Bilgisayar Bilimleri ve Mühendisliği Dergisi

Cilt-16
Sayı-2
2023

(1057, 31)-Aralıklı Dizilerden Üretilen Boole Fonksiyonlar

Boolean Functions Generated from (1057, 31)-Interleaved Sequences

Selçuk KAVUT
Balıkesir Üniversitesi, Mühendislik Fakültesi
Bilgisayar Mühendisliği
Balıkesir, Türkiye
skavut@balikesir.edu.tr
ORCID: 0000-0002-9460-1418

Öz

1983 yılında keşfedildikten itibaren günümüzde halen bilinen en yüksek doğrusal olmama değerine (16276) sahip olan 15 değişkenli Patterson-Wiedemann (PW) fonksiyonlarının, özel bir yapıda bulunan (151, 217)-aralıklı dizilerden üretilen döngüsel simetrik Boole fonksiyonları (DSBF'ler) olarak yorumlanabildiği bilinmektedir. İlgili yayınlarda, aynı doğrusal olmama değerine ulaşan başka bir inşa veya arama yöntemi bilinmemekle birlikte, tam arama veya sezgisel arama yöntemleri ile (151, 217)- ve (217, 151)-aralıklı dizilerden, bükük-bağlaşım sınırını (16256) aşan doğrusal olmama değerine sahip genelleştirilmiş DSBF'lerin elde edilebildiği gösterilmiştir. Ancak, bahsedilen yöntemlerle ulaşılan en iyi doğrusal olmama değeri 16268'i aşamamıştır. Bu çalışmamızda, (1057, 31)-aralıklı dizilerden üretilen DSBF'ler araştırılmış ve sezgisel arama yöntemi ile 16272 doğrusal olmama değerine ulaşılmıştır.

Anahtar Sözcükler: Aralıklı dizi, döngüsel simetrik Boole fonksiyonu (DSBF), doğrusal olmama

Abstract

It is known that Patterson-Wiedemann (PW) functions with 15-variables, which still have the highest known nonlinearity value (16276) since their discovery in 1983, can be interpreted as rotation-symmetric Boolean functions (RSBFs) produced from (151, 217)-interleaved sequences which are in the form of a special structure. In the related literature, though no other search/construction method achieving the same nonlinearity value is known, it has been shown that generalized RSBFs with nonlinearity exceeding the bent-concatenation bound (16256) can be obtained from (151, 217)- and (217, 151)-interleaved sequences by using exhaustive or heuristic search methods. However, the best nonlinearity value reached by these methods could not exceed 16268. In this study, RSBFs produced from (1057, 31)-interleaved sequences are investigated and the nonlinearity value of 16272 is attained by a heuristic search method.

Keywords: Interleaved sequence, nonlinearity, rotation-symmetric Boolean function (RSBF)

Gönderme, düzeltme ve kabul tarihi: 20.11.2022 - 25.02.2023 – 21.03.2023
Makale türü: Araştırma

1. Giriş

Simetrik kriptografide, bir kripto sistemde kullanılan Boole fonksiyonları önemli yapı taşlarıdır ve en önemli kriptografik özelliklerinden birisi, (akan şifrelerde) en iyi afin yaklaşıklama saldırısına [1] ve (blok şifrelerde) doğrusal kripto analize [2] karşı dayanıklılığın sağlanması için yüksek olması gereken doğrusal olmamadır. n değişkenli bir Boole fonksiyonu $f: \mathrm{F}_2^n \to \mathrm{F}_2$, burada $\mathrm{F}_2 = \{0,1\}$, n bit girişi 1 bit çıkışa dönüştüren bir fonksiyon olarak tanımlanır. Çift n sayıları için, n değişkenli Boole fonksiyonların alabileceği en yüksek doğrusal olmama değeri $2^{n-1} - 2^{n/2-1}$ olup, bu değeri alan Boole fonksiyonlara bükük fonksiyonlar denilmektedir. Tek n sayıları için ise, en yüksek doğrusal olmama değerinin üst sınırı $2 \times \left\lfloor 2^{n-2} - 2^{n/2-2} \right\rfloor$ olarak verilmektedir [3]. n bir tek sayı, g ve h fonksiyonları $(n-1)$ değişkenli bükük fonksiyonlar olmak üzere, bu fonksiyonların bağlaşımı olarak tanımlanan n değişkenli f fonksiyonu $f(x_0, x_1, \dots, x_{n-1}) = x_0 g(x_1, x_2, \dots, x_{n-1}) \oplus (1 \oplus x_0) h(x_1, x_2, \dots, x_{n-1})$, bükük bağlaşım sınırı olarak bilinen $2^{n-1} - 2^{(n-1)/2}$ doğrusal olmama değerine sahiptir. $n \leq 7$ tek sayıları için, n değişkenli Boole fonksiyonların alabildiği en yüksek doğrusal olmama değeri bahsedilen bükük-bağlaşım sınırıdır. Bununla birlikte, $n > 7$ herhangi bir tek sayı olmak üzere, yayınlarda n değişkenli Boole fonksiyonların ulaşabileceği en yüksek

doğrusal olmama değeri bilinmemektedir. Bükük bağlaşım sınırından yüksek doğrusal olmama değerine sahip Boole fonksiyonları, yayınlarda Patterson-Weidemann (PW) fonksiyonları olarak bilinen 16276 ($= 2^{15-1} - 2^{(15-1)/2} + 20$) doğrusal olmama değerine sahip ve birbiri ile afin ilişkili olmayan iki 15 değişkenli Boole fonksiyonun 1983 yılında Patterson ve Wiedemann tarafından keşfedilmesiyle [4] ortaya çıkmıştır. Bunun bir sonucu olarak, PW fonksiyonlarından bir tanesi ve bir bükük fonksiyonun dolaysız toplamı ile, $n > 15$ tek sayıları için, $2^{n-1} - 2^{(n-1)/2} + 20 \cdot 2^{(n-15)/2}$ doğrusal olmama değerine sahip n değişkenli Boole fonksiyonlar elde edilebilmektedir. Diğer taraftan, Kavut ve Yücel tarafından 2007 yılında 242 ($= 2^{9-1} - 2^{(9-1)/2} + 2$) doğrusal olmama değerine sahip 9 değişkenli Boole fonksiyonların ortaya çıkarılmasıyla [5], $n > 9$ tek sayıları için, $2^{n-1} - 2^{(n-1)/2} + 2 \cdot 2^{(n-9)/2}$ doğrusal olmama değerine sahip n değişkenli Boole fonksiyonlar, bahsedilen dolaysız toplam yöntemi ile elde edilebilir olmuştur. Ancak bu doğrusal olmama değerinin $n \geq 15$ için PW fonksiyonlarından elde edilen doğrusal olmama değerinden düşük olduğuna dikkat edilmelidir.

