B'nin bir sütun permütasyonu C=$[b_{i_0},\ldots,b_{i_{n-1}}]$ olsun. Bu durumda, üstsimge T ile transpozu ve τ ile SD'nin sadeleştirilmiş versiyonunu [16] gösterirsek, aşağıdaki çıkarımı elde ederiz:

$$\begin{aligned}
\tau_C &= n-\frac{1}{2^{2n}-2^n}\sum_{a\in\mathbb{F}_2^{n^*}}\left|\sum_{\substack{v\in\mathbb{F}_2^n,\\ wt(v)=1}}\sum_{x\in\mathbb{F}_2^n}(-1)^{v\cdot\left(S(x)C\oplus S(x\oplus a)C\right)}\right| \\
&= n-\frac{1}{2^{2n}-2^n}\sum_{a\in\mathbb{F}_2^{n^*}}\left|\sum_{\substack{v\in\mathbb{F}_2^n,\\ wt(v)=1}}\sum_{x\in\mathbb{F}_2^n}(-1)^{vC^T\cdot\left(S(x)\oplus S(x\oplus a)\right)}\right| \\
&= n-\frac{1}{2^{2n}-2^n}\sum_{a\in\mathbb{F}_2^{n^*}}\left|\sum_{k=0}^{n-1}\sum_{x\in\mathbb{F}_2^n}(-1)^{b_{i_k}\cdot\left(S(x)\oplus S(x\oplus a)\right)}\right| \\
&= n-\frac{1}{2^{2n}-2^n}\sum_{a\in\mathbb{F}_2^{n^*}}\left|\sum_{\substack{v\in\mathbb{F}_2^n,\\ wt(v)=1}}\sum_{x\in\mathbb{F}_2^n}(-1)^{vB^T\cdot\left(S(x)\oplus S(x\oplus a)\right)}\right| \\
&= \tau_B.
\end{aligned}$$

□

Böylelikle, SD'yi değiştirmeyen afin dönüşümlerin (veya sütun permütasyonuna göre birbirinden farklı olan ve singüler olmayan ikili matrislerin) sayısını $\frac{\prod_{i=0}^{n-1}(2^n-2^i)}{n!}$ olarak elde ederiz. Bu sayı n=4,...,8 için Tablo 1'de verilmektedir. Örneğin, boyut 6'da bir S-kutusu için bütün afin eşdeğer S-kutuları içinde en düşük SD'ye sahip olanları bulmak için gerçekleştirilen bir kaba kuvvet araması $\approx 2^{80.46}$ S-kutusunun SD'sini hesaplamayı gerektirirken, arama metodumuz bu sayıyı $\approx 2^{24.74}$'e düşürmektedir (Tablo 1'e bkz.). Aşağıda, bu dönüşümler kullanılarak iyi bilinen yapılar için afin eşdeğer S-kutularının SD'leri bulunmaktadır. Ayrıca, boyut 6'da sezgisel bir arama gerçekleştirilerek literatürdeki yapıların SD'leri iyileştirilmiştir.

3. Literatürdeki Yapıların Saydamlık Dereceleri

3.1. Boyut 3 ve 4'te S-kutuları

Boyut 3'te afin eşdeğer olmayan sadece 4 S-kutusu bulunmaktadır [18]. Bunların arasında, sadece ($\mathbb{F}_{2^3}$ üzerinde) ters fonksiyona karşılık gelen S-kutusu sıfırdan farklı doğrusal olmama değerine sahip olduğu için blok şifre tasarımında kullanılabilmektedir [19, 20]. Bu S-kutusunun SD'si 2.571 ($\overline{\tau}=0.857$) olarak bulunmuş ve boyut 3'teki afin dönüşümler altında değişmediği görülmüştür.

[10]'da, boyut 4 için doğrusal olmama ve farksal birbiçimlilik değerleri en iyi olan permütasyonlar optimal olarak nitelendirilmiş ve $G_0,\ldots,G_{15}$ ([10, Tablo 6]) ile temsil edilen, birbiri ile afin eşdeğer olmayan 16 S-kutusunun olduğu bulunmuştur. Bu temsilcilerin herbiri için, 840 afin eşdeğer S-kutusunun (Tablo 1'e bkz.) sağladığı en yüksek ve en düşük SD değerleri Tablo 2'te sunulmuştur. [6]'da, SD değeri 3.2 olan optimal S-kutuları bazı afin dönüşümlerin rasgele üretilmesiyle elde edilmiştir. Tablo 2'den görüldüğü üzere, bu değer karşılık gelen afin dönüşümler uygulandıktan sonra bütün optimal S-kutuları arasında G_0, G_1 ve G_8 temsilcileri tarafından başarılan en düşük SD değeridir. Tablo 2'de, G_3 temsilcisi $\mathbb{F}_{2^4}$ üzerinde ters fonksiyona karşılık gelmektedir ve en düşük SD değeri 3.467 olarak bulunmuştur. Bu değerin [7]'de 3.269 olarak

Tablo 3. Boyut 5'te AB permütasyonların SD'leri.

