



**META-SEZGİSEL ALGORİTMALAR İLE
KRİPTOGRAFİK BOOLE FONKSİYONLARIN
TASARIMI**

**2024
DOKTORA TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ**

Erol ÖZÇEKİÇ

**Tez Danışmanları
Doç. Dr. Hakan KUTUCU
Prof. Dr. Selçuk KAVUT**

**META-SEZGİSEL ALGORİTMALAR İLE KRİPTOGRAFİK BOOLE
FONKSİYONLARIN TASARIMI**

Erol ÖZÇEKİÇ

**Tez Danışmanları
Doç. Dr. Hakan KUTUCU
Prof. Dr. Selçuk KAVUT**

**T.C.
Karabük Üniversitesi
Lisansüstü Eğitim Enstitüsü
Bilgisayar Mühendisliği Anabilim Dalında
Doktora Tezi
Olarak Hazırlanmıştır**

**KARABÜK
Nisan 2024**

Erol ÖZÇEKİÇ tarafından hazırlanan “META-SEZGİSEL ALGORİTMALAR İLE KRİPTOGRAFİK BOOLE FONKSİYONLARIN TASARIMI” başlıklı bu tezin Doktora Tezi olarak uygun olduğunu onaylarım.

Doç. Dr. Hakan KUTUCU

.....

Tez Danışmanı, Bilgisayar Mühendisliği Anabilim Dalı

Prof. Dr. Selçuk KAVUT

.....

Tez İkinci Danışmanı, Balıkesir Üniversitesi, Bilgisayar Mühendisliği Anabilim Dalı

Bu çalışma, jürimiz tarafından Oy Birliği ile Bilgisayar Mühendisliği Anabilim Dalında Doktora tezi olarak kabul edilmiştir. 18/04/2024

Ünvanı, Adı SOYADI (Kurumu)

İmzası

Başkan : Prof. Dr.Ahmet DEMİR (KBÜ)

.....

Üye : Prof. Dr. Murat BEKEN (İBÜ)

.....

Üye : Doç. Dr. Burhan SELÇUK (KBÜ)

.....

Üye : Doç. Dr. Önder EYECİOĞLU (İBÜ)

.....

Üye : Dr. Öğr. Üyesi Kürşat Mustafa KARAOĞLAN (KBÜ)

.....

KBÜ Lisansüstü Eğitim Enstitüsü Yönetim Kurulu, bu tez ile, Doktora derecesini onamıştır.

Doç. Dr. Zeynep ÖZCAN

.....

Lisansüstü Eğitim Enstitüsü Müdürü



“Bu tezdeki tüm bilgilerin akademik kurallara ve etik ilkelere uygun olarak elde edildiğini ve sunulduğunu; ayrıca bu kuralların ve ilkelerin gerektirdiği şekilde, bu çalışmadan kaynaklanmayan bütün atıfları yaptığımı beyan ederim.”

Erol ÖZÇEKİÇ

ÖZET

Doktora Tezi

META-SEZGİSEL ALGORİTMALAR İLE KRİPTOGRAFİK BOOLE FONKSİYONLARIN TASARIMI

Erol ÖZÇEKİÇ

Karabük Üniversitesi

Lisansüstü Eğitim Enstitüsü

Bilgisayar Mühendisliği Anabilim Dalı

Tez Danışmanları:

Doç. Dr. Hakan KUTUCU

Prof. Dr. Selçuk KAVUT

Nisan 2024, 67 sayfa

Bu çalışmada, doğrusal olmama, mutlak gösterge ve cebirsel derece gibi kriptografik özellikleri açısından güçlü olan dengeli Boole fonksiyonları bükük fonksiyonlardan üreten bir genetik arama algoritması tasarlanmıştır. Bükük fonksiyonlar doğrusal olmama ve mutlak gösterge bakımından ideal olmakla birlikte, dengeli değildir. Bu nedenle, tasarlanan genetik algoritma ile Hamming uzaklığı bakımından bükük fonksiyonlara en yakın olan dengeli fonksiyonların oluşturduğu arama uzayında sistematik bir arama gerçekleştirilmiş ve elde edilen sonuçlar literatürde evrimsel veya sezgisel algoritmalar kullanılarak bulunan en iyi sonuçlar ile karşılaştırılmıştır.

Yakın zamanda, $12 \leq n \leq 26$ için mutlak gösterge değeri $2^{n/2}$ 'den düşük olan çift sayıda n değişkene sahip dengeli Boole fonksiyonları, değişken sayısı daha büyük olan bu tür fonksiyonların sonsuz bir sınıfının inşa yöntemine dayanan sezgisel bir

arama algoritması ile üretilmiştir. Çalışmamızda, Hamming uzaklığı açısından büyük fonksiyonlara en yakın olan dengeli Boole fonksiyonların oluşturduğu arama uzayında kriptografik özellikleri optimize etmeyi amaçlayan bir genetik algoritma tasarlanmış ve bunun sonucunda n 'nin tüm bu değerleri için daha iyi mutlak gösterge değerleri literatürde ilk defa elde edilmiştir. Bununla birlikte, $16 \leq n \leq 26$ için elde ettiğimiz Boole fonksiyonların doğrusal olmama değerlerinin $2^{n-1} - 2^{n/2}$ 'den büyük olduğu gözlemlenmiştir. Ayrıca, arama stratejimiz $8 \leq n \leq 16$ için literatürde bilinen en yüksek doğrusal olmama değerine sahip dengeli Boole fonksiyonları üretmiştir.

Anahtar Sözcükler : Boole fonksiyon, Doğrusal olmama, Genetik algoritma, Parçacık sürü algoritması, Mutlak gösterge.

Bilim Kodu : 92403

ABSTRACT

Ph. D. Thesis

DESIGN OF CRYPTOGRAPHIC BOOLEAN FUNCTIONS WITH META-HEURISTIC ALGORITHMS

Erol ÖZÇEKİÇ

**Karabük University
Institute of Graduate Programs
Department of Computer Engineering**

Thesis Advisors:

Assoc. Prof. Dr. Hakan KUTUCU

Prof. Dr. Selçuk KAVUT

April 2024, 67 pages

In this thesis, a genetic search algorithm is designed that generates balanced Boolean functions that are strong in terms of cryptographic properties such as nonlinearity, absolute indicator and algebraic degree from bent functions. Although the bent functions are optimal in terms of nonlinearity and absolute indicator, they are not balanced. For this reason, with the designed genetic algorithm, a systematic search is carried out in the search space formed by the balanced functions closest to the bent functions in terms of Hamming distance, and the results that we obtain are compared with the best results found in the literature using evolutionary or heuristic algorithms.

Recently, balanced Boolean functions with an even number n of variables achieving absolute indicator less than $2^{n/2}$ have been obtained for $12 \leq n \leq 26$ by exploiting a heuristic search algorithm that is based on the construction method of an infinite

class of such functions for higher number of variables. We here design a genetic algorithm aiming to optimize the cryptographic properties of the balanced Boolean functions that are closest to the bent functions in terms of Hamming distance and, consequently, we obtain better absolute indicator values for all of those values of n for the first time in the literature. We also observe that among our results, the functions for $16 \leq n \leq 26$ have nonlinearity greater than $2^{n-1} - 2^{n/2}$. Further, our search strategy produces balanced Boolean functions with the best-known nonlinearity for $8 \leq n \leq 16$.

Key Word : Boolean function, Nonlinearity, Genetic algorithm, Particle swarm algorithm, Absolute indicator.

Science Code : 92403

TEŞEKKÜR

İlk olarak tez çalışmam sırasında bana yardımlarından ve katkılarından dolayı değerli hocam ve danışmanım Doç. Dr. Hakan KUTUCU hocama sonsuz teşekkürlerimi sunmak isterim.

Tez çalışmasının her aşamasında, deneyimleri, bilgisi ve nezaketi ile teze yön veren eş danışmanım Prof. Dr. Selçuk KAVUT hocama; tez süresince yardım severliği ve anlayışları için bana sürekli destek olan eşime ve aileme teşekkür ve saygılarımı sunarım.

İÇİNDEKİLER

	<u>Sayfa</u>
KABUL	ii
ÖZET.....	iv
ABSTRACT.....	vi
TEŞEKKÜR.....	viii
İÇİNDEKİLER	ix
ŞEKİLLER DİZİNİ.....	ixi
ÇİZELGELER DİZİNİ	xiv
SİMGELER VE KISALTMALAR DİZİNİ	xvi
BÖLÜM 1	1
GİRİŞ	1
1.1. LİTERATÜR ÖZETİ	3
1.2. ÇALIŞMANIN LİTERATÜRE KATKILARI	5
BÖLÜM 2	8
BOOLE FONKSİYONLARIN TEMEL KRİPTOGRAFİK ÖZELLİKLERİ.....	8
BÖLÜM 3	11
GENETİK ALGORİTMA	11
BÖLÜM 4	16
GA PARAMETRELERİNİN SEÇİMİ VE BAŞARIM DEĞERLENDİRMESİ	16
4.1. POPÜLASYON BÜYÜKLÜKLERİ	16
4.2. MUTASYON OLASILIKLARI.....	17
4.2.1. 8 değişkenli Boole fonksiyonlar	18
4.2.2. 10 değişkenli Boole fonksiyonlar	21
4.3. SIFIRLAMA	23
4.3.1. 8 değişkenli Boole fonksiyonlar	23

Sayfa

4.3.2. 10 deęişkenli Boole fonksiyonlar	25
4.4. NESİL SAYISI.....	27
4.4.1. 8 deęişkenli Boole fonksiyonlar	27
4.4.2. 10 deęişkenli Boole fonksiyonlar	30
4.5. BAŞARIM DEĞERLENDİRMESİ	32
 BÖLÜM 5	40
ARAMA ÇALIŞMASI	40
 BÖLÜM 6	43
PARÇACIK SÜRÜ OPTİMİZASYONU ALGORİTMASI	43
 BÖLÜM 7	48
7.1. PARÇACIK SÜRÜSÜ OPTİMİZASYONU KAVRAMLARI.....	48
7.1.1 Parçacıklar	48
7.1.2. Sürü	48
7.1.3 Uygunluk Fonksiyonu	49
7.1.4. Kişisel En İyi Deęer	49
7.1.5. Küresel (Global) En İyi Deęer.....	49
7.1.6. Atalet Aęırlığı.....	49
7.1.7. Hız Deęeri.....	50
7.1.8. Hızlandırma Katsayıları.....	50
7.1.9 Sonlandırma Kriteri	50
7.2. PARÇACIK SÜRÜSÜ OPTİMİZASYONU ARAMA SONUÇLARI	51
SONUÇLAR	57
KAYNAKLAR	60
 EK AÇIKLAMALAR A.	65

ÖZGEÇMİŞ	68
----------------	----



ŞEKİLLER DİZİNİ

Sayfa

Şekil 3.1. Genetik algoritma yapısı	12
Şekil 3.2. Bir biçimli çaprazlama algoritması	13
Şekil 4.1. Çizelge 4.2'deki dağılımların doğrusal olmama için aynı sırada karşılık gelen kutu grafikleri	18
Şekil 4.2. Çizelge 4.2'deki dağılımların mutlak gösterge için aynı sırada karşılık gelen kutu grafikleri	20
Şekil 4.3. Çizelge 4.2'deki dağılımların cebirsel derece için aynı sırada karşılık gelen kutu grafikleri	20
Şekil 4.4. 10 değişkenli durumda (a) 0, (b) 0.002, (c) 0.05, (d) 0.1, (e) 0.15 ve (f) 0.2 mutasyon olasılıklarının her biri için doğrusal olmama özelliğine göre elde edilen kutu grafikleri	21
Şekil 4.5. 10 değişkenli durumda (a) 0, (b) 0.002, (c) 0.05, (d) 0.1, (e) 0.15 ve (f) 0.2 mutasyon olasılıklarının her biri için mutlak gösterge özelliğine göre elde edilen kutu grafikleri	22
Şekil 4.6. 10 değişkenli durumda (a) 0, (b) 0.002, (c) 0.05, (d) 0.1, (e) 0.15 ve (f) 0.2 mutasyon olasılıklarının her biri için cebirsel derece özelliğine göre elde edilen kutu grafikleri	22
Şekil 4.7. Çizelge 4.3'teki dağılımların doğrusal olmama için aynı sırada karşılık gelen kutu grafikleri	24
Şekil 4.8. Çizelge 4.3'teki dağılımların mutlak gösterge için aynı sırada karşılık gelen kutu grafikleri	24
Şekil 4.9. Çizelge 4.3'teki dağılımların cebirsel derece için aynı sırada karşılık gelen kutu grafikleri	25
Şekil 4.10. Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için doğrusal olmama özelliğine göre elde edilen kutu grafikleri	26
Şekil 4.11. Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için mutlak gösterge özelliğine göre elde edilen kutu grafikleri	26
Şekil 4.12. Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için cebirsel derece özelliğine göre elde edilen kutu grafikleri	27
Şekil 4.13. Çizelge 4.4'teki dağılımların doğrusal olmama için aynı sırada karşılık gelen kutu grafikleri	29
Şekil 4.14. Çizelge 4.4'teki dağılımların mutlak gösterge için aynı sırada karşılık gelen kutu grafikleri	29