Bükük bağlaşım sınırını aşan doğrusal olmama değerine sahip Boole fonksiyonlarının inşası simetrik kriptografide karşılaşılan en zor problemlerdendir ve ilgili yayınlarda bu tür fonksiyonları ortaya çıkaran çalışmalar temel olarak, doğrusal olmama yönünden zengin kriptografik alt uzayların belirlenmesi ve bu alt uzaylarda tam veya sezgisel arama yöntemlerinin uygulanmasına dayanır. Patterson ve Wiedemann, keşfettikleri Boole fonksiyonları $\mathrm{F}_{2^5}^* \cdot \mathrm{F}_{2^3}^*$ döngüsel grubu aksiyonu altında değişmez özelliğe sahip eş güçlü fonksiyonların oluşturduğu 2^{11} büyüklüğündeki arama uzayında tam arama yürüterek ortaya çıkarmışlardır [4]. Bu fonksiyonların özel bir yapıda bulunan (151, 217)-aralıklı dizilerden elde edilen DSBF'ler olarak yorumlanabileceği, Gangopaphyay ve ark. tarafından gösterilmiştir [6]. Kavut ve Yücel, doğrusal olmama değeri bükük-bağlaşım sınırını aşan 9 değişkenli Boole fonksiyonları arama uzayı 2^{104} büyüklüğündeki (genelleştirilmiş 3-döngüsel simetrik Boole fonksiyonların (3-DSBF'lerin) doğrusal olmama yönünden zengin bir alt uzayı olan) dihedral simetrik Boole fonksiyonları için yürüttükleri sezgisel arama algoritması ile elde etmişlerdir [5]. Yakın zamanda, (151, 217)-aralıklı dizilerden üretilen ve arama uzayı büyüklükleri sırasıyla $2^{28.2}$ ve $2^{47.85}$ olan 3- ve 5-DSBFs'ler için tam arama yapılarak, her iki arama uzayında da bükük bağlaşım sınırından yüksek doğrusal olmama değerine sahip yeni PW türü Boole fonksiyonlar tespit edilmiştir [7]. Daha sonra, PW inşa yönteminin genelleştirildiği [8] çalışmasında ise (217,151)-aralıklı dizilerden üretilen (k-) DSBF'ler için arama yapılmıştır. Özel olarak, arama uzayının büyüklüğü sırasıyla $2^{15.3}$ ve $2^{44.1}$ olan DSBF'ler ve 3-DSBF'ler için tam arama, arama uzayının büyüklüğü $2^{88.1}$ olan 5-DSBF'ler için ise sezgisel arama yöntemleri ile bükük bağlaşım sınırından yüksek doğrusal olmama değerine sahip yeni Boole fonksiyonlar elde edilmiştir. Bununla birlikte, bahsedilen [7, 8] çalışmalarında ulaşılan en yüksek doğrusal olmama değeri 16268 olmuştur.

Çalışmamızda, (1057, 31)-aralıklı dizilerden üretilen DSBF'ler ele alınarak, bu DSBF'lerin oluşturduğu 2^{73} büyüklüğündeki arama uzayında, daha önce 21 değişkenli PW türü fonksiyonlar için kullanılan [9] sezgisel arama algoritması bu çalışmada ele alınan duruma uygulanmıştır. Bunun sonucunda, [7, 8] çalışmalarında ulaşılan en iyi doğrusal olmama değerinden (16268) daha yüksek bir doğrusal olmama değeri (16272) elde edilmiştir. Bu çalışmada ve daha önceki [4, 5, 7-9] çalışmalarında elde edilen bükük-bağlaşım sınırından yüksek doğrusal olmama değerine sahip Boole fonksiyonları dengesiz olduklarından (diğer bir ifadeyle, doğruluk tablolarındaki 0'ların sayısı 1'lerin sayısına eşit olmadığından) herhangi bir kripto sistemde doğrudan kullanılamazlar. Bununla birlikte, bu fonksiyonlar esneklik, cebirsel derece, cebirsel bağışıklık, mutlak gösterge ve doğrusal olmama gibi kriptografik özellikler bakımından güçlü Boole fonksiyonların tasarımı için temel yapıtaşları olarak kullanılmaktadır [10-12]. Özel olarak, [12] çalışmasında PW fonksiyonlarının komşuluğunda kaba kuvvet arama ile dengeli Boole fonksiyonlar elde edilmiş olup, bu çalışmada ise bükük-bağlaşım sınırını aşan doğrusal olmama değerine sahip, aralıklı dizi yapısında ve dengeli olmayan DSBF'ler sezgisel arama yöntemi ile üretilmektedir. Bahsedilen kriptografik özellikleri taşıyan Boole fonksiyonları, özellikle donanım kapasitesinin kısıtlı olduğu hafif sıklet kripto sistemlerde, yaygın şekilde kullanılan kombinasyon üreteci ve filtre üreteci tasarımlarına sahip akan şifreler için doğrusal olmayan birleştirici olarak doğrudan kullanılabilmektedirler. Ayrıca, çalışmamızda elde edilen Boole fonksiyonları döngüsel simetrik olduğundan ve DSBF'ler sahip oldukları (sadece yörünge temsilcilerine karşılık gelen çıkış bitleri ile ifade edilebilmelerini sağlayan) cebirsel özellik nedeniyle verimli bir şekilde gerçekleştirilebildiğinden [13, 14], bulunan DSBF'lerden türetilebilecek güçlü kriptografik özelliklere sahip fonksiyonların verimli bir şekilde gerçekleştirme olanağına sahip olduğu düşünülmektedir.

2. Temel Bilgiler

$f: \mathrm{F}_{2^n} \to \mathrm{F}_2$, n değişkenli bir Boole fonksiyon olsun. F_{2^n} sonlu cisminin elemanları, derecesi n olan bir indirgenemez polinom ile elde edilen ve n bit ile gösterilen ikili polinomlar olduğundan, f fonksiyonu eşdeğer olarak $\mathrm{F}_2^n \to \mathrm{F}_2$ biçiminde düşünülebilir. Her $\alpha \in \mathrm{F}_{2^n}$ için, $f(\alpha) = f(\alpha^2)$ koşulunu sağlayan fonksiyonlara eş güçlü fonksiyonlar denilmektedir. Burada, eğer bahsedilen indirgenemez polinom bir primitif polinom olarak seçilir ve normal taban kullanılırsa, eş güçlü fonksiyonlar DSBF'lere [15, 16], her $\alpha \in \mathrm{F}_{2^n}$ için $f(\alpha) = f(\alpha^{2^k})$ koşulunu sağlayan fonksiyonlar ise, burada k bir sabit ve $k|n$, (genelleştirilmiş) k-DSBF'lere [5] karşılık gelir. Yayınlarda keşfedilen bükük bağlaşım sınırından yüksek doğrusal olmama değerine sahip fonksiyonların (k-)DSBF'ler sınıfına ait olmaları, bu sınıfın doğrusal olmama yönünden zengin olduğunun göstergesidir.