AB permütasyonların Temsilcileri		Mutlak Gösterge	Derece	$\tau_{\min}(\overline{\tau}_{\min})$	$\tau_{\max}(\overline{\tau}_{\max})$
Gold, Kasami	α^3	32	2	4.839 (0.968)	4.839 (0.968)
Gold, Niho	α^5				
Welch	α^7	8	3	4.645 (0.929)	
Kasami	α^{13}			4.629 (0.926)	

Tablo 4. Çift boyut n için, farksal birbiçimliliği 4 ve doğrusal olmama değeri $2^{n-1}-2^{\frac{n}{2}}$ olan permütasyonlar.

Fonksiyon	Koşul	Referans
x^{2^n-2}	n çift	[24]
$x^{2^{\frac{n}{2}}+2^{\frac{n}{4}}+1}$	$n \equiv 4 \bmod 8$	[25]
$\sum_{i=0}^{2^n-3} x^i$	$n \equiv 2 \bmod 4$	[26, 27]
x^{2^i+1}	ebob(i,n)=2, $n \equiv 2 \bmod 4$	[24, 28]
$x^{2^{2i}-2^i+1}$	ebob(i,n)=2, $n \equiv 2 \bmod 4$	[29]
$\alpha x^{2^i+1}+\alpha^{2^{\frac{n}{3}}} x^{2^{-\frac{n}{3}}+2^{\frac{n}{3}+i}}$	$\alpha : \mathbb{F}_{2^n}$'nin bir primitif elemanı, $9 \mid (n+3i)$, ebob(i,n)=2, $n \equiv 6 \bmod 12$ ve $9 \nmid n$	[30]
$\left(F(x)+F(x)^{2^i}\right)\Big\vert_H$	$H=\{x \in \mathbb{F}_{2^{n+1}} \mid tr_{n+1}(x)=0\}$, $F(x)=x^{\frac{1}{2^i+1}}+tr_{(n+1,3)}(x+x^{2^{2s}})$, $s \equiv i \bmod 3$, ebob$(i,n+1)$=1, $n \equiv 2 \bmod 6$	[31]
$\left(\beta x^{\frac{2^i}{2^i+1}}+\beta^{2^i} x^{\frac{1}{2^i+1}}\right)\Big\vert_{H_\beta}$	$\beta \in \mathbb{F}^*_{2^{n+1}}$, $H_\beta=\{\beta x^{2^i}+\beta^{2^i} x \mid x \in \mathbb{F}_{2^{n+1}}\}$, ebob$(i,n+1)$=1, n çift ve ≥ 4	
$\left(\beta x^{\frac{2^i}{2^i+1}}+\beta^{2^i} x^{\frac{1}{2^i+1}}+x\right)\Big\vert_{H_\beta}$		

Tablo 5. Boyut 6'daki APN permütasyonun [12] ve Tablo 4'te verilen yapılardan üretilen S-kutularının SD'leri.

Fonksiyon*	Mutlak Gösterge	Derece	$\tau_{\min}(\overline{\tau}_{\min})$	$\tau_{\max}(\overline{\tau}_{\max})$
x^{62}	16	5	5.694 (0.949)	5.802 (0.967)
$x^{62}+(x+x^2)^{63}+1$	16	5	5.667 (0.945)	5.810 (0.968)
x^5	64	2	5.714 (0.952)	5.905 (0.984)
x^{13}	32	3	5.524 (0.921)	5.714 (0.952)
$\left(\beta x^{\frac{2^i}{2^i+1}}+\beta^{2^i} x^{\frac{1}{2^i+1}}\right)\Big\vert_{H_\beta}$	32	4	5.567 (0.928)	5.829 (0.972)
$\left[\left(\beta x^{\frac{2^i}{2^i+1}}+\beta^{2^i} x^{\frac{1}{2^i+1}}\right)\Big\vert_{H_\beta}\right]^{-1}$	32	3	5.595 (0.933)	5.841 (0.974)
$\left(\beta x^{\frac{2^i}{2^i+1}}+\beta^{2^i} x^{\frac{1}{2^i+1}}+x\right)\Big\vert_{H_\beta}$	32	4	5.563 (0.927)	5.829 (0.972)
$\left[\left(\beta x^{\frac{2^i}{2^i+1}}+\beta^{2^i} x^{\frac{1}{2^i+1}}+x\right)\Big\vert_{H_\beta}\right]^{-1}$	32	4	5.560 (0.927)	5.829 (0.972)
APN permütasyon [12]	64	4	5.639 (0.940)	5.905 (0.984)