Şekil 4.15. Çizelge 4.4'teki dağılımlarının cebirsel gösterge için aynı sırada karşılık gelen kutu grafikleri.....	30
Şekil 4.16. Maksimum nesil sayısının (a) 5000, (b) 10000, (c) 15000 ve (d) 20000 olduğu durumlar için doğrusal olmama özelliğine göre elde edilen kutu grafikleri.....	31
Şekil 4.17. Maksimum nesil sayısının (a) 5000, (b) 10000, (c) 15000 ve (d) 20000 olduğu durumlar için mutlak gösterge özelliğın egöre elde edilen kutu grafikleri.....	31
Şekil 4.18. Maksimum nesil sayısının (a) 5000, (b) 10000, (c) 15000 ve (d) 20000 olduğu durumlar için cebirsel derece özelliğine göre elde edilen kutu grafikleri.....	32
Şekil 4.19. 8 değişkenli Boole fonksiyonlar durumunda doğrusal olmama dağılımı.....	33
Şekil 4.20. 10 değişkenli Boole fonksiyonlar durumunda doğrusal olmama dağılımı.....	34
Şekil 4.21. 12 değişkenli Boole fonksiyonlar durumunda doğrusal olmama dağılımı.....	34
Şekil 4.22. 8 değişkenli Boole fonksiyonlar durumunda mutlak gösterge dağılımı.....	35
Şekil 4.23. 10 değişkenli Boole fonksiyonlar durumunda mutlak gösterge dağılımı.....	35
Şekil 4.24. 12 değişkenli Boole fonksiyonlar durumunda mutlak gösterge dağılımı.....	36
Şekil 6.1. Parçacık Sürüşü Optimizasyonu Algoritma Yapısı.....	45
Şekil 6.2. Parçacık Sürüşü Optimizasyonu Sıfırlama Adım Grafiğı.....	54
Şekil 6.3. Parçacık Sürüşü Optimizasyonu Sıfırlama Adımı Uygulanmayan Grafik.....	55

ÇİZELGELER DİZİNİ

Sayfa

Çizelge 4.1.	Bir kombinasyonun (başlangıç popülasyon boyutu, seçim boyutu, ebeveyn popülasyon boyutu) üçlüsü ile temsil edildiği 10 ve 12 değişkenli Boole fonksiyonları için bilinen en iyi doğrusal olmama değerlerini veren kombinasyonlar	17
Çizelge 4.2.	Farklı mutasyon olasılıkları için 8 değişkenli 200000 Boole fonksiyonun kriptografik özelliklere göre dağılımı.....	19
Çizelge 4.3.	Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için 8 değişkenli 200000 Boole fonksiyonun kriptografik özelliklerine göre dağılımları.....	23
Çizelge 4.4.	Farklı maksimum nesil sayıları için 8 değişkenli Boole fonksiyonun kriptografik özelliklerine göre dağılımları28	
Çizelge 4.5.	n -değişkenli Boole fonksiyonları için dağılımları Şekil 4.19-4.24'te verilen doğrusal olmama değerlerinin ortalamaları (μ) ve standart sapmaları (σ), burada $n = 8, 10$ ve 12 'dir	38
Çizelge 4.6.	n -değişkenli Boole fonksiyonları için dağılımları şekil 4.19-4.24'te verilen mutlak gösterge değerlerinin ortalamaları (μ) ve standart sapmaları (σ), burada $n = 8, 10$ ve 12 'dir	38
Çizelge 5.1.	Deneysel parametre değerleri.....	40
Çizelge 5.2.	100 nesil için tüketilen süreler ve dengeli fonksiyonların sayısı.....	40
Çizelge 5.3.	Bükük fonksiyonun komşuluğunda doğrusal olmama değeri 116 olan dengeli Boole fonksiyonlarının sınıflandırılması	41
Çizelge 5.4.	f bükük fonksiyonunu üreten $\omega^{(i)}$ vektörleri, $i = 1, 2, \dots, 16$	41
Çizelge 6.1.	Elde ettiğimiz en iyi profillerin literatürdeki en iyi sonuçlarla karşılaştırılması (herhangi bir f Boole fonksiyonun profili ($Nl_f; \Delta_f; d_f$) üçlüsü ile gösterilmektedir.)	43
Çizelge 6.2.	8 (Standart PSO), 8 (PSO Luca) - 8 (PSO Luca-Reset), 10 (PSO Luca) - 10 (PSO Luca - Reset), 12 (PSO Luca) değişkenli Boole fonksiyonları için bilinen en iyi doğrusal olmama değerlerini veren kombinasyonlar... ..	60
Çizelge 6.3.	PSO deneysel parametre değerleri.....	61
Çizelge 6.4.	200 parçacık için tüketilen süreler ve dengeli fonksiyonların sayısı... ..	61

Çizelge 6.5. Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için 8 değişkenli 38699837 Boole fonksiyonu ile 8 değişkenli 4514024 Boole fonksiyonu kriptografik özelliklerine göre dağılımları.....	62
Çizelge 6.6. Sıfırlama adımının (PSO Luca-Reset) uygulandığı ve (PSO Luca) uygulanmadığı en iyi durumlar için 10 ve 12 değişkenli Boole fonksiyonlarının kriptografik özelliklerine göre dağılımları.	64
Çizelge 7.1. Elde ettiğimiz en iyi GA profillerin literatürdeki en iyi sonuçlarla karşılaştırılması (Herhangi bir f Boole fonksiyonun profili (Nlf ; Δf ; df) üçlüsü ile gösterilmektedir.).....	66
Çizelge 7.2. Elde ettiğimiz en iyi PSO profillerin literatürdeki en iyi sonuçlarla karşılaştırılması (Herhangi bir f Boole fonksiyonun profili (Nlf ; Δf ; df) üçlüsü ile gösterilmektedir.).....	67
Çizelge 7.3. Elde ettiğimiz en iyi GA ve PSO profillerin karşılaştırılması (Herhangi bir f Boole fonksiyonun profili (Nlf ; Δf ; df) üçlüsü ile gösterilmektedir.).....	67
Çizelge 7.1. 8, 10 ve 12 değişkenli Boole fonksiyonları için bilinen en iyi doğrusal olmama değerlerini veren tüm kombinasyonlar.	67
Çizelge 7.2. 8 (Standart PSO), 8 (PSO Luca) - 8 (PSO Luca-Reset), 10 (PSO Luca) - 10 (PSO Luca - Reset), 12 (PSO Luca) değişkenli Boole fonksiyonları için bilinen en iyi doğrusal olmama değerlerini veren kombinasyonlar.....	67
Çizelge 7.3. PSO deneysel parametre değerleri..	67
Çizelge 7.4. 200 parçacık için tüketilen süreler ve dengeli fonksiyonların sayısı....	67
Çizelge 7.5. Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için 8 değişkenli 38699837 Boole fonksiyonu ile 8 değişkenli 4514024 Boole fonksiyonu kriptografik özelliklerine göre dağılımları..	67
Çizelge 7.6. Sıfırlama adımının (PSO Luca-Reset) uygulandığı ve (PSO Luca) uygulanmadığı en iyi durumlar için 10 ve 12 değişkenli Boole fonksiyonlarının kriptografik özelliklerine göre dağılımları.	67
Çizelge 7.7. Elde ettiğimiz en iyi GA profillerin literatürdeki en iyi sonuçlarla karşılaştırılması.	67
Çizelge 7.8. Elde ettiğimiz en iyi PSO profillerin literatürdeki en iyi sonuçlarla karşılaştırılması.....	67
Çizelge 7.9. Elde ettiğimiz en iyi GA ve PSO profillerin karşılaştırılması	67

SİMGELER VE KISALTMALAR DİZİNİ

SİMGELER

NL_f : doğrusal olmama
 Δ_f : mutlak gösterge
 d_f : cebirsel derece
 W_f : Walsh-Hadamard dönüşümü
 r_f : özilinti fonsiyonu
 d : Hamming uzaklığı
 wt : Hamming ağırlığı
 GF : Galois cismi

KISALTMALAR

GA : Genetik Algoritma
MM : Maiorana-McFarland
PSO : Particle Swarm Optimization

BÖLÜM 1

GİRİŞ

Bir kriptosistemin güvenliği, Shannon [1] tarafından ortaya konulan karmaşıklık ve yayılma ilkelerinin sağlanmasına bağlıdır. Boole fonksiyonları, bu ilkelerin başarılması amacıyla simetrik kriptografide kullanılan önemli yapıtaşlarıdır; blok şifrelerde yerleştirme kutularını oluştururken, akan şifrelerde ise doğrusal olmayan filtre veya birleştirici olarak kullanılmaktadırlar. Karmaşıklık ilkesi, kapalı metin ile açık metin ve gizli anahtar arasındaki cebirsel ilişkinin olabildiğince karmaşık olması gerektiğini, yayılma ilkesi ise açık metine veya gizli anahtara uygulanan herhangi bir değişikliğin kapalı metinde tahmin edilemez bir farklılığa yol açması gerektiğini ifade eder. Kriptografik açıdan güçlü bir Boole fonksiyonun sahip olması gereken birçok kriptografik özellik bulunmaktadır ve genellikle bir özelliği iyileştirmek başka bir özelliğin kötüleşmesine yol açabilmektedir. Çalışmamızda, bahsedilen kriptografik özelliklerin en önemlilerinden doğrusal olmama, mutlak gösterge, cebirsel derece ve dengelilik ele alınmıştır. Kriptosistemde kullanılan bir Boole fonksiyonun karmaşıklık prensibi açısından yüksek doğrusal olmama ve yüksek cebirsel dereceye sahip olması, yayılma prensibi açısından ise mutlak gösterge değerinin düşük olması ve dengeli olması gerekmektedir. Düşük mutlak gösterge akan şifrelerde farksal ve hata saldırılarına [2, 3] karşı dayanıklılık sağlarken, yüksek doğrusal olmama ve yüksek cebirsel derece özellikleri akan şifrelerde sırasıyla hızlı korelasyon saldırısına [4] ve Berlekamp-Massey algoritmasına [5] karşı, blok şifrelerde ise sırasıyla doğrusal kriptanalize [6] ve yüksek mertebeden farksal kriptanalize [7] karşı kriptosistemin dayanıklılığını artırır.