Her $x \in \mathrm{F}_{2^n}$ için $Tr(x) = x \oplus x^2 \oplus x^{2^2} \oplus \ldots \oplus x^{2^{n-1}}$ ve $c \in \mathrm{F}_2$ olmak üzere, n değişkenli bir afin fonksiyon $Tr(\alpha x) \oplus c$ biçimde tanımlanır. $h_\alpha(x) = Tr(\alpha x) \oplus 1$ ve $l_\alpha(x) = Tr(\alpha x)$ olsun, burada $l_\alpha(x)$ doğrusal fonksiyon olarak isimlendirilir. n değişkenli iki fonksiyon f ve g için, aralarındaki uzaklık $d(f,g)$, 2^n elemanlı doğruluk tabloları arasındaki Hamming uzaklığı olarak tanımlanır. Diğer bir ifadeyle, $d(f,g) = |\{x \in \mathrm{F}_{2^n} : f(x) \neq g(x)\}|$. Herhangi bir

Boole fonksiyon f için doğrusal olmama değeri, tüm afin fonksiyonlara (yani, $h_\alpha(x)$ ve $l_\alpha(x)$ fonksiyonlarına) olan Hamming uzaklıkların en küçüğü olarak ifade edilmektedir.

$p, q > 2$ birer asal sayı olmak üzere $n = pq$ ve $f: \mathrm{F}_{2^n} \to \mathrm{F}_2$ fonksiyonu $\mathrm{F}_{2^p}^*$ döngüsel grubu altında değişmez olsun. Bu durumda, f fonksiyonu aşağıda verilen ve her bir sütunu tümü 0 veya tümü 1 olan bir (d, r)-aralıklı dizi biçiminde yorumlanabilir:

$$\begin{bmatrix} f(\omega^0) & f(\omega^1) & f(\omega^2) & \dots & f(\omega^{d-1}) \\ f(\omega^d) & f(\omega^{d+1}) & f(\omega^{d+2}) & \dots & f(\omega^{2d-1}) \\ f(\omega^{2d}) & f(\omega^{2d+1}) & f(\omega^{2d+2}) & \dots & f(\omega^{3d-1}) \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ f\left(\omega^{(r-1)d}\right) & f\left(\omega^{(r-1)d+1}\right) & f\left(\omega^{(r-1)d+2}\right) & \dots & f(\omega^{rd-1}) \end{bmatrix},$$

burada $r = 2^p - 1$, $d = (2^n - 1)/r$ ve ω, F_{2^n} sonlu cisminin bir primitif elemanıdır. Bu gösterimde, $f(0)$ değeri keyfi olarak 0 veya 1 alınabilir; çalışmamızda $f(0) = 0$ alınmıştır. Verilen aralıklı dizinin satırlarını 0'dan $r - 1$'e ve sütunlarını 0'dan $d - 1$'e numaralandıralım. Eğer f fonksiyonu eş güçlü ise, negatif olmayan bir s tamsayısı için

$$i \sim j \text{ ancak ve ancak } i \equiv j2^s \bmod d$$

olarak tanımlanan eşdeğerlik ilişkisine göre sütunların eşdeğerlik sınıflarına bölüntüleneceğine dikkat edilmelidir, burada $i, j \in \{0,1, \dots, d-1\}$. Diğer bir ifadeyle, (d, r)-aralıklı dizisi ile temsil edilen eşgüçlü bir f Boole fonksiyonunun, aynı eşdeğerlik sınıfındaki bütün sütunları ya tümü 1 ya da tümü 0 olan sütunlardan oluşur. Bu eşdeğerlik ilişkisini ρ_d ile gösterelim. Çalışmamızda ele aldığımız $n = 15$ durumu için, ρ_{1057} eşdeğerlik ilişkisi ile (1057, 31)-aralıklı dizilerden elde edilen eşgüçlü fonksiyonların sayısının (diğer bir ifadeyle, arama uzayının büyüklüğünün) 2^{73} olduğu görülebilir.

Aralıklı dizi gösterimine sahip herhangi bir f fonksiyonu için, tümü 1 olan sütunların ℓ tane olduğunu kabul edersek, bu fonksiyonun tüm afin fonksiyonlara olan uzaklıkları aşağıdaki gibi hesaplanabilir [4]:

$$d(f, \mathbf{0}) = \ell(2^p - 1), \quad d(f, \mathbf{1}) = 2^n - \ell(2^p - 1),$$
$$d(f, l_\alpha) = 2^{n-1} - 2^p t(\alpha) + \ell,$$
$$d(f, h_\alpha) = 2^{n-1} + 2^p t(\alpha) - \ell, \qquad (1)$$

burada, $\alpha \in \mathrm{F}_{2^n}^*$ olmak üzere, $t(\alpha)$ değeri f ve h_α fonksiyonlarının aynı pozisyonlarındaki tümü 1 olan sütunlarının sayısını, $\mathbf{0}$ ve $\mathbf{1}$ ise sırasıyla tümü 0 ve tümü 1 olan 2^n uzunluğundaki ikili dizileri göstermektedir. Doğrusal olmama tanımından, f fonksiyonunun bükük bağlaşım sınırından yüksek doğrusal olmama değerine sahip olabilmesi için, (1) ile verilen eşitlikler vasıtasıyla, aşağıdaki eşitsizliklerin sağlanması gerektiği görülmektedir:

$$\kappa^- < \ell < \kappa^+, \qquad (2)$$

$$\frac{1}{2^p}(\kappa^- - 2^{\frac{n-1}{2}}) < t(\alpha) < \frac{1}{2^p}(\kappa^+ + 2^{\frac{n-1}{2}}), \qquad (3)$$

burada $\kappa^\pm = (2^{n-1} \pm 2^{\frac{n-1}{2}})/(2^p - 1)$. ℓ için verilen (2) koşulu, f fonksiyonunun Hamming ağırlığını (eşdeğer olarak, tümü 1 olan sütunların sayısını) belirlediği için, ağırlık koşulu olarak adlandırılmaktadır. (3) ile verilen koşulun sağlanması için $2^n - 1$ eşitsizliğin sağlanması gerektiği düşünülebilir; ancak, Gangopadhyay ve ark. tarafından gösterildiği [6] gibi, ρ_d eşdeğerlik ilişkisi ile elde edilen tüm eşdeğerlik sınıflarının sayısı kadar eşitsizlikten oluşan bir eşitsizlik sisteminin çözülmesi, bu koşulun sağlanması için yeterlidir.

Bölüm 3'te verilen arama algoritmasında, F_2^{15} sonlu cisminin gerçekleştirilmesi için $x^{15} + x + 1$ primitif polinomu kullanılmıştır.