* $[F(x)]^{-1}$: $F(x)$'in bileşimsel tersini göstermekte ve $\beta \in \mathbb{F}^*_{2^7}$, $i=1,\ldots,6$ olmak üzere $H=\{x \in \mathbb{F}_{2^7} \mid tr_7(x)=0\}$ ve $H_\beta=\{\beta x^{2^i}+\beta^{2^i} x \mid x \in \mathbb{F}_{2^7}\}$ ile verilmektedir.

Tablo 6. DSSK sınıfında doğrusal olmama değeri 24 ve farksal birbiçimliliği 4 olan permütasyonlardan elde edilen SD değerleri.

Mutlak Gösterge	Derece	DSSK'ların SD'leri		DSSK sayısı	Eleme sonrası DSSK sayısı	Afin Eşdeğer S-kutularının SD'leri	
		$\tau_{\min}(\overline{\tau}_{\min})$	$\tau_{\max}(\overline{\tau}_{\max})$			$\tau_{\min}(\overline{\tau}_{\min})$	$\tau_{\max}(\overline{\tau}_{\max})$
16	5	*5.714* (*0.952*)	5.810 (0.968)	128×12	2	*5.667* (*0.945*)	5.810 (0.968)
24	4	5.452 (0.909)	5.905 (0.984)	11776×12	184	5.452 (0.909)	5.905 (0.984)
32	3	5.333 (0.889)	5.810 (0.968)	640×12	10	5.333 (0.889)	5.833 (0.972)
32	4	5.333 (0.889)	5.905 (0.984)	411648×12	6432	5.333 (0.889)	5.905 (0.984)
40	4	5.380 (0.897)	5.905 (0.984)	1140800×12	17825	5.380 (0.897)	5.905 (0.984)
40	5	*5.619* (*0.937*)	5.762 (0.960)	128×12	2	*5.488* (*0.915*)	5.853 (0.976)
48	4	*5.380* (*0.897*)	5.905 (0.984)	233216×12	3644	*5.369* (*0.895*)	5.905 (0.984)
64	2	5.714 (0.952)	5.905 (0.984)	192×12	4	5.714 (0.952)	5.905 (0.984)
64	3	*5.380* (*0.897*)	5.905 (0.984)	10432×12	172	*5.254* (*0.876*)	5.905 (0.984)
64	4	**5.238** (**0.873**)	5.905 (0.984)	523328×12	8247	**5.238** (**0.873**)	5.905 (0.984)

verilen alt sınır değerinden yüksek olduğuna dikkat ediniz. Bununla birlikte, hem ters fonksiyon ile aynı doğrusal olmama, farksal birbiçimlilik ve cebirsel dereceye sahip, hem de SD değeri alt sınırdan daha düşük olan optimal S-kutularının var olduğu Tablo 2'den görülmektedir. Bölüm 2.3'te, farksal birbiçimliliği 4 olan ve literatürde bilinen en yüksek doğrusal olmama değeri 24'e sahip 6×6 DSSK'lar için de benzer sonuçlar elde edilmektedir.

3.2. Boyut 5'te S-kutuları

Burada, boyut 5'te permütasyon olan AB S-kutularının SD'lerini ele alınmaktadır. Bu S-kutularından afin eşdeğer olmayan sadece 4 tane bulunduğu ve Tablo 3'te listelendiği gibi herbirinin $\mathbb{F}_{2^5}$ üzerinde bir üstel fonksiyona karşılık geldiği gösterilmiştir [21]. $\alpha \to \alpha^5$ ve $\alpha \to \alpha^3$ ile verilen (aynı zamanda sırasıyla Niho ve Kasami fonksiyonlarına da karşılık gelen) Gold fonksiyonlarının afin dönüşümler altında aynı kaldığı görülmektedir. Diğer bir ifadeyle, 4.839 olarak bulunan SD değeri afin dönüşümler altında değişmezdir. Bununla birlikte, Welch fonksiyonundan üretilen afin eşdeğer S-kutuları arasındaki en düşük SD (4.645), Gold fonksiyonunun SD'sinden daha iyidir ve boyut 5'te bütün AB permütasyonları kullanılarak bulunan en düşük SD (4.629), $\alpha \to \alpha^{13}$ ile verilen diğer Kasami fonksiyonundan elde edilmektedir. Benzer şekilde, boyut 7'de literatürdeki AB permütasyonlarını ele aldığımızda, en düşük SD değeri $\alpha \to \alpha^{57}$ ile verilen Kasami fonksiyonundan 6.764 olarak elde edilmiştir.