Dengelilik ve yüksek doğrusal olmama özellikleri gibi kriptografik kriterlerin birbiriyle çelişebilen doğasından ve (n değişkenli Boole fonksiyonlar için 2^n olan) arama uzayının çok büyük olmasından dolayı en iyi kriptografik özelliklere sahip Boole fonksiyonların tasarımı, simetrik kriptografi literatüründe önemli ve aktif bir

araştırma problemidir. Genel olarak, güçlü kriptografik özelliklere sahip Boole fonksiyonların tasarımı sezgisel optimizasyon veya cebirsel inşa yöntemleri ile gerçekleştirilebilmektedir. Cebirsel inşa yöntemlerinin temel avantajı, özellikle büyük değişken sayısına sahip kriptografik Boole fonksiyonların tasarlanabilmesidir; bununla birlikte, bu tür inşaların sayısı ilgili literatürde azdır [8]. Sezgisel arama yöntemleri ise (değişken sayısı arttıkça arama uzayı çok fazla büyüdüğünden, büyük değişken sayıları için verimsizleşmesine rağmen) özellikle işlemci ve bellek kapasitelerinin sınırlı olduğu hafif sıklet kriptografide kullanılabilen daha küçük değişken sayılarına sahip Boole fonksiyonlarını cebirsel inşa yöntemleri ile karşılaştırıldığında çok daha fazla sayıda üretebilmektedirler. Ayrıca, literatürde cebirsel inşa yöntemlerinin sezgisel arama ile birlikte kullanılması kriptografik açıdan çok önemli bazı Boole fonksiyonların elde edilmesini sağlamıştır [9, 10].

n değişkenli bir Boole fonksiyonu için, n sayısı çift iken en yüksek doğrusal olmama değeri $2^{n-1} - 2^{n/2-1}$ 'dir ve bu doğrusal olmama değerine sahip Boole fonksiyonları büyük fonksiyonlar olarak isimlendirilir (n sayısı tek iken $n \geq 9$ için en yüksek doğrusal olmama değerinin üst sınırı $2\lfloor 2^{n-2} - 2^{n/2-2} \rfloor$ olarak verilmekte [11], fakat bu değere sahip Boole fonksiyonlarının olup olmadığı literatürde bilinmemektedir). Büyük fonksiyonlar en yüksek doğrusal olmama değerine sahip olmakla birlikte dengeli değildirler (doğruluk tablosundaki 0'ların sayısı 1'lerin sayısına eşit olan Boole fonksiyonlarına dengeli denir). Özel olarak, n değişkenli bir büyük fonksiyonu dengeli hale getirmek için doğruluk tablosundaki en az $2^{n/2-1}$ tane bitin tümleyenini almak gerekmektedir. Bu işlemin sonucunda ise doğrusal olmama değeri kaçınılmaz olarak bozulmaktadır. n değişkenli dengeli Boole fonksiyonların sahip olduğu en yüksek doğrusal olmama değeri $n \geq 8$ için literatürde bilinmemektedir ve n sayısı çift iken Dobbertin sanıtı [12] bu değer $2^{n-1} - 2^{n/2} + \text{nlb}(n/2)$ olduğunu belirtmektedir, burada $\text{nlb}(n/2)$, $n/2$ değişkenli dengeli Boole fonksiyonların sahip olduğu en yüksek doğrusal olmama değeridir.

Aşağıda, Boole fonksiyon tasarımı için literatürde kullanılan sezgisel arama yöntemleri ve bu yöntemlerden elde edilen en iyi kriptografik özellikler sunulmuştur.

1.1. LİTERATÜR ÖZETİ

1997 yılında Millan vd. [13, 14] tarafından evrimsel arama yönteminin kriptografik Boole fonksiyonlarının tasarımında tepe tırmanma ve genetik algoritma kullanılarak ilk kez uygulanmasından bu yana, birçok araştırmacı farklı arama yöntemleri ile güçlü kriptografik özelliklere sahip Boole fonksiyonlarının elde edilmesi problemini ele almıştır. Millan ve ark. uyguladıkları genetik algoritmayı [13], arama uzayını sadece dengeli Boole fonksiyonları ile sınırlayacak ve iki adımlı tepe tırmanma algoritması [14] ile birleştirecek şekilde geliştirmişlerdir [15].

Clark ve Jacob [16], tepe tırmanma ile takip edilen tavlama benzetimi algoritması şeklinde tanımladıkları iki aşamalı optimizasyon yöntemi kullanarak, Millan ve ark. tarafından elde edilen sonuçları [15] iyileştirmişlerdir. Clark ve Jacob [16], tavlama benzetimi algoritmasından elde edilen Boole fonksiyonuna tepe tırmanma algoritması ile doğrusal olmama yönünden yerel optimizasyon uygulamışlardır. Kullanılan tavlama benzetimi algoritmasının maliyet fonksiyonu ise, üretilen herhangi bir Boole fonksiyonu için, (en yüksek doğrusal olmama değerine sahip) bükük fonksiyonların sahip olduğu Walsh-Hadamard spektrumundan mutlak değerce sapmalarının tümü hesaba katılacak şekilde belirlenmiştir.

Clark ve ark. [17], ayarlama parametresine sahip daha genel bir maliyet fonksiyonu kullanarak daha önce Clark ve Jacob [16] tarafından kullanılan iki aşamalı optimizasyon yöntemini, doğrusal olmama yönünden yerel optimizasyonla birlikte mutlak gösterge yönünden yerel optimizasyon da gerçekleştirerek uygulamışlar ve Clark ve Jacob [16] çalışmasında bulunan sonuçları iyileştirmişlerdir. Kavut ve Yücel [18], ayarlama parametresi olmayan ve Walsh-Hadamard spektrumunun yanı sıra, otokorelasyon spektrumunu da hesaba katan bir maliyet fonksiyonu kullanarak, tavlama benzetimine dayalı iki aşamalı ve üç aşamalı arama yöntemleri ile, Clark ve ark. [17] çalışmasındaki sonuçların mutlak gösterge değerlerini iyileştirmişlerdir.

Yukarıda bahsedilen arama yöntemleri, rasgele üretilen herhangi bir Boole fonksiyonun kriptografik özelliklerini iyileştirmeye çalışmaktadır. Burnett [19] ise doktora tezinde, geri-izleme yapılabilen ve önceden belirlenen bir doğrusal olmama

değerinin altına düşmeyecek şekilde rasgele seçilen bir bükük fonksiyonu dengeli hale getiren bir arama algoritması tasarlamıştır. Bu yöntem, uygulaması basit olmakla birlikte önceki yöntemlerin tümünden daha iyi sonuçlar vermiştir.

Izbenko ve ark. [20], (Burnett [19] çalışmasında olduğu gibi) rasgele seçilen bükük fonksiyonları başlangıç fonksiyonları olarak kullanmışlar ve doğrusal olmama değerini düşüren belirli sayıda bit değişikliğine izin veren tepe tırmanmaya dayalı bir arama yöntemi ile bükük fonksiyonları dengeli hale getirmişlerdir. Bunun sonucunda elde edilen sonuçlar, Burnett [19] çalışmasındaki sonuçlarla doğrusal olmama değerleri açısından aynıdır.

Mariot ve Leporati [21], parçacık pozisyonlarının bir Boole fonksiyonunun doğruluk tablosu olarak yorumlandığı ayrık parçacık sürü optimizasyonu yöntemini tepe tırmanma ile birleştirerek ve maliyet fonksiyonunu doğrusal olmama değeri ile mutlak gösterge değerinin farkı şeklinde seçerek tasarladıkları arama algoritmasını dengeli Boole fonksiyonlarına uygulamışlardır. Bu çalışmada elde edilen sonuçlar, daha önceki çalışmalarda bulunan sonuçları iyileştirememiştir.

Yakın zamanda, Behera ve Gangopadhyay [22], Gower'ın ikinci mertebeden normunun [23] maliyet fonksiyonu olarak seçildiği ve genetik algoritma ile birlikte yerel aramanın da gerçekleştirildiği bir hibrit arama yöntemini uygulamışlardır. Bu çalışmada, hem dengeli Boole fonksiyonları hem de bükük fonksiyonlar arama algoritmasının başlangıç fonksiyonları olarak kullanılmış ve sonraki durumda daha iyi sonuçların elde edildiği gözlenmiştir. Elde edilen en iyi sonuçlar, [19] ve [20] çalışmalarındaki sonuçlarla doğrusal olmama değerleri açısından aynıdır. Bununla birlikte, [19] çalışmasındaki sonuçların mutlak gösterge değerleri bakımından [20] ve [22] çalışmalarında bulunan sonuçlardan daha iyi olduğu görülmektedir.

Çift değişken sayısına sahip n değişkenli dengeli Boole fonksiyonlarının bilinen en yüksek doğrusal olmama değeri $2^{n-1} - 2^{n/2} + n \log(n/2)$, Dobbertin'in [12] çalışmasında normal bir bükük fonksiyonun ($2^{n/2}$ uzunluğunda) tümüyle sıfır bloğunun dengeli hale getirilmesiyle sağlanmıştır; bu işlem, gerçekte bir bükük fonksiyonu dengeli hale getirmek için gereken minimum bit değişikliği sayısını ($2^{n/2-1}$) sağlamaktadır.

Ancak, iyi bilindiği üzere, [12] çalışmasındaki bu inşanın sahip olduğu mutlak gösterge değerlerinden daha iyi mutlak gösterge değerlerine sahip yüksek doğrusal olmama değerine sahip Boole fonksiyonları mevcuttur. Bu doğrultuda, çift n için dengeli bir Boole fonksiyonunun maksimum mutlak göstergesinin $2^{n/2}$ 'den az olamayacağı sanıtı ortaya konulmuştur [24]. Bu sanıt, ilk olarak [25] çalışmasında $n = 14$ için başlangıç fonksiyonu olarak rastgele üretilmiş bir bükük fonksiyonla başlayan sezgisel bir arama yöntemi kullanılarak çürütülmüştür. Bundan kısa bir süre sonra, aynı sanıt 10 değişkenli döngüsel simetrik Boole fonksiyonları sınıfında en dik iniş prensibine dayalı bir arama yöntemi uygulanarak, $n = 10$ için [9] çalışmasında çürütülmüştür. Bu iki arama sonucunun dışında, mutlak göstergesi $2^{n/2}$ 'den küçük olan n değişkenli dengeli Boole fonksiyonlarının teorik inşaları yakın zamanda [26] ve [27] çalışmalarında sırasıyla $n \geq 46$ ($n \equiv 2 \pmod{4}$) ve $n \geq 52$ ($n \equiv 0 \pmod{4}$) için elde edilmiştir. Ayrıca, [26] çalışmasında, tasarlanan inşanın ürettiği Boole fonksiyonları uygun şekilde değiştirilerek, $n = 18, 22$ ve 26 için mutlak göstergesi $2^{n/2}$ 'den küçük olan n değişkenli dengeli Boole fonksiyonları elde edilmiştir. Daha sonra, [27] çalışmasında en dik iniş prensibine dayalı arama yönteminin kullanılmasıyla, [26] çalışmasındaki sonuçlar daha da geliştirilmiş ve $n = 12, 14, 16, 20, 24$ için daha fazla örnek sağlanmıştır. [26] ve [27] çalışmalarında elde edilen Boole fonksiyonları, Dillon bükük fonksiyonunun [28] ($2^{n/2+1}$ bit uzunluğunda) iki bloğunun değiştirilmesiyle oluşturulmuştur.

1.2. ÇALIŞMANIN LİTERATÜRE KATKILARI

Yukarıdaki tartışmadan da anlaşılacağı üzere, mutlak göstergesi $2^{n/2}$ 'den küçük olan çift sayıda n değişkenine sahip dengeli Boole fonksiyonları, çoğunlukla bükük fonksiyonların modifiye edilmesiyle üretilir. Çalışmamızda, bu tür dengeli Boole fonksiyonları üretmek için tasarladığımız genetik algoritma (diğer çalışmalarda olduğu gibi) bükük fonksiyonlardan faydalanmaktadır; ancak, aşağıdaki gibi bazı önemli farklılıklar bulunmaktadır.

- Aramamız, bükük bir fonksiyondan $2^{n/2-1}$ uzaklığında olan dengeli Boole fonksiyonları arasında gerçekleştirilir ve bu nedenle, örneğin [25] çalışması

ile karşılaştırıldığında, arama sırasında dengelilik özelliğini elde etmeye çalışmamız gerekmez.

- Her ne kadar [12] çalışmasındaki inşadan üretilen Boole fonksiyonları aynı uzaklığa sahip olsa da, arama stratejimiz ilgili bit değişikliklerini bükük bir fonksiyonun belirli bir bloğuyla sınırlamaz.
- Teorik bir insanın koşulları ile (örneğin, [26, 27] çalışmalarında olduğu gibi) sınırlanmamaktadır; bunun yerine, aramamız daha geneldir ve arama uzayı, Hamming mesafesi açısından bükük bir fonksiyona en yakın olan tüm dengeli Boole fonksiyonlarıdır.

Burada, ele aldığımız n -değişkenli dengeli Boole fonksiyonları için, daha önce [20] çalışmasında $n = 8, 10$, ve 12 için değiştirilmiş bir tepe tırmanma yöntemi uygulanmıştır. Buna ek olarak, bu değişken sayıları için bükük fonksiyonlar, [22] çalışmasında hibrit bir genetik algoritmanın başlangıç popülasyonunu oluşturmak için kullanılmış ve bu popülasyon, bükük fonksiyonlara olan uzaklığı sınırlamadan, dengeli Boole fonksiyonları oluşturmak için kullanılmıştır. Bizim yaklaşımımız temel olarak [20] çalışmasında kullanılan arama uzayına, çift sayıda $n (\in [8, 26])$ değişkene sahip dengeli Boole fonksiyonlar için küresel bir optimizasyon algoritması uygulamakta ve bu da ilgili literatürde elde edilenlerden daha iyi kriptografik özellikler sağlamaktadır. Özel olarak, bulduğumuz mutlak göstergeler $n \geq 12$ için bilinen en iyi değerleri iyileştirmekte ve bu mutlak göstergelere sahip Boole fonksiyonları $n \geq 16$ için $2^{n-1} - 2^{n/2}$ 'den daha büyük doğrusal olmama değerlerini elde etmektedir. Ayrıca, çalışmamızda bilinen en iyi doğrusal olmama değerleri $n \geq 16$ için elde edilmiştir.