Bu bölümde anlatılanların örneklendirilmesi amacıyla, $\mathrm{F}_{2^2}^*$ döngüsel grubu altında değişmez olan 4 değişkenli Boole fonksiyonları ele alalım ve F_2^4 sonlu cisminin gerçekleştirilmesi için $x^4 + x + 1$ primitif polinomu kullanalım. Örnekteki Boole fonksiyonlar, tümü 1 veya tümü 0 olan sütunlardan oluşan (5, 3)-aralıklı diziler ile temsil edilebilir ve bu durumda (**0** doğrusal fonksiyonu dışında) tüm doğrusal fonksiyonlar, daha önce bahsedilen aralıklı dizinin tanımından, aşağıdaki matrisler ile ifade edilebilir:

$$I_0 = \begin{bmatrix} 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}, I_1 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \end{bmatrix},$$
$$I_2 = \begin{bmatrix} 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{bmatrix}, I_3 = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \end{bmatrix},$$
$$I_4 = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \end{bmatrix}, I_5 = \begin{bmatrix} 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \end{bmatrix},$$
$$I_6 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \end{bmatrix}, I_7 = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{bmatrix},$$
$$I_8 = \begin{bmatrix} 0 & 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}, I_9 = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 \\ 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix},$$
$$I_{10} = \begin{bmatrix} 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{bmatrix}, I_{11} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{bmatrix},$$
$$I_{12} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 1 \end{bmatrix}, I_{13} = \begin{bmatrix} 1 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix},$$
$$I_{14} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 \end{bmatrix},$$

burada I_i matrisi, F_2^4 sonlu cisminin bir primitif elemanı ω olmak üzere, $\alpha = \omega^i$ için $l_\alpha(x) = Tr(\alpha x)$ doğrusal fonksiyonuna karşılık gelen aralıklı dizidir. $h_\alpha(x) = Tr(\alpha x) \oplus 1$ fonksiyonlarına karşılık gelen aralıklı dizilerin ise yukarıda verilen matrislerin tümleyenleri olarak (diğer bir ifadeyle, matrisleri oluşturan bitlere mod 2'ye göre 1 ekleyerek) elde edilebildiği görülmektedir.

Örneğin, aşağıdaki aralıklı diziye sahip bir f Boole fonksiyonunun doğrusal olmama değerini (1) eşitliklerini kullanarak bulalım:

$$\begin{bmatrix} 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 \end{bmatrix}.$$

$n = 4, p = 2$ ve tümü 1 olan 2 tane sütun olduğundan ($\ell = 2$ anlamına gelir), $d(f, \mathbf{0}) = 2(2^2 - 1) = 6$ ve $d(f, \mathbf{1}) = 2^4 -$

$2(2^2-1)=10$ bulunur. Verilen aralıklı dizide ikinci ve dördüncü sütunlar tümü 1 sütunlarıdır. $t(\alpha)$ değeri, h_α fonksiyonunu temsil eden aralıklı dizinin bu pozisyonlarda bulunan tümü 1 olan sütunlarının sayısıdır. Böylelikle $t(\alpha)$ değerleri $\alpha=\omega^i$ olmak üzere, $i=0,1,\dots,14$ için sırasıyla 0, 0, 1, 0, 1, 0, 0, 1, 0, 1, 0, 0, 1, 0, 1 olarak bulunur. Bu değerlere karşılık gelen $d(f,l_\alpha)$ ve $d(f,h_\alpha)$ uzaklıkları ise sırasıyla 10, 10, 6, 10, 6, 10, 10, 6, 10, 6, 10, 10, 6, 10, 6 ve 6, 6, 10, 6, 10, 6, 6, 10, 6, 10, 6, 6, 10, 6, 10 olarak elde edilir. Doğrusal olmama değeri tüm afin fonksiyonlara olan en küçük uzaklık olarak tanımlandığından, f Boole fonksiyonunun doğrusal olmama değerinin 6 olduğu görülmektedir. En yüksek doğrusal olmama değerine sahip olduğundan, burada f bir bükük fonksiyondur.

Şimdi $\mathrm{F}_{2^2}^*$ döngüsel grubu altında değişmez olan 4 değişkenli tüm bükük fonksiyonları bulalım. Bu durumda, (1) ile verilen uzaklıkların tümü 5'ten büyük olmalıdır:

$d(f,\mathbf{0})=3\ell>5,\quad d(f,\mathbf{1})=16-3\ell>5,$
$d(f,l_\alpha)=8-4t(\alpha)+\ell>5,$
$d(f,h_\alpha)=8+4t(\alpha)-\ell>5.$

Burada, $n=4$ için bükük fonksiyonların doğrusal olmama değeri 6 olduğundan, yukardaki uzaklıklar doğrudan 6'ya eşit alınabilirdi. Bununla birlikte, örneğimizin çalışmamızda izlenen yöntemle paralel olması amacıyla uzaklıklar 5'ten büyük olarak yazılmıştır (Çalışmamızda ele alınan $n=15$ durumu için en yüksek doğrusal olmama değeri bilinmemektedir ve (1) ile verilen uzaklıklar bükük-bağlaşım sınırından büyük olarak seçilmiştir.). ℓ ve $t(\alpha)$ birer tamsayı olmak zorunda olduklarından, elde edilen bu eşitsizlikler aşağıda gibi ifade edilebilir:

$2\le\ell\le3,$

$0\le t(\alpha)\le1$ ($\ell=2$ için) ve $1\le t(\alpha)\le1$ ($\ell=3$ için).

ℓ değeri tümü bir olan sütunların sayısı olduğundan, bu sütunların 2 veya 3 tane olması gerektiği görülmektedir. Dolayısıyla bu koşulu sağlayan aralıklı dizilerin sayısı $\binom{5}{2}+\binom{5}{3}=20$ olarak bulunur. $t(\alpha)$ için elde edilen diğer koşullar ise Gangopadhyay ve ark. tarafından PW inşası için verilen algoritmanın [6] örneğimize uygulanması ile aşağıdaki eşitsizlik sistemlerine indirgenebilir:

$0\le s_j\le1$ ($\ell=2$ için) ve $1\le s_j\le1$ ($\ell=3$ için),

burada $s_j=f(\omega^j)$, $j\in\{0,1,2,3,4\}$, f Boole fonksiyonuna karşılık gelen aralıklı dizinin j. sütununun ilk elemanını temsil etmektedir. $\ell=3$ için bulunan sistem ($s_j=1\ \forall j\in\{0,1,2,3,4\}$), aralıklı dizinin tüm sütunlarının tümü 1 olan sütunlar olması gerektiğini gösterir; bu ise tümü 1 olan sütun sayısının 3 olması koşulu ile çeliştiğinden, ℓ değerinin 3 olamayacağı anlamına gelir (dolayısıyla, yukarda bulunan aralıklı dizilerin sayısı 20'den 10'a düşer). Diğer taraftan, $\ell=2$ için bulunan sistem ($0\le s_j\le1\ \forall j\in\{0,1,2,3,4\}$) herhangi bir kısıtlamaya neden olmadığından, f'nin bükük fonksiyon olması için tek koşul $\ell=2$ ağırlık koşuludur; diğer bir ifadeyle, f'nin aralıklı dizisinde herhangi 2 sütunun tümü 1 ve diğer sütunların tümü 0 olan sütunlar olmasıdır. Bunun sonucunda, $\binom{5}{2}=10$ tane bükük fonksiyon elde edilir. Bir Boole fonksiyonunun doğruluk tablosundaki tüm bitlerin tümleyeni alındığında doğrusal olmama özelliği değişmeyeceğinden, bu şekilde elde edilen Boole fonksiyonlar da hesaba katıldığında toplam olarak 20 bükük fonksiyon bulunmuş olur.