3.3. Boyut 6'da S-kutuları

Çift boyutta APN permütasyonların varlığı, boyut 6'da bir karşı örnek 2009'da bulunana [12] dek bilinmemekteydi. Bu karşı örnek halen çift boyutta bilinen tek APN permütasyondur. Bu nedenle, bu permütasyon ile birlikte Tablo 4'te listelediğimiz farksal birbiçimliliği 4 olan ve en yüksek doğrusal olmama değeri 24'e sahip permütasyonlar da ele alınarak, bütün bu yapılardan afin dönüşümler ile elde edilen SD değerleri Tablo 5'te sunulmuştur. Bahsedilen APN permütasyondan elde edilen en düşük SD değeri 5.639 iken, diğer SD'ler arasındaki en iyi değerin 5.524 olduğu görülmektedir. Bununla birlikte, en iyi SD'nin elde edildiği $x \to x^{13}$ fonksiyonu düşük cebirsel dereceye sahip olduğundan daha yüksek mertebeden farksal ataklara karşı dayanıklı değildir. Bu yüzden, kuadratik ve kübik fonksiyonların SD'lerini göz ardı ettiğimizde, cebirsel derecesi ≥ 4 olan yapılar arasında elde edilen en iyi SD'nin 5.560 olduğu görülmektedir.

Tablo 5'te, farksal birbiçimliliği 4 olan ve en yüksek doğrusal olmama değeri 24'e sahip sadece birkaç yapı mevcuttur. Bununla birlikte, [13]'te gösterildiği gibi, boyut 6'daki DSSK sınıfında bu iki kriptografik özelliği sağlayan 2332288×12 permütasyon bulunmaktadır. [8]'de bu DSSK'lardan elde edilen en iyi SD'nin 5.238 olduğu bulunmuştur; bu değer Tablo 5'te elde edilen en düşük SD'den fark edilir derecede daha iyidir. Burada, bahsedilen DSSK'lardan afin dönüşümler ile başarılan en düşük SD'ler bulunmaktadır. Euler'in totient fonksiyonu $\varphi(n)$ ve satırların permütasyonuna göre farklı olan $\mathbb{F}_2^n$ üzerindeki $n\times n$ büyüklüğünde singüler olmayan dolanır matrislerin sayısı N olmak üzere, boyut n'de verilen bir DSSK için döngüsel simetriklik özelliğini koruyan afin dönüşümlerin sayısının $4N^2n\varphi(n)$ olduğu bilinmektedir [13]. İlk olarak, bu afin dönüşümler vasıtasıyla, 2332288×12 DSSK arasında afin eşdeğer olanlar elenmiş ve herbiri karşılık gelen afin eşdeğer DSSK'lar kümesinin temsilcisi olan 36522 DSSK elde edilmiştir. Daha sonra, 36522 DSSK'nın herbirinin sağladığı en düşük SD değerini bulmak için, Tablo 1'de toplam sayısı $\approx 2^{24.74}$ olarak verilen afin dönüşümlerin tümü kullanılmış ve karşılık gelen SD değerleri hesaplanmıştır. Tablo 6'da sonuçlar listelenmiş ve [8]'de elde edilenlerle karşılaştırılmıştır. En düşük 10 SD'den (italik gösterilen) 4 tanesinin iyileştirildiği ve (koyu gösterilen) en iyi SD'nin afin dönüşümlerle değişmediği gözlenmektedir.

Tablo 6'da görülen en düşük SD değerine sahip bir DSSK aşağıda verilmektedir:

(0, 10, 20, 7, 40, 60, 14, 38, 17, 27, 57, 1, 28, 62, 13, 44, 34, 15, 54, 47, 51, 21, 2, 6, 56, 8, 61, 9, 26, 24, 25, 29, 5, 35, 30, 19, 45,

32, 31, 22, 39, 55, 42, 3, 4, 36, 12, 46, 49, 41, 16, 11, 59, 33, 18, 23, 52, 37, 48, 43, 50, 53, 58, 63).