Günümüze kadar birçok araştırmacı, birden fazla kriptografik özelliği karşılayan çeşitli boyutlarda Boole fonksiyonları tasarlamak için farklı metasezgisel teknikleri (yerel arama, tavlama benzetimi, parçacık sürüsü optimizasyonu, genetik algoritma, genetik programlama gibi) araştırmışlardır. İlgili literatürde, çalışmaların çoğu değişken sayısı en fazla 16 olan Boole fonksiyonlarını ele almaktadır ve eniyilenmesi amaçlanan en yaygın kriptografik özellikler dengelilik, doğrusal olmama ve mutlak göstergedir. Kriptografik Boole fonksiyonlarının tasarımına yönelik metasezgisel algoritmaların yakın tarihli bir incelemesi [29] çalışmasında bulunmaktadır.

Bir sonraki bölümde, Boole fonksiyonlarının temel kriptografik özellikleri sunulacaktır. Boole fonksiyonlarının daha kapsamlı bir incelemesi ve tartışması için [8, 30] çalışmaları kaynak referanslar olarak kullanılabilir. Daha sonra, Bölüm 3'te çalışmamızda kullandığımız genetik algoritma ve arama sırasında büyük bir fonksiyona olan mesafeyi sabit tutan arama stratejimiz anlatılmaktadır. Genetik algorithmada kullanılan deneysel parametrelerin belirlenmesini sağlayan istatistiksel çıkarımlar ve genetik aramanın başarımlarını değerlendirilmesi Bölüm 4'te sunulmaktadır. Genetik aramanın yürütülmesinde kullanılan bilgisayar sistemi, hesaplama süresi gibi gerçekleştirme bilgilerinin sunulduğu ve rastgele arama algoritması ile karşılaştırılmasının yapıldığı Bölüm 5'ten sonra, Bölüm 6'da Parçacık Sürü Optimizasyonu ve Algoritması, Bölüm 7'de Parçacık Sürü Optimizasyonu Kavramları ve buna ait arama sonuçlarına değinildikten sonra Bölüm 8'de genel sonuçlar sunulmaktadır.

BÖLÜM 2

BOOLE FONKSİYONLARIN TEMEL KRİPTOGRAFİK ÖZELLİKLERİ

n -değişkenli bir Boole fonksiyonu $f : GF(2)^n \rightarrow GF(2)$, n giriş bitini bir çıkış bitine yollayan bir fonksiyon olarak tanımlanır ve 2^n uzunluğundaki bitlerden oluşan doğruluk tablosuyla eşsiz olarak ifade edilebilir. Bir f Boole fonksiyonunun Hamming ağırlığı $wt(f)$ doğruluk tablosundaki 1'lerin sayısı, aynı değişken sayısına sahip herhangi iki Boole fonksiyonu f ve g arasındaki Hamming uzaklığı $d(f, g)$ ise birbirinden farklı çıkış bitleri veren giriş vektörlerinin sayısıdır (diğer bir ifadeyle, $d(f, g) = wt(f \oplus g)$). Dengeli bir Boole fonksiyonu, doğruluk tablosunda 0'ların ve 1'lerin sayısı birbirine eşit olan bir Boole fonksiyonu olarak tanımlanır; başka bir deyişle, n -değişkenli dengeli bir Boole fonksiyonunun Hamming ağırlığı 2^{n-1} 'dir.

$w = (w_1, \dots, w_n)$, $x = (x_1, \dots, x_n) \in GF(2)^n$ ve $c \in GF(2)$ olmak üzere, $f(x) = w \cdot x \oplus c = w_1x_1 \oplus w_2x_2 \oplus \dots \oplus w_nx_n \oplus c$ fonksiyonu afin fonksiyon, $c = 0$ olması durumunda ise doğrusal fonksiyon olarak adlandırılır, burada $w \cdot x$, w ve x vektörlerinin iç çarpımıdır. n -değişkenli herhangi bir f Boole fonksiyonunun Eşitlik 2.1 ile verilen Walsh-Hadamard dönüşümü $W_f(w)$, doğrusal fonksiyon $w \cdot x$ ile korelasyonu veren ve $[-2^n, 2^n]$ aralığında tamsayı değeri alan bir dönüşümdür.

$$W_f(w) = \sum_{x \in GF(2)^n} (-1)^{f(x)} (-1)^{w \cdot x} \quad (2.1)$$

Bir f Boole fonksiyonunun doğrusal olmama değeri NL_f , tüm afin fonksiyonlara olan Hamming uzaklıklarının en düşüğü olarak tanımlanır ve Walsh-Hadamard spektrumundaki mutlak değerce en büyük değeri ile aşağıdaki gibi hesaplanabilir.

$$NL_f = 2^{n-1} - (1/2) \max_{w \in GF(2)^n} |W_f(w)| \quad (2.2)$$

Parseval teoremine göre, Walsh-Hadamard spektrumundaki tüm değerlerin kareleri toplamı sabittir ve Eşitlik 2.3'te gösterildiği gibi 2^{2n} 'ye eşittir.

$$\sum_{w \in \text{GF}(2)^n} W_f(w)^2 = 2^{2n} \quad (2.3)$$

Bu teoremden, bir Boole fonksiyonun Walsh-Hadamard spektrumundaki en büyük mutlak değerin alabileceği en düşük değerin $2^{n/2}$ olduğu görülmektedir. Bu nedenle, en yüksek doğrusal olmama değeri, doğrusal olmama ölçütünden $2^{n-1} - 2^{n/2-1}$ olarak elde edilir. Bu doğrusal olmama değerine sahip bir Boole fonksiyonu bükük olarak isimlendirilir ve sadece çift n değerleri için bükük fonksiyonlar mevcuttur. Literatürdeki evrimsel veya sezgisel arama algoritmaları tarafından kullanılan maliyet/uygunluk fonksiyonları, ağırlıklı olarak Parseval teoremine dayanmaktadır [16-18, 22].

Aşağıda verilen otokorelasyon fonksiyonu $r_f(d)$, bir Boole fonksiyonun girişine belirli bir fark uygulanmış versiyonu ile arasındaki korelasyonu verir.

$$r_f(d) = \sum_{x \in \text{GF}(2)^n} (-1)^{f(x)} (-1)^{f(x \oplus d)} \quad (2.4)$$

f Boole fonksiyonunun d vektörüne göre birinci dereceden türevi $f(x) \oplus f(x \oplus d)$ olarak tanımlanır. Buna göre, bir Boole fonksiyonunun otokorelasyonu birinci derece türevinde ortaya çıkan dengesizlik olarak düşünülebilir. Otokorelasyon spektrumundaki $r_f(\mathbf{0})$ dışında (Eşitlik 2.5'te gösterildiği gibi) en büyük mutlak değer AC_f , mutlak gösterge olarak tanımlanır.

$$AC_f = \max_{d \neq \mathbf{0} \in \text{GF}(2)^n} |r_f(d)| \quad (2.5)$$

burada $\mathbf{0} = (0, 0, \dots, 0)$ ($r_f(\mathbf{0}) = 2^n$ olduğuna dikkat ediniz). Mutlak gösterge ile birlikte, yayılma özelliğini ölçmek için kullanılan bir başka ölçüt ise otokorelasyon spektrumundaki değerlerin kareleri toplamı $(\sum_{d \in \text{GF}(2)^n} r_f(d)^2)$ olarak tanımlanan karesel toplam göstergesidir. Bir Boole fonksiyon için karesel toplam göstergesinin,

bükük fonksiyonların karesel Walsh-Hadamard spektrumundan sapmalarının karesel toplamı ile orantılı olduđu aşağıdaki teoremle ifade edilmektedir.

Teorem 2.1. [31]. n -değişkenli bir Boole fonksiyon f için aşağıdaki eşitlik geçerlidir:

$$\sum_{d \neq \mathbf{0} \in \text{GF}(2)^n} r_f(d)^2 = 2^{-n} \sum_{w \in \text{GF}(2)^n} (W_f(w)^2 - 2^n)^2 \quad (2.6)$$

Herhangi bir Boole fonksiyonu, cebirsel normal biçim ile eşsiz olarak gösterilebilir:

$$f(x) = \bigoplus_{0 \leq i \leq n-1} a_i x_i \bigoplus_{0 \leq i < j \leq n-1} a_{ij} x_i x_j \bigoplus \dots \bigoplus a_{01\dots n-1} x_0 x_1 \dots x_{n-1} \bigoplus c \quad (2.7)$$

burada, $a_i, a_{ij}, \dots, a_{01\dots n-1} \in \text{GF}(2)$. Cebirsel derece d_f , sıfırdan farklı katsayıya sahip en fazla değişkenli terimdeki değişken sayısıdır.