Örneğimizde eşgüçlü bükük fonksiyonların var olmadığı da görülebilir. Özel olarak, ρ_5 eşdeğerlik ilişkisine göre aralıklı dizinin sütunları bölüntülendiğinde, ilk sütun dışındaki tüm sütunlar aynı eşdeğerlik sınıfına ait olmaktadır. Bu durum ağırlık koşulunun sağlanmasını olanaksız kıldığından, $\mathrm{F}_{2^2}^*$ döngüsel grubu altında değişmez olan 4 değişkenli bükük fonksiyonların içinde eşgüçlü bir Boole fonksiyon olmadığı sonucuna varılır.

$f:\mathrm{F}_2^n\to\mathrm{F}_2$, n değişkenli bir Boole fonksiyon olsun. Aynı değişken sayısına sahip bir g fonksiyonu için, $f(x)g(x)=0\ \forall x\in\mathrm{F}_2^n$ koşulu sağlanıyorsa, g fonksiyonuna f fonksiyonunun sıfırlayıcısı denir. $f'(x)=f(x)\oplus1\ \forall x\in\mathrm{F}_2^n$ olmak üzere, f ve f' fonksiyonlarının sıfırdan farklı tüm sıfırlayıcılarının oluşturduğu kümeleri sırasıyla $AN(f)$ ve $AN(f')$ ile gösterelim. f fonksiyonunun cebirsel bağışıklığı $AN(f)\cup AN(f')$ kümesindeki fonksiyonların en küçük cebirsel derecesi olarak tanımlanır. n değişkenli bir Boole fonksiyonu için cebirsel bağışıklığın en fazla $\lceil n/2\rceil$ olduğu bilinmektedir [17]. Doğrusal olmama, mutlak gösterge ve cebirsel derece gibi diğer kriptografik özelliklerin tanımları örneğin [18] çalışmasında bulunabilir. [18] çalışmasında n biti m bite gönderen ve çok çıkışlı Boole fonksiyonları olarak tanımlanan S-kutuları (yerleştirme kutuları) ele alınırken, bu çalışmada n biti 1 bite gönderen (tek çıkışlı) Boole fonksiyonların ele alındığına dikkat edilmelidir.

3. Arama Algoritması

Ağırlık koşulunu kullanarak, (2) ile verilen eşitsizlikten $n=15$ ve $p=5$ için $525\le\ell\le532$ elde edildiğinden, (1057, 31)-aralıklı dizisinin 1057 sütunundan en az 525 ve en fazla 532 tanesi tümü 1 olan sütunlar olmak zorundadır. Diğer taraftan, ρ_{1057} eşdeğerlik ilişkisine göre 70 tanesi 15'er, 2 tanesi 3'er ve 1 tane 1 sütundan oluşan 73 eşdeğerlik sınıfının bulunduğu görülebilir. Bu nedenle, ağırlık koşulunun sağlanması için tümü 1 olan sütunların, her biri 15 sütun içeren (70 eşdeğerlik sınıfından) 35 eşdeğerlik sınıfına ait tüm sütunlar olması gerektiği sonucuna varılır. Bu durumda, tümü 1 olan sütunların sayısı $15\times35=525$ olduğundan, geriye kalan (3 sütunlu ve 1 sütunlu) 3 eşdeğerlik sınıfının herhangi birisinde bulunan sütunlar rastgele tümü 1 veya tümü 0 olan sütunlar olabilir. Böylelikle, gerçekleştirdiğimiz arama ağırlık koşulunu sağlayan Boole fonksiyonlar için yürütüldüğünden, 2^{73} olan arama uzayının büyüklüğü $2^{69.6}\left(\approx\binom{70}{35}\times2^3\right)$ büyüklüğüne düşmektedir. Bu çalışmada, daha önce $n=21$ durumu için önerilen [9] sezgisel arama algoritması Şekil 1'de sunulduğu gibi $n=15$ durumuna uyarlanarak, bahsedilen arama uzayı için yürütülmüştür.

Kullanılan arama algoritması, Boole fonksiyon tasarımında uygun maliyet fonksiyonu seçimiyle güçlü kriptografik özellikleri ortaya çıkardığı kanıtlanmış [19, 20] en dik iniş prensibine dayalı arama algoritmasıdır. Tavlama benzetimi ve tepe tırmanma gibi benzer arama algoritmaları ile

karşılaştırıldığında, bu algoritmanın tavlama benzetiminden ve tavlama benzetiminin ise genetik arama ve tepe tırmanmadan daha verimli sonuçlar ürettiği sırasıyla [19] ve [21] çalışmalarında gösterilmiştir. En dik iniş prensibine dayalı arama yönteminin bahsedilen diğer yöntemler ile karşılaştırması ve daha iyi sonuçlar üretebilmesinin sebepleri [18] çalışmasında tartışılmıştır.

(1057, 31)-aralıklı dizisi ile temsil edilen bir Boole fonksiyonun doğrusal olmama değeri, karşılık gelen doğruluk tablosu elde edilerek ve Walsh-Hadamard dönüşümü hesaplanarak ile bulunabilir. Ancak, n değişkenli bir Boole fonksiyonu için Walsh-Hadamard dönüşümünün hesaplama karmaşıklığı en iyilenmiş durumda $O(n2^n)$ olduğundan, bu yöntem oldukça maliyetlidir. Bunun yerine, önceki bölümde bahsedildiği üzere Gangopadhyay ve ark. tarafından gösterildiği [6] gibi, ağırlık koşulunu sağlayan bir Boole fonksiyonun bükük-bağlaşım sınırından yüksek doğrusal olmama değerine sahip olup olmadığını belirlemek için, ρ_d eşdeğerlik ilişkisinin ürettiği eşdeğerlik sınıflarının sayısı kadar (bizim durumumuz için bu sayı 73) eşitsizlikten oluşan bir eşitsizlik sisteminin sağlanıp sağlanmadığına bakılabilir. Gangopahyay ve ark.'nın PW inşası (diğer bir ifadeyle, (151, 217)-aralıklı diziler ile temsil edilen eş güçlü Boole fonksiyonları) için eşitsizlik sistemini üreten algoritması, bu çalışmada ele aldığımız (1057, 31)-aralıklı diziler ile temsil edilen eş güçlü Boole fonksiyonları için uyarlanmış ve bükük-bağlaşım sınırını aşan doğrusal olmama değerine ulaşmak için sağlanması gereken eşitsizlik sistemi (aşağıda verilen (5) ile gösterildiği biçimde) elde edilmiştir.