Bir DSSK donanım veya yazılımda, bit dilimlime tekniği ve koordinat fonksiyonları arasındaki döngüsel simetriklik özelliğinden faydalanarak verimli bir şekilde gerçekleştirilebilir [22, 23]. Bunun yanı sıra, sadece yörünge temsilcilerinin kullanılmasıyla gerçekleştirilmesi de mümkündür (verimli bir FPGA implementasyonu için [4]'e bkz.). Bununla birlikte, bir S-kutusunun SD'si implementasyon metodundan bağımsız olarak elde edilmesine rağmen, FGA dayanıklılığı bundan etkilenebilmektedir. Örneğin, [4]'de bir DSSK'nın verimli bir gerçekleştirmesinin, o DSSK'yı kullanan AES algoritmasının son turundaki anahtarı açığa çıkarmak için gerekli olan güç ölçümlerinin sayısını aramalı tablo olarak gerçekleştirmesi ile karşılaştırıldığında artırabileceği gösterilmiştir.

4. Sezgisel ve Rasgele Arama

Boyut 6'da rasgele üretilen yaklaşık 3000000 S-kutusu içinden doğrusal olmama değeri 18'den yüksek ve farksal birbiçimliliği 8'den düşük olanlar ele alınmış ve bunlarından arasından en düşük SD'ye sahip olan S-kutularının kriptografik özellikleri Tablo 7'de sunulmuştur. Rasgele arama sonucunda doğrusal olmama değeri 20'den yüksek veya farksal birbiçimlilik değeri 6'dan düşük olan bir S-kutusuna rastlanılmamıştır. Tablo 7'de rasgele arama ile elde edilen en iyi SD değerlerinin Tablo 5'te verilen yapılar için bulunan değerlere yakın olduğu, bununla birlikte DSSK'lar için Tablo 6'da bulunan en iyi değerden oldukça kötü olduğu görülmektedir. Bu sonuçları iyileştirmek için, aşağıda bijektif S-kutularının tüm arama uzayında ($\approx 2^{296}$) en dik iniş prensibine dayalı özyineli arama algoritması [8, 13, 32] gerçekleştirilmiştir.

Tablo 7. Sezgisel ve rasgele arama ile bulunan en iyi sonuçlar.

Doğrusal Olmama	Mutlak Gösterge	Farksal Birbiçimlilik	$\tau_S(\overline{\tau}_S)$
Rasgele arama			
20	40	6	5.552 (0.925)
18	40	6	5.520 (0.920)
Sezgisel arama			
22	40	6	5.234 (0.872)
20	32	4	5.381 (0.897)
20	40	6	5.063 (0.844)

[8]'de DSSK'lar için önerilen maliyet fonksiyonu, aşağıda verildiği gibi herhangi bir boyuttaki tüm S-kutuları için genelleştirilerek arama algoritmasında kullanılmıştır:

$$Maliyet(S) = \frac{A}{(2^n-1)(2^{4n}-2^{3n})} \sum_{\substack{u\in\mathbb{F}_2^{n*} \\ \omega\in\mathbb{F}_2^n}} \left(W_S^2(\omega,u)-2^n\right)^2 + \frac{1}{n}\tau_S.$$

Bu fonksiyon, boyutu n olan ve S ile gösterilen herhangi bir S-kutusunun maliyetini hesaplamaktadır. Maliyet fonksiyonunda kullanılan $W_S(\omega,u)$ terimi, S-kutusunun $u\cdot S(x)$ ile belirlenen bileşen fonksiyonunun ω noktasındaki Walsh-Hadamard dönüşümü ve A parametresi ise S-kutusunun doğrusal olmama değeri ile SD'si arasında denge kurmak için kullanılan ayarlama parametresidir. Uyguladığımız arama algoritmasında, deneysel olarak bulunan A parametresi 9 ile 16 arasında değerler almaktadır.

Bir S-kutusunun herhangi bir bileşen fonksiyonu doğrusal olduğunda

$$\sum_{\omega\in\mathbb{F}_2^n} \left(W_S^2(\omega,u)-2^n\right)^2 = 2^{4n}-2^{3n}$$

eşitliği sağlandığından ve sıfırdan farklı bileşenlerin sayısı 2^n-1 olduğundan, $\frac{1}{(2^n-1)(2^{4n}-2^{3n})}$ çarpanı toplam teriminin en yüksek değerini 1'e normalize etmektedir. Benzer şekilde, SD'nin alabileceği en yüksek değerin n olduğu varsayıldığında [1], maliyet fonksiyonundaki $\frac{1}{n}$ çarpanının τ_S'nin en yüksek değerini 1'e normalize ettiği görülmektedir. Bundan dolayı, eşitliğin sağ tarafındaki ilk terim S-kutusunu doğrusal olmama bakımından, diğer terim ise SD bakımından eniyileştirmektedir. Gerçekleştirdiğimiz en dik iniş prensibine dayalı özyineli arama algoritmasının yapay kodu aşağıda verilmektedir.