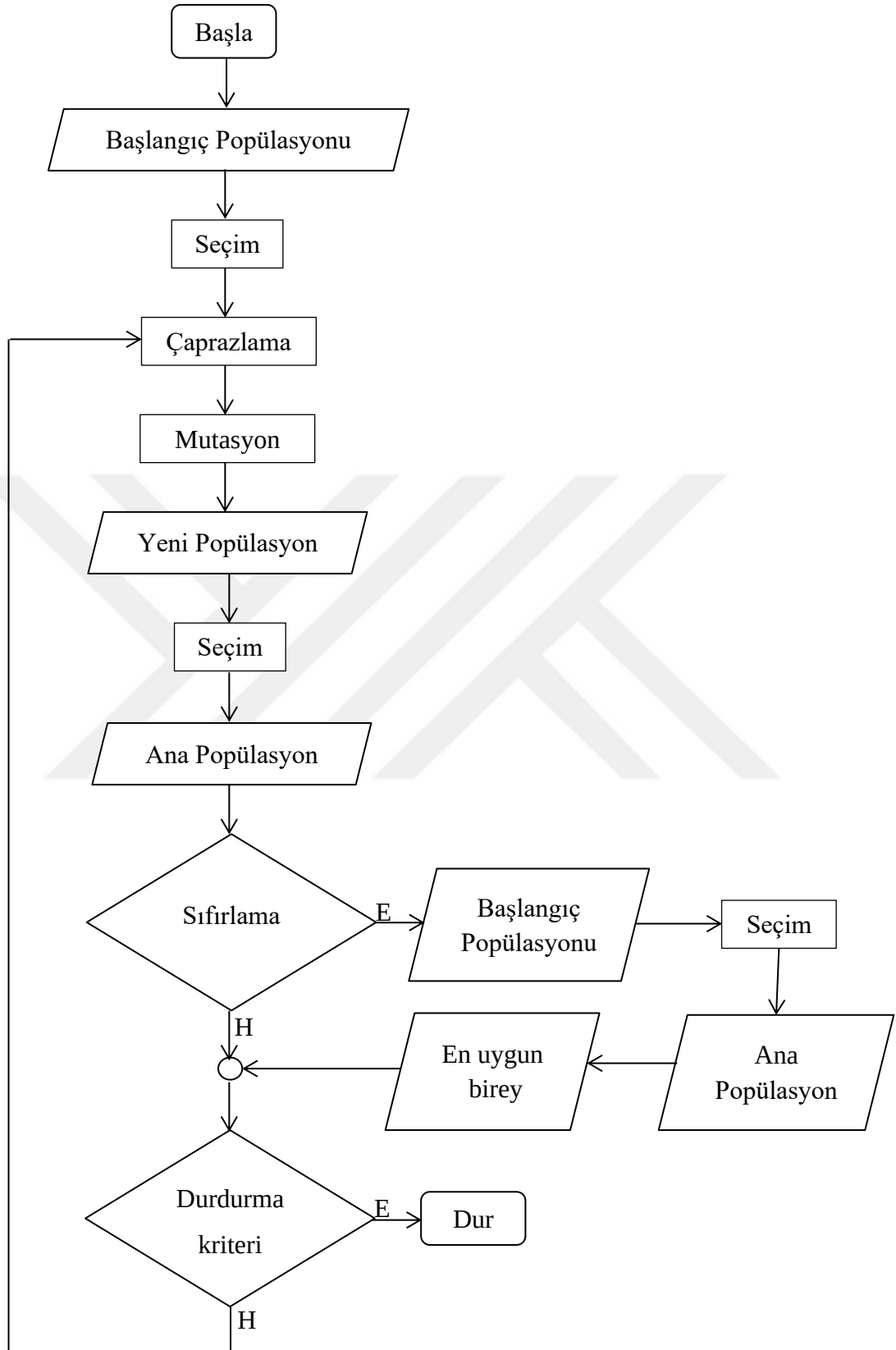
BÖLÜM 3

GENETİK ALGORİTMA

Darwin'in en uygun olanın hayatta kalması ilkesine dayanan genetik algoritma (GA) [32], optimizasyon ve arama problemlerinde en yaygın olarak uygulanan evrimsel algoritmadır. GA, bir popülasyondan seçilen herhangi bir ebeveynin, yani bir çift bireyin bir çocuk ürettiği doğal seçim olarak bilinen evrimsel sürece dayanır. Bu süreçte mutasyonlar meydana gelebilir; ancak mutasyondan sonra, yalnızca en uygun bireyler bir sonraki nesil için hayatta kalır. Çalışmamızda kullanılan genetik algoritmanın genel yapısı Şekil 3.1'de gösterilmektedir. Şekil 3.1'deki başlangıç popülasyonu, sabit bir bükük fonksiyona en yakın mesafede rastgele oluşturulmuş dengeli Boole fonksiyonlarından oluşmaktadır. Elitizm yaklaşımı ve k -turnuva mekanizması ile gerçekleştirdiğimiz seçim işlemi, Şekil 3.2 ile verilen çaprazlama stratejisi kullanılarak, çocukların üretildiği ana popülasyonu oluşturmak için başlangıç popülasyonuna uygulanır. Elitizm yaklaşımında, bir popülasyondaki en uygun bireyler, yani en iyi uygunluk değerlerine sahip dengeli Boole fonksiyonlar hayatta kalır. Buna karşılık, k -turnuva yönteminde, rastgele seçilen k birey arasından en uygun olanı hayatta kalır. Çalışmamızda, bir f Boole fonksiyonu için uygunluk fonksiyonu olarak [9, 18] çalışmalarında kullanılan Eşitlik 2.8 ile verilen $uygunluk_f$ maliyet fonksiyonu seçilmiştir.

$$uygunluk_f = \sum_{w \in GF(2)^n} (W_f(w)^2 - 2^n)^2 \quad (2.8)$$

Kullanılan uygunluk fonksiyonu ile, Teorem 2.1'den görüldüğü gibi hem otokorelasyon değerlerinin hem de Walsh-Hadamard spektrum değerlerinin birlikte eniyilenmesi (bükük fonksiyonların ideal olan otokorelasyon ve Walsh-Hadamard spektrumu değerlerine yakınlaştırma) hedeflenmiştir.



Şekil 3.1. Genetik algoritma yapısı.

1. $g(x) = p_1(x) \forall x \in GF(2)^n$ öyle ki $p_1(x) = p_2(x)$
2. $I_1 = \{x \in GF(2)^n : f(x) = 0 \& p_1(x) = 1\}$
3. $I_2 = \{x \in GF(2)^n : f(x) = 0 \& p_2(x) = 1\}$
4. $J_1 = I_1 \setminus I_1 \cap I_2$
5. $J_2 = I_2 \setminus I_1 \cap I_2$
6. $g(x) = 1 \forall x \in J_1 \cup J_2$
7. $J_1 \cup J_2$ 'de bulunan x vektörlerinin rasgele secilen varısı için $a(x) = 0$

Şekil 3.2. Birbiçimli çaprazlama algoritması.

Gerçekleştirdiğimiz genetik algortmada, herhangi bir bükük fonksiyon kullanılabilmesine rağmen, büyüklüğünü 1000 olarak belirlediğimiz başlangıç popülasyonunu oluşturmak için Maiorana-McFarland (MM) tipi bir bükük fonksiyon [33] rastgele seçilmekte ve dengeli Boole fonksiyonlar seçilen bu bükük fonksiyondan üretilmektedir. Deneylerimizde, ürettiğimiz herhangi bir bükük fonksiyon $2^{n-1} - 2^{n/2-1}$ Hamming ağırlığına sahiptir, yani doğruluk tablosundaki sıfırların sayısı birlerin sayısından $2^{n/2}$ daha fazladır. Başlangıç popülasyonu üretildikten sonra, popülasyondaki her bir bireyin uygunluk değeri hesaplanmakta ve ardından en iyi uygunluk değerlerine sahip 100 tanesi elitizm yaklaşımı ile seçilmektedir. Elde edilen bu 100 bireyden k -turnuva yöntemi ile belirlenen 40 tanesi ana popülasyonu oluşturmaktadır (algoritmamızda $k = 3$ olarak alınmıştır).

Ana popülasyon oluşturulduktan sonra, algoritma çaprazlama işlemi ile başlayan üretim döngüsüne girer. Ana popülasyondan çocukları elde etmek için kullanılan tek noktalı, iki noktalı, birbiçimli ve kısmi uyum gibi çeşitli çaprazlama yöntemleri vardır. Burada, Şekil 3.2 ile verilen ve n değişkenli bir bükük fonksiyona $2^{n/2-1}$ uzaklıkta olan (ana popülasyona ait) herhangi iki bireyin çiftleşmesinden üretilen çocukların bu bükük fonksiyona aynı uzaklığı koruduğu tek tip çaprazlama kullanılmaktadır. Şekil 3.2'de f , g , p_1 ve p_2 fonksiyonları sırasıyla bükük fonksiyonu, çocukları, ilk bireyi ve ikinci bireyi temsil eder. Çaprazlama algoritması, p_1 ve p_2 bireylerine ait bitlerin (aynı konuma ait) her bir çiftini kontrol ederek başlar ve her

ikisi de eşitse değerlerini çocuğa atar. Daha sonra, sonraki iki adımda verildiği gibi, f bükük fonksiyonunun sıfır olduğu ve ilk birey p_1 'in (ikinci birey p_2 'nin) bir olduğu her konum I_1 'e (I_2 'ye) atanır. Çaprazlama işlemi, çocuğa $J_1 \cup J_2$ 'deki pozisyonların rastgele seçilen yarısı için 0, diğer yarısı için 1 atanarak tamamlanır, burada J_1 ve J_2 sırasıyla hem I_1 hem de I_2 'ye ait pozisyonların I_1 ve I_2 'den çıkarılmasıyla oluşan kümelerdir. Gerçekleştirdiğimiz GA'da çocuklar, ana popülasyondaki her olası birey çiftinden Şekil 3.2'de verilen çaprazlaması kullanılarak üretilir. Diğer bir deyişle, çaprazlama olasılığını 1 olarak alınmaktadır. g çocuğunun dengeli olduğuna ve f bükük fonksiyonuna $2^{n/2-1}$ uzaklıkta olduğuna dikkat edilmelidir.

Mutasyon, çeşitliliği sağlamak için çaprazlamadan elde edilen çocuklara uygulanır. Bir çocuğun doğruluk tablosundan rastgele seçilen 0 ve 1 çiftinin yer değiştirmesi ile gerçekleştirilir, öyle ki bükük fonksiyonun doğruluk tablosunda bu iki bitin karşılık gelen konumlarında sıfır bulunmalıdır. Böylelikle, mutasyon işleminden sonra (bükük fonksiyona) mesafenin aynı kaldığı görülebilir. Değişken sayısı n arttıkça arama uzayı süper üstel olarak büyüdüğünden (bkz. Çizelge 5.2), yüksek mutasyon olasılıkları ebeveynlerin yakınında arama yapılmasını engelleyebilir. Bu nedenle, çalışmamızda herhangi bir çocuğun mutasyona uğrama olasılığı n arttıkça azalacak şekilde $2/2^n$ olarak alınmıştır. Mutasyon işleminden sonra elde edilen çocuklar (daha önce başlangıç popülasyonundan seçilen) ebeveyn popülasyonuna eklenir. Daha sonra, mevcut popülasyona daha önce bahsedilen seçim işlemi uygulanarak, yeni bir ebeveyn popülasyonu oluşturulur.

Döngünün son aşaması olarak, ana popülasyonda çeşitliliği artırmak için, [15] çalışmasında önerilenin biraz değiştirilmiş bir versiyonu olan bir sıfırlama adımı uygulanmaktadır. [15] çalışmasında, birkaç nesil boyunca en iyi uygunluk değerinde bir iyileşme olmazsa, en uygun bireyi koruyan ve ana popülasyonun geri kalanını rastgele oluşturan isteğe bağlı bir sıfırlama adımı uygulanmaktadır. Çalışmamızda sıfırlama adımı, her neslin ana popülasyonundaki tüm bireylerinin uygunluk değerleri dikkate alarak uygulanmıştır. Özel olarak, bu değerler bir nesil için aynıysa, bunlardan biri tutulur ve diğer 39 birey rastgele 1000 büyüklüğünde yeni bir popülasyon oluşturularak ve ardından bu popülasyona seçim işlemi uygulanarak oluşturulur. Ayrıca, bu adımda GA, mevcut neslin ana popülasyonu içindeki en

uygun bireyi çıktı olarak verir. Döngü, maksimum nesil sayısı olan ve deneylerimiz boyunca 100 ila 20000 arasında değişen durdurma kriteri karşılanana kadar devam etmektedir.



BÖLÜM 4

GA PARAMETRELERİNİN SEÇİMİ VE BAŞARIM DEĞERLENDİRMESİ

4.1. POPÜLASYON BÜYÜKLÜKLERİ

GA'nın başarımı, başlangıç popülasyonunun büyüklüğü, ana popülasyonun büyüklüğü ve başlangıç popülasyonundan seçilen bireylerin sayısı gibi parametrelerin ince ayarına bağlıdır. Çalışmamızda, 8, 10 ve 12 değişkenli Boole fonksiyonları için çok sayıda deneyin gerçekleştirilmesiyle, bu parametrelerin (Bölüm 3'te bahsedilen) değerlerini belirlemek amacıyla bir parametre ayarlama aşaması yürütülmüştür. Özel olarak, her bir değişken sayısı için büyüklükleri 500, 1000, 1500 ve 2000 olan başlangıç popülasyonları, 20, 40, 60 ve 80 olan ana popülasyon büyüklükleri ve 50, 100, 150 ve 200 olan seçim büyüklükleri ile deneyler yapılmıştır. Bu parametre kombinasyonlarından, ana popülasyon büyüklüğünün seçim büyüklüğünü aştığı kombinasyonlar çıkarıldıktan sonra, 64 kombinasyondan geriye 56 kombinasyon kalmaktadır. Her bir kombinasyon için parametre ayarlama aşamasında 20000 iterasyonluk bir durdurma kriteri uygulanmıştır. Kombinasyon sonuçlarına göre 8, 10 ve 12 değişkenli Boole fonksiyonları için elde edilen en iyi parametreler kümesi, bu çalışmada ele alınan tüm Boole fonksiyonları için kullanılmıştır.

Çalışmamızda dengeli Boole fonksiyonlarının doğrusal olmama özelliğini eniyilemek hedeflendiğinden, bahsedilen kombinasyonlar karşılık gelen doğrusal olmama sonuçları açısından değerlendirilmiştir. Bir kombinasyon, elde ettiği ortalama değer açısından değerlendirildiğinde, kötü bir çözümün iyi çözümlerin ihmal edilmesine yol açabileceği açıkça görülmektedir. Bu nedenle, ortalama değerler yerine, kombinasyonları karşılaştırmak için ulaştıkları en iyi doğrusal olmama değerleri dikkate alınmıştır. 8 değişkenli Boole fonksiyonları için, her parametre kombinasyonunun bilinen en iyi doğrusal olmama değeri olan 116'yı elde

ettiği gözlenmiştir. 10 ve 12 değişkenli durumlar için, 11 ve 4 kombinasyon sırasıyla bilinen en iyi doğrusal olmama değerleri olan 492 ve 2010 değerlerini elde etmektedir. Bu kombinasyonlar Çizelge 4.1’de verilmiştir (Çizelge 4.1’de bir kombinasyon (başlangıç popülasyon büyüklüğü, seçim büyüklüğü, ana popülasyon büyüklüğü) üçlüsü ile temsil edilmektedir). Görülebileceği gibi, en iyi doğrusal olmama değeri 10 değişkenli durumda 500, 1000, 1500 ve 2000 büyüklüklerindeki tüm başlangıç popülasyonları için ve 12 değişkenli durumda ise 1000 ve 2000 büyüklüklerindeki başlangıç popülasyonları için elde edilmiştir. Her iki durum için de 1000 ve 2000 popülasyon büyüklükleri en iyi doğrusal olmama değerini sağladığından, başlangıç popülasyonu için 1000 büyüklüğü tercih edilmiştir. Ana popülasyon büyüklüklerine bakıldığında, 10 değişkenli Boole fonksiyonları için en iyi doğrusal olmama değeri 492’nin büyüklüğü 20 ve 40 olan ana popülasyonlar ile elde edildiği, 12 değişkenli Boole fonksiyonları için ise en iyi doğrusal olmama değeri 2010’un büyüklüğü 40 olan ana popülasyonlar ile elde edildiği görülmektedir. Bu nedenle, ana popülasyon için hem 10 hem de 12 değişkenli durumlarda en iyi doğrusal olmama değerini veren 40 büyüklüğü seçilmiştir. Son olarak, hem 10 hem de 12 değişkenli durumlar için en iyi doğrusal olmama değeri seçim büyüklüğü 100 iken ile elde edildiğinden, seçim büyüklüğü 100 olarak alınmıştır.