Girdi: Ağırlık koşulunu sağlayacak şekilde rastgele üretilen kısaltılmış doğruluk tablosu s_{aday}
Çıktı: Bükük-bağlaşım sınırını aşan doğrusal olmama değerini veren yineleme çıktısı s_min
$s \leftarrow s_{aday}$;
for $K = 0$ to $N - 1$ **do** {
  $k \leftarrow 0$;
  //s vektöründe 15 elemanlı eşdeğerlik sınıflarına
  //karşılık gelen 70 bitten
  $y_0 \leftarrow$ 0'ların pozisyonları; // (35 tane)
  $y_1 \leftarrow$ 1'lerin pozisyonları; // (35 tane)
  $y_2 \leftarrow$ Geriye kalan bitlerin pozisyonları; // (3 tane)
  for $i = 0$ to 34 **do**
    for $j = 0$ to 34 **do** {
      $s_{y_0[i]}$ ve $s_{y_1[j]}$'i birbiri ile değiştir;
      $SET[k] \leftarrow s_{değişen}$; $M[k] \leftarrow maliyet_{değişen}$;
      $k \leftarrow k + 1$; $s \leftarrow s_{aday}$;}
  for $i = 1$ to 7 **do**
    for $j = 0$ to 2 **do** {
      $s_{y_2[j]} = s_{y_2[j]}$^$((i\&(1 \ll j)) \gg j)$;
      $SET[k] \leftarrow s_{değişen}$; $M[k] \leftarrow maliyet_{değişen}$;
      $k \leftarrow k + 1$; $s \leftarrow s_{aday}$;}
  $maliyet_{min} \leftarrow M$ dizisinin en küçük $maliyet_{değişen}$ değeri;
  $s_{min} \leftarrow$ Karşılık gelen SET dizisinin $s_{değişen}$ elemanı;
  while $s_{min} \in S$ **do** {
    $maliyet_{min}$ değerini M dizisinden çıkart;
    $maliyet_{min} \leftarrow M$ dizisinin en küçük değeri;
    $s_{min} \leftarrow$ Karşılık gelen SET dizisinin $s_{değişen}$ elemanı;}
  $NL_{s_{min}} \leftarrow s_{min}$'den elde edilen doğrusal olmama değeri;
  if $NL_{s_{min}} > 16256$ **then**
    return s_{min};
  $s \leftarrow s_{min}$;
  $s_{aday} \leftarrow s$;
  $S[K] \leftarrow s$;}

Şekil 1. Sezgisel arama algoritması

(1057, 31)-aralıklı dizisinin (0'dan 1056'ya kadar numaralandırılan) sütunlarını ρ_{1057} eşdeğerlik ilişkisine göre bölüntülediğimizde ortaya çıkan 73 eşdeğerlik sınıfının her birini, eşdeğerlik sınıfını gösteren sütun numaralarının en küçüğü ile temsil edersek, bu temsilciler 0, 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, 25, 27, 33, 35, 37, 39, 41, 43, 45, 47, 49, 51, 53, 55, 57, 59, 61, 65, 71, 73, 75, 77, 81, 85, 89, 97, 99, 103, 105, 107, 109, 113, 115, 119, 121, 123, 129, 131, 151, 161, 163, 165, 171, 173, 177, 179, 181, 185, 193, 195, 197, 225, 227, 229, 243, 245, 259, 353, 361 ve 453 olarak bulunur. Böylelikle, (1057, 31)-aralıklı dizi ile temsil edilen eş güçlü bir Boole fonksiyonu f, uzunluğu 73 olan kısaltılmış doğruluk tablosu

$$s = (s_0, \dots, s_{72}) = \left(f(\omega^0), \dots, f(\omega^{361}), f(\omega^{453})\right) \quad (4)$$

ile gösterilebilir. Bu durumda, elde ettiğimiz eşitsizlik sistemi

$$13 \leq \sum_{j=0}^{72} A_{i,j} s_j \leq 20 \quad (5)$$

biçimindedir. Burada eşitsizliğin alt ve üst sınırları (3) koşulundan hesaplanmaktadır ve 73×73 büyüklüğündeki $[A_{i,j}]$ katsayı matrisini elde eden algoritmanın MATLAB kodu [22]'de verilen bağlantıda sunulmuştur.

Şekil 1'de görülen algoritma, ağırlık koşulunu sağlayan rastgele bir aday çözüm s_{aday} ile başlamakta ve her yinelemede $35 \times 35 + 7 = 1232$ komşuluk üretilmektedir. Herhangi bir yineleme girdisi s için komşuluklar (y_0 ile verilen) 0 değerine sahip 35 pozisyondan birisinin (y_1 ile verilen) 1 değerine sahip 35 pozisyondan birisi ile karşılıklı yer değiştirmesi ve geriye kalan 3 pozisyondaki bitlerin olası tüm farklı değerleri almasıyla elde edilmektedir. Her bir komşuluk için hesaplanan maliyet değeri ($maliyet_{değişen}$) M dizisine ve karşılık gelen komşuluk ($s_{değişen}$) ise SET dizisine kaydedilir. Sonrasında, daha önce yineleme çıktısı olarak üretilmemiş ve en düşük maliyete sahip komşuluk (s_{min}) için doğrusal olmama değeri $NL_{s_{min}}$ hesaplanır; eğer bu değer bükük-bağlaşım sınırından (16256) yüksekse algoritma çıktısı olarak verilir. Gerçekleştirdiğimiz aramada, en aza indirgenmeye çalışılan ve Şekil 2'de verilen algoritma ile hesaplanan maliyet değeri, herhangi bir komşuluk $s = s_{değişen}$ için (5) ile gösterilen eşitsizlik sisteminin alt ve üst sınırlarından sapmalarının kareleri toplamıdır. Maliyet değeri sıfır olan 73 bit uzunluğundaki her çözüm, bükük-bağlaşım değerinden yüksek doğrusal olmama değerine sahip bir Boole fonksiyonu temsil etmektedir.