En dik iniş prensibine dayalı özyineli arama algoritması.

Girdi: Rasgele üretilen S-kutusu S_r, yineleme sayısı N

$S \leftarrow S_r$
for $i \in \{0,1,\ldots,N-1\}$ **do**
  $K \leftarrow S$'nin komşuluğundaki tüm S-kutuları
  $j \leftarrow 0$
  for $S_K \in K$ **do**
    $M[j] \leftarrow Maliyet(S_K)$
    $j \leftarrow j+1$
  $M_{\min} \leftarrow M$ dizisindeki en düşük değer
  $S_{\min} \leftarrow K$ içerisinde karşılık gelen S_K
  while $S_{\min} \in STOK$ **do**
    M dizisinden $M_{\min}$ değerini çıkar
    $M_{\min} \leftarrow M$ dizisindeki en düşük değer
    $S_{\min} \leftarrow K$ içerisinde karşılık gelen S_K
  $STOK[i] \leftarrow S_{\min}$
  $S \leftarrow S_{\min}$

Çıktı: Özyineleme çıkışlarının kaydedildiği $STOK$ dizisi

Algoritmada görüldüğü gibi, en dik iniş prensibine dayalı arama algoritması rasgele üretilen bir S-kutusu (S_r) ile başlamakta ve N yinelemeden sonra durmaktadır. Yineleme çıkışları algoritma çıktısı olarak $STOK$ dizisinde kaydedilmektedir. S'nin bir komşusunu, herhangi iki çıkışının birbiri ile yerdeğiştirmiş versiyonu olarak tanımladığımızdan, S'nin olası tüm komşularından oluşan K dizisinde $\binom{64}{2} = 2016$ S-kutusu bulunmaktadır. Algoritmanın parametreleri deneysel olarak belirlenmiş ve ayarlama parametresi A'nın (daha önce bahsedildiği gibi 9 ile 16 arasında) aldığı 8 farklı değerin her biri için arama algoritması 150 kere koşulmuş, her bir koşma için yineleme sayısı N ise 2000 olarak seçilmiştir. Windows 8 Pro işletim sistemi ve Intel(R) Core(TM) i7-3630QM CPU @ 2.40Ghz işlemciye sahip bir bilgisayarda bütün

çekirdekler kullanılarak, verilen parametrelerle arama algoritmasının gerçekleştirilmesi yaklaşık bir gün sürmüştür.

Arama sonucunda elde ettiğimiz (cebirsel derecesi 5 olan) S-kutularının kriptografik özellikleri Tablo 7'de sunulmaktadır. Bu S-kutularının SD'lerinin afin dönüşüm ile iyileşmediği gözlenmiştir. Tabloda verilen en düşük SD değerinin (5.063), bir önceki bölümde elde edilen en iyi SD değerinden (5.238) oldukça düşük olduğu ve karşılık gelen S-kutusunun yüksek cebirsel derecenin yanı sıra nispeten yüksek doğrusal olmama, düşük farksal birbiçimlilik ve mutlak göstergeye sahip olduğu görülmektedir. Bununla birlikte, gerçekleştirdiğimiz arama algoritmasında (*STOK* dizisinde kaydedilen) 2400000 S-kutusu üretilmiş olmasına rağmen, doğrusal olmama değeri 24 olan bir S-kutusuna rastlanılmamış ve farksal birbiçimliliği 4 olan S-kutuları arasında en düşük SD değeri 5.381 olarak bulunmuştur.

Aşağıda, Tablo 7'de elde edilen en düşük SD değerine sahip S-kutusu verilmektedir:

(0, 63, 47, 26, 59, 53, 49, 21, 48, 45, 39, 19, 30, 12, 10, 2, 17, 61, 43, 3, 60, 13, 38, 27, 7, 40, 29, 4, 58, 33, 36, 24, 18, 52, 57, 1, 62, 8, 37, 42, 11, 46, 28, 6, 54, 41, 5, 56, 34, 15, 14, 16, 23, 32, 25, 50, 20, 31, 35, 51, 22, 44, 9, 55).