Çizelge 4.1. Bir kombinasyonun (başlangıç popülasyon boyutu, seçim boyutu, ebeveyn popülasyon boyutu) üçlüsü ile temsil edildiği 10 ve 12 değişkenli Boole fonksiyonları için bilinen en iyi doğrusal olmama değerlerini veren kombinasyonlar.

Değişken sayısı	Kombinasyonlar
10	(500, 100, 20) (500, 100, 60)
	(1000, 50, 20) (1000, 100, 40) (1000, 200, 40)
	(1500, 100, 20) (1500, 150, 80) (1500, 200, 40)
	(2000, 50, 20) (2000, 100, 20) (2000, 100, 40)
12	(1000, 100, 40) (1000, 150, 40)
	(2000, 100, 60) (2000, 200, 40)

4.2. MUTASYON OLASILIKLARI

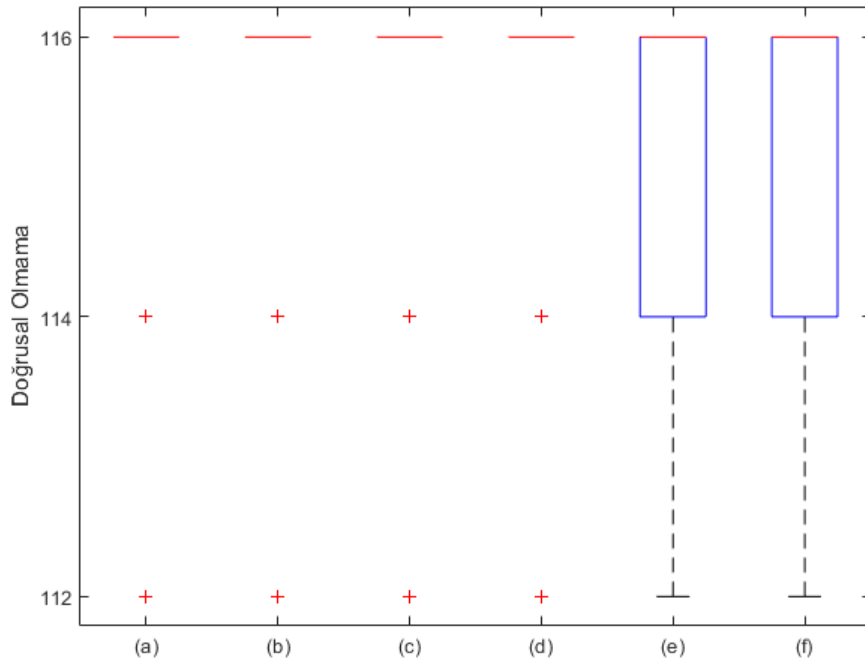
Farklı mutasyon olasılıklarının elde edilen sonuçlara etkisini gözlemlemek amacıyla, her biri maksimum nesil sayısı 20000 olan genetik algoritmanın 10 kere çalışması

sonucu üretilen Boole fonksiyonların kriptografik özellikleri 8 ve 10 değişkenli durumlar için aşağıda istatistiksel olarak yorumlanmıştır.

4.2.1. 8 Değişkenli Boole Fonksiyonlar

0, 0.008 ($\approx 2/256$), 0.05 ($\approx 13/256$), 0.1 ($\approx 26/256$), 0.15 ($\approx 38/256$) ve 0.2 ($\approx 51/256$) mutasyon olasılıklarının her biri için, en iyi nesil çıktısı olarak üretilen 200000 ($=20000 \times 10$) 8 değişkenli Boole fonksiyonun kriptografik özelliklerine göre sınıflandırılması Çizelge 4.2’de verilmiştir.

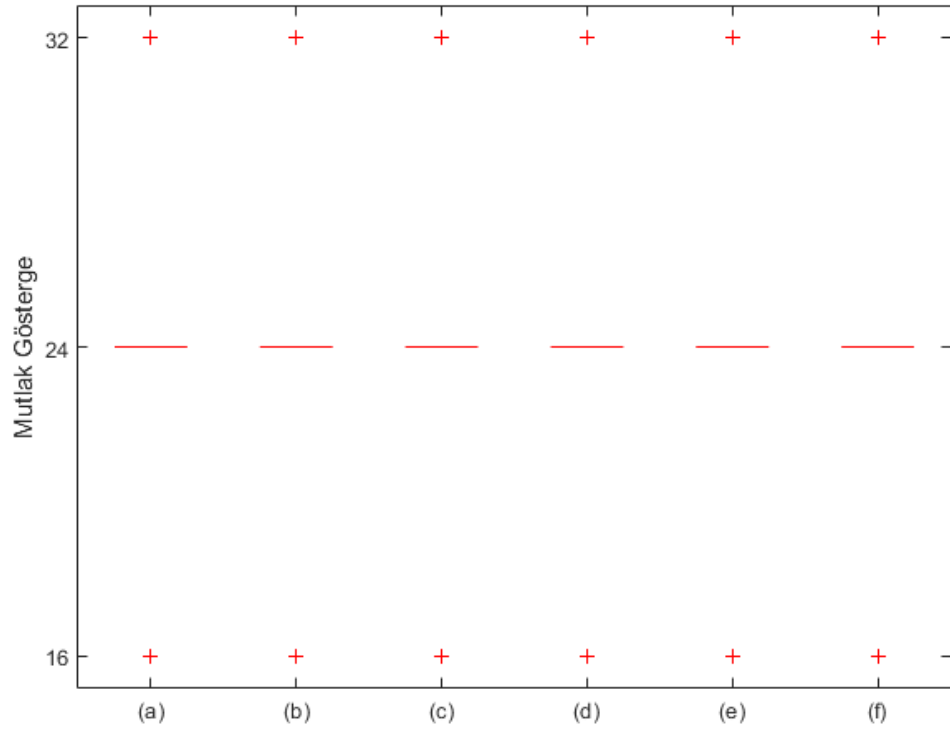
Çizelge 4.2’de elde edilen dağılımları karşılaştırmak amacıyla, karşılık gelen kutu grafikleri doğrusal olmama, mutlak gösterge ve cebirsel derece özellikleri için sırasıyla Şekil 4.1, Şekil 4.2 ve Şekil 4.3’te sunulmuştur. Şekil 4.1’den, Çizelge 4.2’deki (a), (b), (c) ve (d) sonuçlarının (e) ve (f) sonuçlarına kıyasla doğrusal olmama yönünden daha iyi oldukları, diğer bir ifadeyle doğrusal olmama değeri 116 olan Boole fonksiyonların 0.15’ten küçük mutasyon olasılıklarında daha çok sayıda bulunduğu görülmektedir. Şekil 4.2 ve 4.3’ten ise, mutlak gösterge ve cebirsel derece için farklı mutasyon olasılıklarının belirgin bir etkisinin olmadığı gözlenmektedir.



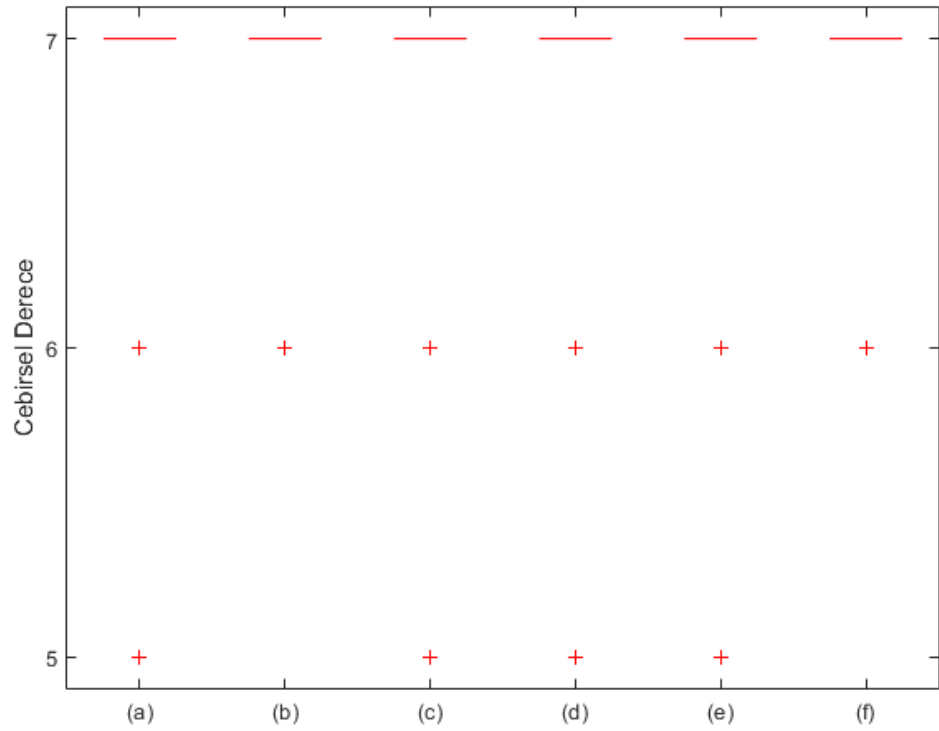
Şekil 4.1. Çizelge 4.2’deki dağılımların doğrusal olmama için aynı sırada karşılık gelen kutu grafikleri.

Çizelge 4.2. Farklı mutasyon olasılıkları için 8 değişkenli 200000 Boole fonksiyonun kriptografik özelliklerine göre dağılımları.

Mutasyon Olasılığı: 0					Mutasyon Olasılığı: 0.008 ($\approx 2/256$)					Mutasyon Olasılığı: 0.05 ($\approx 13/256$)				
NL	AI	d	#		NL	AI	d	#		NL	AI	d	#	
112	16	6	4		112	16	6	1		112	16	6	1	
112	16	7	5		112	16	7	53		112	16	7	7	
112	24	6	261		112	24	6	422		112	24	6	373	
112	24	7	21293		112	24	7	22319		112	24	7	22166	
112	32	5	1		112	32	6	54		112	32	5	1	
112	32	6	22		112	32	7	4718		112	32	6	35	
112	32	7	4514		114	24	7	12032		112	32	7	4256	
114	24	7	11757		114	32	7	7560		114	16	7	2	
114	32	7	7384		116	24	7	148752		114	24	7	12036	
116	24	7	150864		116	32	6	730		114	32	7	7584	
116	32	6	679		116	32	7	3359		116	16	7	1	
116	32	7	3216							116	24	7	149688	
										116	32	6	804	
										116	32	7	3046	
(a)					(b)					(c)				
Mutasyon Olasılığı: 0.1 ($\approx 26/256$)					Mutasyon Olasılığı: 0.15 ($\approx 38/256$)					Mutasyon Olasılığı: 0.2 ($\approx 51/256$)				
NL	AI	d	#		NL	AI	d	#		NL	AI	d	#	
112	16	7	10		112	16	6	1		112	16	6	3	
112	24	5	1		112	16	7	30		112	16	7	39	
112	24	6	283		112	24	6	305		112	24	6	282	
112	24	7	23117		112	24	7	24783		112	24	7	26263	
112	32	6	49		112	32	5	2		112	32	6	29	
112	32	7	4500		112	32	6	44		112	32	7	4906	
114	16	7	1		112	32	7	4881		114	16	7	1	
114	24	7	12111		114	16	7	4		114	24	7	13163	
114	32	7	7690		114	24	7	12557		114	32	7	7940	
116	16	7	1		114	32	7	7866		116	24	7	143491	
116	24	7	148513		116	24	6	1		116	32	6	682	
116	32	6	693		116	24	7	145884		116	32	7	3201	
116	32	7	3031		116	32	6	680						
					116	32	7	2962						
(d)					(e)					(f)				