Girdi: Kısaltılmış doğruluk tablosu s
Çıktı: s'nin maliyet değeri $maliyet_s$
for $i = 0$ to 72 **do** {
  $c \leftarrow 0$;
  for $j = 0$ to 72 **do**
    $c \leftarrow c + A_{i,j} s_j$;
  if $(c < 13)$
    $maliyet_s = maliyet_s + (c - 13)^2$;
  else if $(c > 20)$
    $maliyet_s = maliyet_s + (c - 20)^2$;}
return c;

Şekil 2. Maliyet değerinin hesaplanması

Çizelge-1: Bükük-bağlaşım sınırını aşan doğrusal olmama (DO) değerine sahip kısaltılmış doğruluk tabloları (CD: Cebirsel Derece, MG: Mutlak Gösterge, CB: Cebirsel Bağışıklık)

DO	CD	MG	CB	Kısaltılmış doğruluk tablosu
16272	10	544	7	(0111011001001001011010111000010010111100100000100111110010111010111000100)
16272	10	544	7	(0010110111110110001110111010111011000001110010001000011110100010000101001)
16271	15	548	7	(1111011001001001011010111000010010111100100000100111110010111010111000100)
16271	15	548	7	(1010110111110110001110111010111011000001110010001000011110100010000101001)
16270	10	536	7	(1011111011100011010111001110010011010010110001101000100010010001010110100)
16270	10	536	7	(1101101111111010110110001101010101100001110100101000001100000010001010110)
16269	15	292	7	(0111011111110110001111000001010010001101111000010110001010001000010010110)
16269	15	532	7	(0011111011100011010111001110010011010010110001101000100010010001010110100)
16269	15	380	7	(0110111011101110101100110000011111111001101000110001101010000100001000101)
16269	15	532	7	(0101101111111010110110001101010101100001110100101000001100000010001010110)
16269	15	228	7	(0110101001010111100110110101100101101100100011101011011100000011010001001)
16269	15	532	7	(0011111100100101111110100110101000100101000110011111000001001100001011101)
16268	10	376	7	(1110111011101110101100110000011111111001101000110001101010000100001000101)
16268	10	232	7	(1110101001010111100110110101100101101100100011101011011100000011010001001)
16268	10	536	7	(1011111100100101111110100110101000100101000110011111000001001100001011101)
16268	10	776	7	(1110010111011000100011111000010001001110001001010111101000111110111000101)

Daha önce [18] çalışmasında, S-kutularının tasarımı için kullanılan en dik iniş prensibine dayalı arama algoritmasının zaman karmaşıklığı elde edilmiştir. Benzer argümanlarla, eşdeğerlik sınıflarının sayısı $e\left(\approx \frac{2^n-1}{n(2^p-1)}\right)$ olmak üzere bir yinelemedeki komşuluk sayısı yaklaşık olarak $\left(\frac{e}{2}\right)^2$ kabul edilirse, her bir komşulukta (Şekil-2'den verilen) maliyet değerinin hesaplanması için e^2 tane çarpma işlemi gerektiğinden, bu çalışmada gerçekleştirilen en dik iniş prensibine dayalı arama algoritmasının zaman karmaşıklığı sabit bir yineleme sayısı (N) için $O(e^4)$ olarak bulunabilir. Ayrıca, yineleme çıktılarını kaydetmek için ihtiyaç duyulan bellek miktarının $N \times e$ bit olduğu görülmektedir.

4. Bulgular

Arama algoritması C programlama dilinde yazılmış ve yineleme sayısı $N = 4000$ seçilerek, Intel Xeon E5-1650 3.5GHz işlemci ve 16 GB belleğe sahip bir bilgisayarda 12000 kere koşulmuştur. Yaklaşık iki gün süren bu arama sonucunda bükük-bağlaşım sınırından yüksek doğrusal olmama değerine sahip 35 Boole fonksiyon bulunmuş, ancak bu Boole fonksiyonlardan sadece 16 tanesinin (kısaltılmış) doğruluk tablolarının birbirinden farklı oldukları gözlenmiştir. Bunlardan 4 tanesi 16268, 6 tanesi 16269 ve ikişer tanesi 16270, 16271, 16272 doğrusal olmama değerlerine sahiptir. Bulunan 16 Boole fonksiyonun kısaltılmış doğruluk tabloları Çizelge-1'de sunulmakta ve karşılık gelen 2^{15} uzunluğundaki doğruluk tabloları, eşitsizlik sistemini üreten algoritmanın kodu ile birlikte [22]'de verilmektedir.

Çizelge-1'de, elde edilen Boole fonksiyonların diğer kriptografik özellikleri cebirsel derece, cebirsel bağışıklık ve mutlak gösterge verilmektedir. Patterson ve Wiedemann tarafından keşfedilen [4] 16276 doğrusal olmama değerine sahip iki PW fonksiyonu bulunmaktadır ve her ikisinin de mutlak göstergesi 160 olmakla birlikte, birinin cebirsel derecesi ve bağışıklığı sırasıyla 9 ve 6 iken diğerinin cebirsel derecesi ve bağışıklığı sırasıyla 8 ve 7'dir. PW fonksiyonlarından başka mutlak gösterge değeri 160 veya daha iyi olan 15 değişkenli Boole fonksiyonlar literatürde bilinmemektedir. Ayrıca, tek sayıda değişkene sahip Boole fonksiyonların mutlak gösterge değerleri için bildiğimiz kadarıyla genel bir alt sınır da bilinmemektedir. Bununla birlikte, 9, 11 ve 21 değişkenli Boole fonksiyonlar için bilinen en iyi mutlak gösterge değerleri sırasıyla 24 [20], 56 [20] ve 1564'tür [6, 23]. Bunlardan ilk ikisi dengeli, sonuncusu ise dengeli olmayan Boole fonksiyonlara aittir.

PW fonksiyonları ile karşılaştırıldığında, Çizelge-1'de verilen Boole fonksiyonların cebirsel derece bakımından daha iyi oldukları, buna karşın mutlak gösterge ve doğrusal olmama açılarından ise PW fonksiyonlarının daha iyi oldukları görülmektedir. Bunun yanı sıra, Çizelge-1'de başarılan en yüksek doğrusal olmama değeri (16272), daha önce [7, 8] çalışmalarında elde edilen sonuçtan (16268) daha iyidir. Doğrusal olmama değeri tek sayı olan n değişkenli bir Boole fonksiyonun cebirsel derecesinin n olduğu bilinmektedir. Bu nedenle, Çizelge-1'deki 16271 ve 16269 doğrusal olmama değerlerine sahip Boole fonksiyonların cebirsel dereceleri 15'tir. Ayrıca, tek sayıda değişkene sahip bir Boole fonksiyonun optimum cebirsel bağışıklığa sahip olabilmesi için dengeli olması gerekmektedir [24]. Bu nedenle, PW fonksiyonları ve Çizelge-1'deki Boole fonksiyonları dengeli olmadıkları için optimum cebirsel bağışıklığa sahip değillerdir. Bahsedilen fonksiyonlar dengeli olmadıklarından esneklik özelliği göstermezler ve bu fonksiyonların hiçbirisinin korelasyon bağışıklığı özelliğine sahip olmadığı gözlenmiştir.