5. Tartışma ve Sonuç

Bu çalışmada, bir S-kutusunun SD'sinin değişebileceği afin dönüşümler elde edilmiş ve bu sonuç kullanılarak, literatürde bilinen küçük büyüklükteki yapıların (doğrusal olmama değeri 24 ve farksal birbiçimliliği 4 olan) 6×6 DSSK'lar [13] ile birlikte sahip oldukları en iyi SD değerleri bulunmuştur. Doğrusal olmama, farksal birbiçimlilik ve cebirsel derece gibi birçok kriptografik özellik afin dönüşümler altında değişmedinden, afin eşdeğer S-kutuları arasında FGA saldırılarına karşı daha iyi dayanıklılık sağlayan en düşük SD değerine sahip olanlar kriptosistemlerde tercih edilmektedir. Bu S-kutularını verimli bir şekilde elde edilmesini sağlayan arama yöntemimiz bahsedilen amaca katkı sağlamaktadır. Ayrıca, bu yöntemi kullanarak boyut 6 için elde ettiğimiz SD değerleri, bütün S-kutularının oluşturduğu arama uzayında en dik iniş prensibine dayalı özyineli arama algoritmasının gerçekleştirilmesi ile önemli düzeyde iyileştirilmiştir.

Son olarak, özgün tanımında [1] sıfır olduğu varsayılan koordinat fonksiyonları arasındaki çapraz ilinti terimleri de hesaba katılarak, SD'nin farklı bir tanımı yapılmıştır [16]. Ele aldığımız 6×6 DSSK'ların değiştirilmiş SD bakımından değerlendirilmesi ve çapraz ilinti terimlerinin FGA dayanıklılığı üzerindeki etkisinin pratik YKA uygulamalarıyla gösterilmesinin açık bir araştırma problemi olduğu düşünülmektedir.

Kaynakça

[1] Prouff, E. DPA attack and S-boxes. 2005. Fast Software Encryption, February 21-23, Paris, France, LNCS Vol. 3557, 424-441, Springer Berlin Heidelberg.

[2] Mazumdar, B., Mukhopadhyay, D. 2016. Construction of rotation symmetric S-Boxes with high nonlinearity and improved DPA resistivity. IEEE Transactions on Computers, 66(1), 59-72.

[3] Mazumdar, B., Mukhopadhyay, D., Sengupta, I. 2013. Constrained search for a class of good bijective S-boxes with improved DPA resistivity. IEEE Transactions on Information Forensics and Security, 8(12), 2154-2163.

[4] Mazumdar, B., Mukhopadhyay, D., Sengupta, I. 2013. Design and implementation of rotation symmetric S-boxes with high nonlinearity and high DPA resiliency. IEEE International Symposium on Hardware-Oriented Security and Trust (HOST), June 2-3, Austin TX, USA, 87-92.

[5] Picek, S., Ege, B., Batina, L., Jakobovic, D., Chmielewski, Ł., Golub, M. 2014. On Using Genetic Algorithms for Intrinsic Side-channel Resistance: The Case of AES S-box. The First Workshop on Cryptography and Security in Computing Systems – CS2'14, January 20, Vienna, Austria, 13-18.

[6] Picek, S., Ege, B., Papagiannopoulos, K., Batina, L., Jakobović, D. 2014. Optimality and beyond: The case of 4×4 S-boxes. HOST 2014, May 6-7, Arlington VA, USA, 80-83.

[7] Carlet, C. 2005. On highly nonlinear S-boxes and their inability to thwart DPA attacks. INDOCRYPT 2005, December 10-12, Bangalore, India, LNCS Vol. 3797, 49-62, Springer Berlin Heidelberg.

[8] Evci, M. A., Kavut, S. 2014. DPA resilience of rotation-symmetric S-boxes. IWSEC 2014, August 27-29, Hirosaki, Japan, LNCS Vol. 8639, 146-157, Springer International Publishing.

[9] Sarkar, S., Maitra, S., Chakraborty, K. 2014. Differential power analysis in Hamming weight model: How to choose among (extended) affine equivalent S-boxes. INDOCRYPT 2014, December 14-17, New Delhi, India, LNCS Vol. 8885, 360-373, Springer International Publishing.

[10] Leander, G., Poschmann, A. 2007. On the classification of 4 Bit S-Boxes. WAIFI 2007, June 21-22, Madrid, Spain, LNCS Vol. 4547, 159-176, Springer Berlin Heidelberg.

[11] Borghoff, J., Canteaut, A., Güneysu, T., Kavun, E. B., Knezevic, M., Knudsen, L. R., Leander, G., Nikov, V., Paar, C., Rechberger, C., Rombouts, P., Thomsen, S. S., Yalçın, T. 2012. PRINCE – A low-latency block cipher for pervasive computing applications. ASIACRYPT 2012, December 2-6, Beijing, China, LNCS Vol. 7658, 208-225, Springer Berlin Heidelberg.