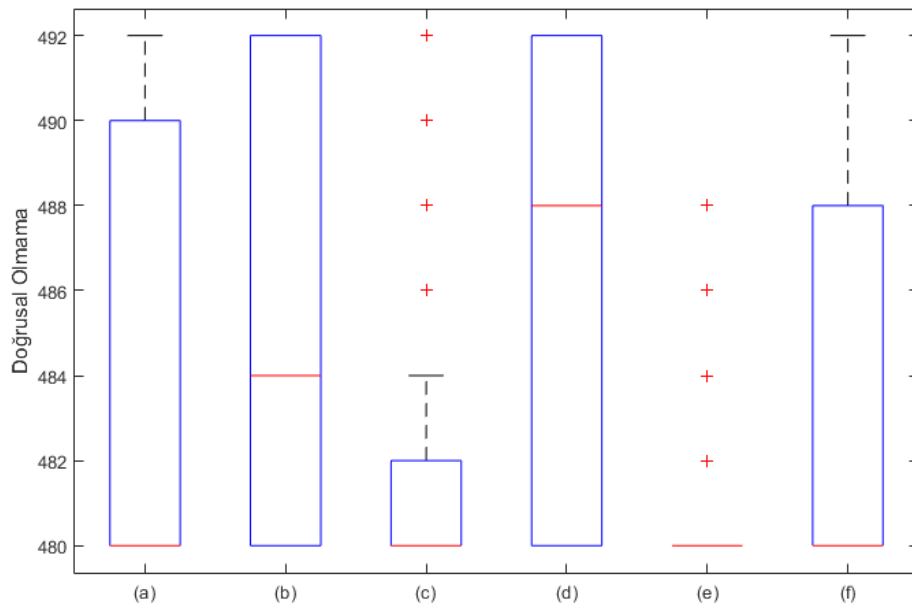
Şekil 4.2. Çizelge 4.2'deki dağılımların mutlak gösterge için aynı sırada karşılık gelen kutu grafikleri.



Şekil 4.3. Çizelge 4.2'deki dağılımların cebirsel derece için aynı sırada karşılık gelen kutu grafikleri.

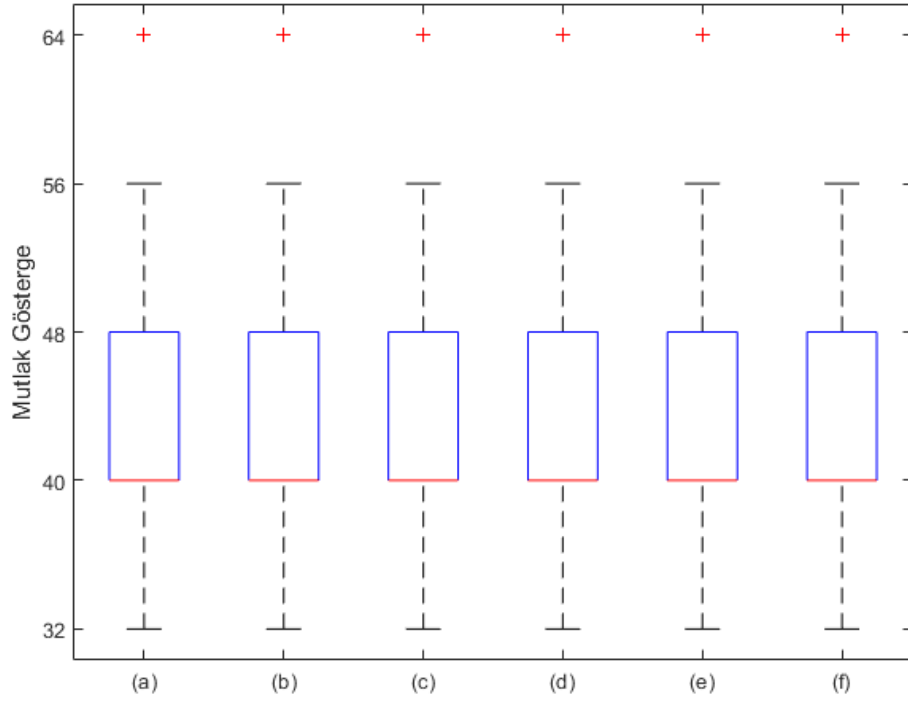
4.2.2. 10 Değişkenli Boole Fonksiyonlar

0, 0.002 ($\approx 2/1024$), 0.05 ($\approx 51/1024$), 0.1 ($\approx 102/1024$), 0.15 ($\approx 154/1024$) ve 0.2 ($\approx 205/1024$) mutasyon olasılıklarının her biri için, en iyi nesil çıktısı olarak üretilen 200000 ($= 20000 \times 10$) 10 değişkenli Boole fonksiyonun kriptografik özelliklerine göre sınıflandırması yapılmış ve bulunan sonuçların doğrusal olmama, mutlak gösterge ve cebirsel derece özellikleri için kutu grafikleri sırasıyla Şekil 4.4, Şekil 4.5 ve Şekil 4.6’da verilmiştir.

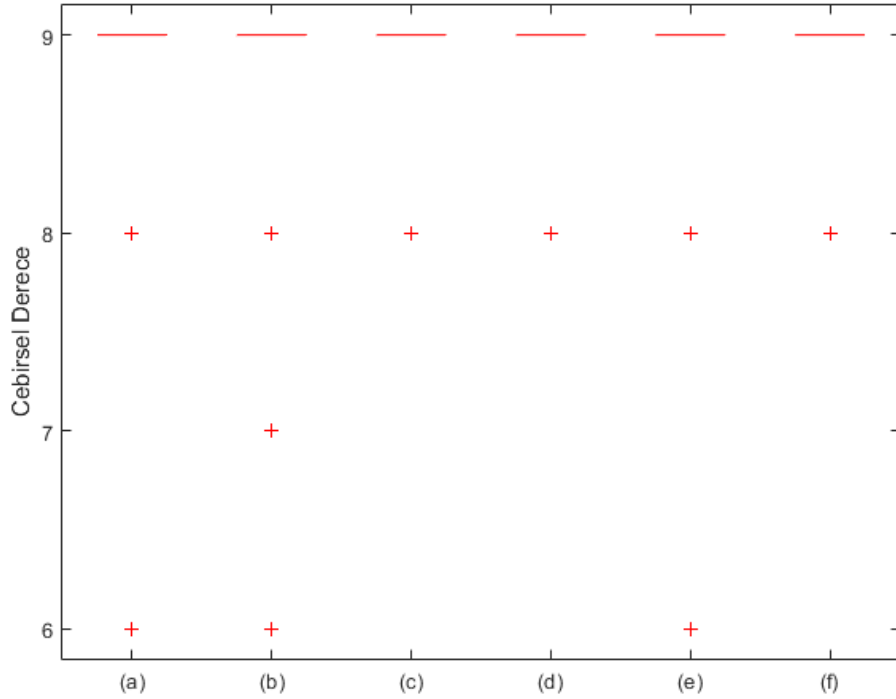


Şekil 4.4. 10 değişkenli durumda (a) 0, (b) 0.002, (c) 0.05, (d) 0.1, (e) 0.15 ve (f) 0.2 mutasyon olasılıklarının her biri için doğrusal olmama özelliğine göre elde edilen kutu grafikleri.

Şekil 4.4’ten, en iyi mutasyon olasılıklarının (b) ve (d)’de verilen kutu grafiklerine karşılık gelen 0.002 ve 0.1 olasılıkları olduğu; bununla birlikte, 0.1 olasılığı için orta değer diğer mutasyon olasılığına göre daha yüksek olduğu gözlenmektedir. Mutlak gösterge için farklı mutasyon olasılıklarının aynı istatistiksel sonucu verdiği Şekil 4.5’ten, elde edilen cebirsel derecelerin ağırlıklı olarak 9 olduğu ise Şekil 4.6’dan görülmektedir.



Şekil 4.5. 10 değişkenli durumda (a) 0, (b) 0.002, (c) 0.05, (d) 0.1, (e) 0.15 ve (f) 0.2 mutasyon olasılıklarının her biri için mutlak gösterge özelliğine göre elde edilen kutu grafikleri.



Şekil 4.6. 10 değişkenli durumda (a) 0, (b) 0.002, (c) 0.05, (d) 0.1, (e) 0.15 ve (f) 0.2 mutasyon olasılıklarının her biri için cebirsel derece özelliğine göre elde edilen kutu grafikleri.

4.3. SIFIRLAMA

Sıfırlama adımının elde edilen sonuçlara etkisini gözlemlemek amacıyla, her biri maksimum nesil sayısı 20000 olan genetik algoritmanın 10 kere çalışması sonucu üretilen Boole fonksiyonların kriptografik özellikleri 8 ve 10 değişkenli durumlar için aşağıda istatistiksel olarak yorumlanmıştır.

4.3.1. 8 Değişkenli Boole Fonksiyonlar

Sıfırlama adımının uygulandığı ve uygulanmadığı durumlarda, en iyi nesil çıktısı olarak üretilen 200000 ($=20000 \times 10$) 8 değişkenli Boole fonksiyonun kriptografik özelliklerine göre sınıflandırılması Çizelge 4.3'te verilmiştir.

Çizelge 4.3. Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için 8 değişkenli 200000 Boole fonksiyonun kriptografik özelliklerine göre dağılımları.

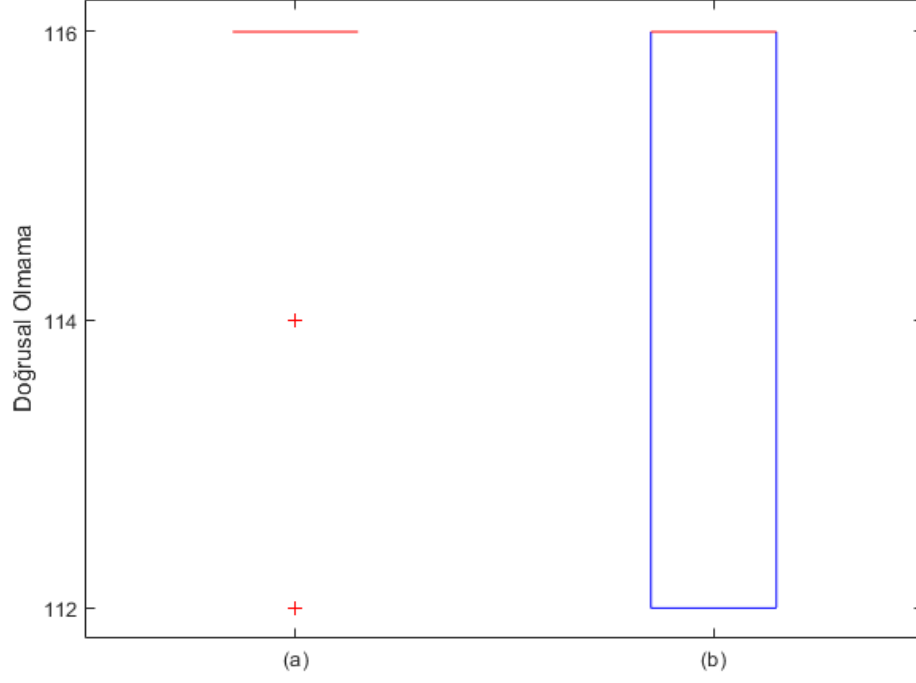
<i>NL</i>	<i>AI</i>	<i>d</i>	#	<i>NL</i>	<i>AI</i>	<i>d</i>	#
112	16	6	2	112	24	7	70480
112	16	7	9	112	32	7	9508
112	24	6	344	114	24	7	61
112	24	7	21805	114	32	7	487
112	32	6	37	116	24	7	103646
112	32	7	4152	116	32	7	15818
114	16	7	1				
114	24	7	11943				
114	32	7	7365				
116	24	6	1				
116	24	7	150136				
116	32	6	687				
116	32	7	3518				

(a)