Çalışmamızın doğal bir uzantısı olarak (1057, 31)-aralıklı diziler ile temsil edilen 3-DSBF'ler ve 5-DSBF'ler için de arama yapılmış, fakat arama uzaylarının çok büyük olması (sırasıyla 2^{217} ve 2^{353}) nedeniyle bükük-bağlaşım sınırını aşan sonuçlar elde edilememiştir. Daha verimli arama algoritmalarının tasarlanması veya arama uzaylarının küçültülmesine olanak

sağlayan yeni yöntemlerin geliştirilmesi, literatürde ulaşılamayan doğrusal olmama değerlerinin elde edilebilmesi için önemli açık problemlerdir.

5. Sonuç

Bu çalışmada, (1057,31)-aralıklı diziler ile temsil edilen DSBF'lerin oluşturduğu ve büyüklüğü $2^{69.6}$ olan arama uzayında sezgisel arama yürütülerek, daha önce (151,217)- ve (217,151)-aralıklı diziler ile temsil edilen genelleştirilmiş DSBF'lerin oluşturdukları arama uzaylarında yapılan tam arama ve sezgisel arama yöntemlerinin ulaştığı [7, 8] doğrusal olmama değeri iyileştirilmiştir. Ayrıca, bükük-bağlaşım sınırını aşan Boole fonksiyonları literatürde esneklik, cebirsel bağışıklık, cebirsel derece ve mutlak gösterge gibi diğer kriptografik özellikler açısından güçlü Boole fonksiyonların tasarımı için kullanıldığından [10-12], elde ettiğimiz sonuçların bu yönde katkı sağlayabilecek nitelikte olduğu düşünülmektedir.

Kaynakça

[1] Ding, C., Xiao, G., Shan, W. The stability theory of stream ciphers, Springer, Berlin, 1991.

[2] Matsui, M. Linear cryptanalysis method for DES cipher, Springer, Berlin, 1994, EUROCRYPT 1993, LNCS, vol. 765, pp. 386-397.

[3] X.-D. Hou. On the norm and covering radius of the first order Reed-Muller codes, IEEE Trans. Inf. Theory, 1997, 43(3), pp. 1025-1027.

[4] Patterson, N. J., Wiedemann, D. H. The covering radius of the (215, 16) Reed-Muller code is at least 16276, IEEE Trans. Inf. Theory, 1983, 29(3), pp. 354-356.

[5] Kavut, S., Yücel, M. D. 9-variable Boolean functions with nonlinearity 242 in the generalized rotation symmetric class, Inf. Comput., 2010, 208(4), pp. 341-350.

[6] Gangopadhyay, S., Keskar, P. H., Maitra, S. Patterson-Wiedemann construction revisited, Discret. Math., 2006, 306(14), pp. 1540-1556.

[7] Kavut, S. New Patterson-Wiedemann type functions with 15 variables in the generalized rotation-symmetric class, Turk. J. Electr. Eng. Comp. Sci., 2017, 25(6), pp. 4901-4906.

[8] Kavut, S. A Modified Patterson-Wiedemann Construction Having Nonlinearity Greater Than Bent Concatenation Bound, Rostock, Germany, 2022, WCC 2022.

[9] Kavut, S., Maitra, S. Patterson-Wiedemann type functions on 21 variables with nonlinearity greater than bent concatenation bound, IEEE Trans. Inf. Theory, 2016, 62(4), pp. 2277-2282.

[10] Zhang, W.G. High-meets-low: construction of strictly almost optimal resilient Boolean functions via fragmentary Walsh spectra, IEEE Trans. Inf. Theory, 2019, 65(9), pp. 5856-5864.

[11] Sarkar, S., Maitra, S. Idempotents in the neighbourhood of Patterson-Wiedemann functions having Walsh spectra zeros, Des. Codes Cryptogr., 2008, 49, pp. 95-103.

[12] Kavut, S. Improved cryptographic properties of Boolean functions obtained from the neighbourhood of Patterson-Wiedemann functions. Cryptogr. Commun., 2023, 15, pp. 433-442.

[13] Stănică, P., Maitra, S. Rotation symmetric Boolean functions – Count and cryptographic properties, Discret. Appl. Math., 2008, 156(10), pp. 1567-1580.

[14] Pieprzyk, J., Qu, C. X. Fast hashing and rotation-symmetric functions, J. Universal Comput. Sci. 1999, 5(1) pp. 20-31.

[15] Filiol, E., Fontaine, C. Highly nonlinear balanced Boolean functions with a good correlation immunity, Springer, Berlin, 1998, EUROCRYPT 1998, LNCS, vol. 1403, pp. 475-488.

[16] Fontaine, C. On some cosets of the first-order Reed-Muller code with high minimum weight, IEEE Trans. Inf. Theory, 1999, 45(4), pp. 1237-1243.

[17] Courtois, N. T., Meier, W. Algebraic attacks on stream ciphers with linear feedback, Springer, Berlin, 2003, EUROCRYPT 2003, LNCS, vol. 2656, pp. 345-359.

[18] Kavut, S. Bazı alt uzaylarda kriptografik açıdan eniyilenmiş büyük S-kutuları, EMO Bilimsel Dergi, 2022, 12(1), pp. 43-51.

[19] Kavut, S., Yücel, M. D. Güçlü kriptografik özelliklere sahip Boole işlevleri tasarımında yeni bir algoritma, Ankara, Türkiye, 2005, 1. Ulusal Kriptoloji Sempozyumu, Bildiriler Kitabı, pp. 95-105.

[20] Kavut, S. Maitra, S., Yücel, M. D. Search for Boolean functions with excellent profiles in the rotation symmetric class, IEEE Trans. Inf. Theory, 2007, 53(5), pp. 1743-1751.

[21] Clark, J. A., Jacob, J. L. Two-stage optimisation in the design of Boolean functions, Springer, Berlin, 2000, ACISP 2000, LNCS, vol. 1841, pp. 242-254.

[22] Kavut, S. Truth tables and system of inequalities for (1057, 31)-interleaved sequences, GitHub, URL: https://github.com/Selcuk-kripto/1057_31 (Erişim tarihi: 20.11.2022).

[23] Kavut, S. Correction to the paper: Patterson-Wiedemann construction revisited, Discret. Appl. Math., 2016, 202, pp. 185-187.

[24] Dalai, D. K., Gupta, K. C., Maitra, S. Results on algebraic immunity for cryptographically significant Boolean functions, Springer, Berlin, 2004, INDOCRYPT 2004, LNCS, vol. 3348, pp. 92-106.