[12] Browning, K. A., Dillon, J. F., McQuistan, M. T., Wolfe, A. J. 2009. An APN permutation in dimension six. The 9th Conference on Finite Fields and

Applications - Fq9, July 13-17, Dublin, Ireland, Contemporary Mathematics Vol. 518, 33-42, AMS USA.

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

[14] Kavut, S. 2015. DPA resistivity of small size S boxes. The 3rd International Symposium on Digital Forensics and Security – ISDFS 2015, 11-12 May, Ankara, Turkey, 64-69.

[15] Rothaus, O. S. 1976. On bent functions. Journal of Combinatorial Theory, 20a, 300-305.

[16] Chakraborty, K., Sarkar, S., Maitra, S., Mazumdar, B., Mukhopadhyay, D., Prouff, E. 2017. Redefining the Transparency Order. Designs, Codes and Cryptography, 82(1), 95-115.

[17] Nguyen, C., Tran, L., Nguyen, K. 2014. On the resistance of Serpent-type 4 bit S-Boxes against differential power attacks. IEEE Fifth International Conference on Communications and Electronics – ICCE 2014, 30 Jul - 01 Aug 2014, Danang, Vietnam, 542-547.

[18] Cannière, C. D. 2007. Analysis and design of symmetric encryption algorithms. University of Leuven, 164p, Doctoral Dissertation, Leuven.

[19] Daemen, J., Govaerts, R., Vandewalle, J. 1993. A new approach to block cipher design. Fast Software Encryption, December 9-11, Cambridge, U. K., LNCS Vol. 809, 18-32, Springer Berlin Heidelberg.

[20] Knudsen, L., Leander, G., Poschmann, A., Robshaw, M. J. B. 2010. PRINTcipher: A block cipher for IC-printing. CHES 2010, August 17-20, Santa Barbara, USA, LNCS Vol. 6225, 16-32, Springer-Verlag Berlin Heidelberg.

[21] Brinkmann, M., Leander, G. 2008. On the classification of APN functions up to dimension five. Designs, Codes and Cryptography, 49(1-3), 273-288.

[22] Daemen, J. 1995. Cipher and hash function design strategies based on linear and differential cryptanalysis. University of Leuven, 252p, Doctoral Dissertation, Leuven.

[23] Rijmen, V., Barreto, P. S. L. M., Filho, D. L. G. 2008. Rotation symmetry in algebraically generated cryptographic substitution tables. Inf. Process. Lett., 106(6), 246-250.

[24] Nyberg, K. 1993. Differentially Uniform Mappings for Cryptography. EUROCRYPT'93, May 23–27, Lofthus, Norway, LNCS Vol. 765, 55-64, Springer Berlin Heidelberg.

[25] Bracken, C., Leander, G. 2010. A highly nonlinear differentially 4 uniform power mapping that permutes fields of even degree. Finite Fields and Their Applications, 16(4), 231-242.

[26] Li, Y., Wang, M., Yu, Y. 2013. Constructing differentially 4-uniform permutations over $GF(2^{2k})$ from the inverse function revisited. http://eprint.iacr.org/2013/731 (Erişim Tarihi: 01.02.2017).

[27] Yu, Y., Wang, M., and Li, Y. 2011. Constructing differential 4-uniform permutations from known ones. http://eprint.iacr.org/2011/047 (Erişim tarihi: 01.02.2017).

[28] Gold, R. 1968. Maximal recursive sequences with 3-valued recursive crosscorrelation functions. IEEE Trans. Inform. Theory, 14, 154-156.

[29] Kasami, T. 1971. The weight enumerators for several classes of subcodes of the second order binary Reed-Muller codes. Inform. Control, 18, 369-394.

[30] Bracken, C., Tan, C. H., Tan, Y. 2012. Binomial differentially 4 uniform permutations with high nonlinearity. Finite Fields and Their Applications, 18(3), 537-546.

[31] Li, Y., Wang, M. 2014. Constructing differentially 4-uniform permutations over $GF(2^{2m})$ from quadratic APN permutations over $GF(2^{2m+1})$. Des. Codes Cryptogr., 72(2), 249-264.

[32] Kavut, S., Yücel, M. D. 2005. Güçlü Kriptografik Özelliklere Sahip Boole İşlevleri Tasarımında Yeni bir Algoritma. I. Ulusal Kriptoloji Sempozyumu, 18-20 Kasım, Ankara, 95-105.