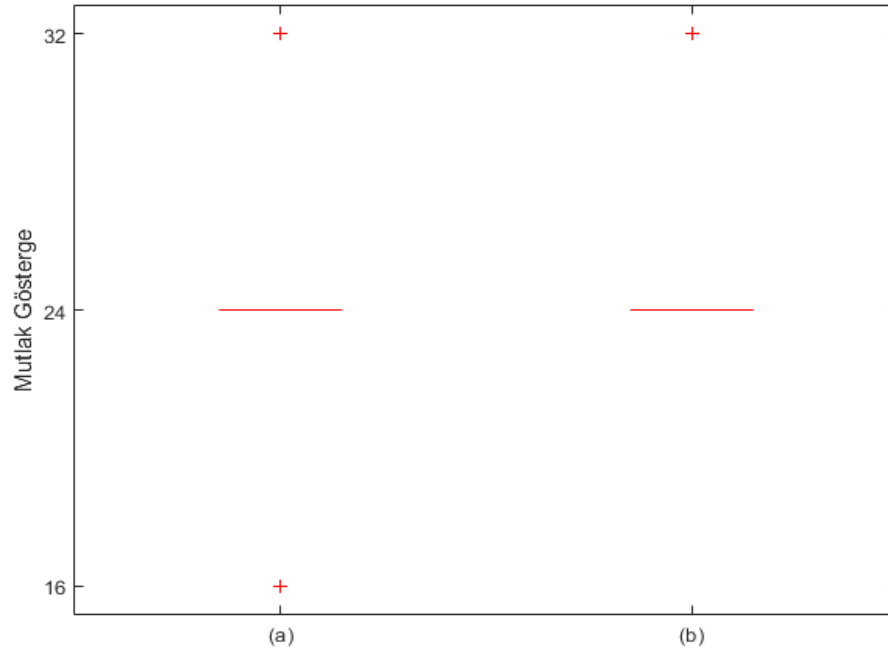
(b)

Çizelge 4.3'ten, sıfırlama adımının uygulandığı durumda hem doğrusal olmama değeri 116 olan Boole fonksiyonların daha fazla üretildiği hem de en iyi mutlak gösterge değeri 16'nın elde edildiği görülmektedir. Cebirsel derecesi 6 olan Boole fonksiyonların bu adımın uygulandığı durumda üretildiği görülmekle birlikte, bunların sayısının oldukça düşük olduğuna dikkat edilmelidir. Bu sonuçlar, Çizelge

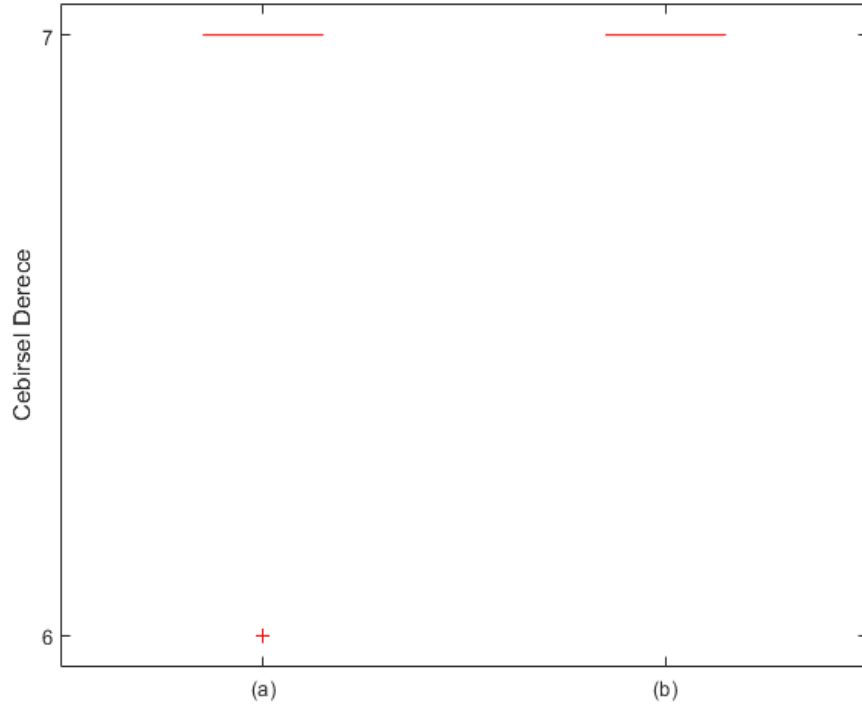
4.3'teki dağılımlara karşılık gelen kutu grafikleri Şekil 4.7-4.9'dan da görülebilmektedir.



Şekil 4.7. Çizelge 4.3'teki dağılımların doğrusal olmama için aynı sırada karşılık gelen kutu grafikleri.



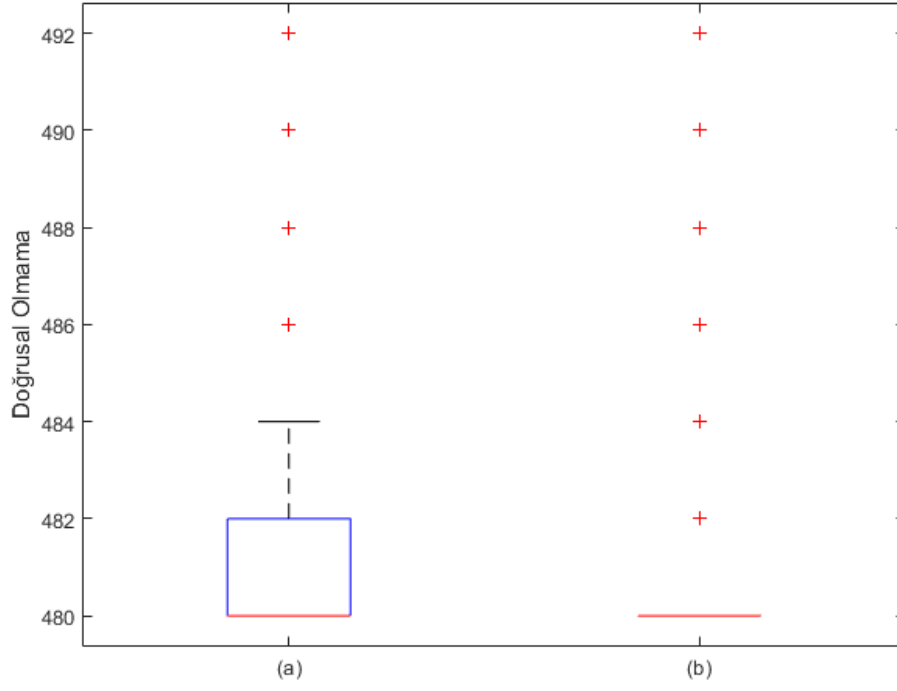
Şekil 4.8. Çizelge 4.3'teki dağılımların mutlak gösterge için aynı sırada karşılık gelen kutu grafikleri.



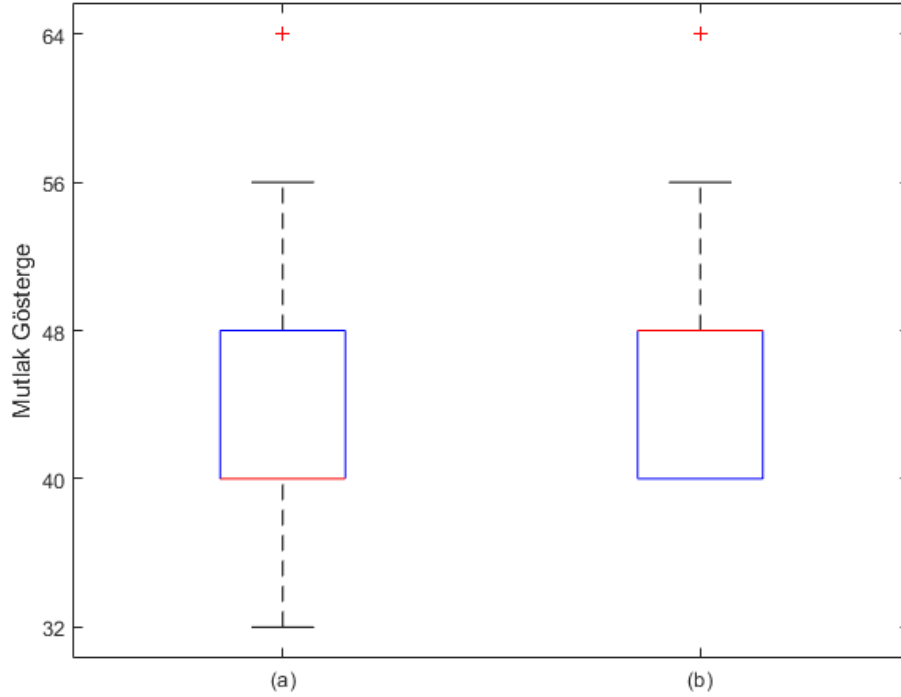
Şekil 4.9. Çizelge 4.3'teki dağılımların cebirsel derece için aynı sırada karşılık gelen kutu grafikleri.

4.3.2. 10 Değişkenli Boole Fonksiyonlar

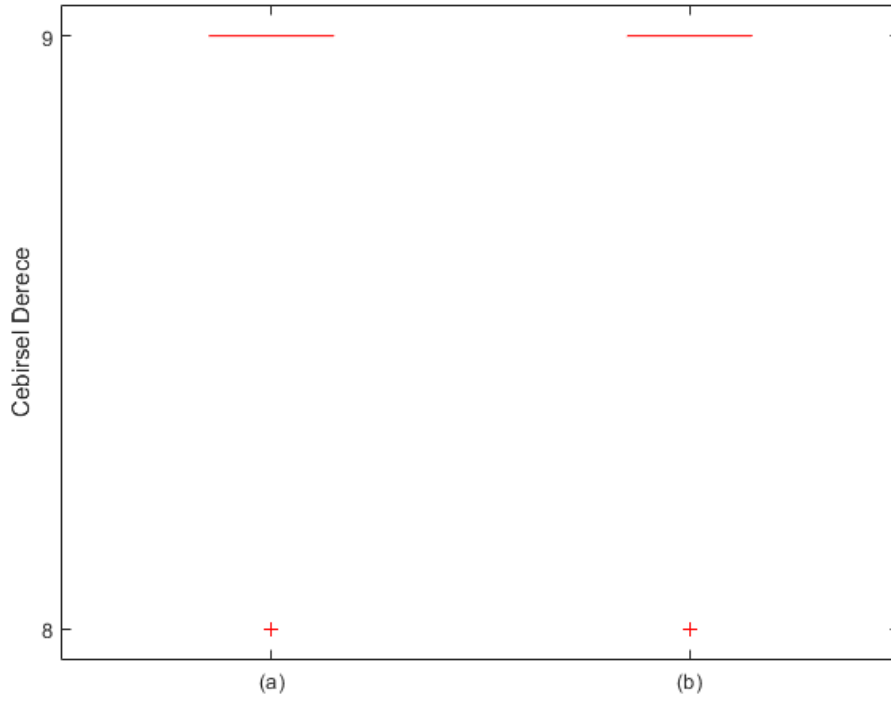
Sıfırlama adımının uygulandığı ve uygulanmadığı durumlarda, en iyi nesil çıktısı olarak üretilen 200000 ($= 20000 \times 10$) 10 değişkenli Boole fonksiyonun kriptografik özelliklerine göre sınıflandırması yapılmış ve bulunan sonuçların doğrusal olmama, mutlak gösterge ve cebirsel derece özellikleri için kutu grafikleri sırasıyla Şekil 4.10, Şekil 4.11 ve Şekil 4.12'de verilmiştir. Sıfırlama adımının uygulandığı durumda, doğrusal olmama değeri yüksek olan Boole fonksiyonların daha fazla üretildiği Şekil 4.10'dan, en iyi mutlak gösterge değerlerinin elde edildiği Şekil 4.11'den görülmektedir. Şekil 4.12 ise bu adımın uygulanması ve uygulanmaması durumlarında cebirsel derece özelliği için aynı istatistiksel sonucun elde edildiğini göstermektedir.



Şekil 4.10. Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için doğrusal olmama özelliğine göre elde edilen kutu grafikleri.



Şekil 4.11. Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için mutlak gösterge özelliğine göre elde edilen kutu grafikleri.



Şekil 4.12. Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için cebirsel derece özelliğine göre elde edilen kutu grafikleri.

4.4. NESİL SAYISI

Nesil sayısının elde edilen sonuçlara etkisini gözlemlemek amacıyla, farklı maksimum nesil sayıları için genetik algoritmanın 10 kere çalışması sonucu üretilen Boole fonksiyonların kriptografik özellikleri 8 ve 10 değişkenli durumlar için aşağıda istatistiksel olarak yorumlanmıştır.

4.4.1. 8 Değişkenli Boole Fonksiyonlar

Maksimum nesil sayısının 5000, 10000, 15000 ve 20000 olduğu durumların her biri için, en iyi nesil çıktısı olarak üretilen sırasıyla 50000 ($=5000 \times 10$), 100000 ($=10000 \times 10$), 150000 ($=15000 \times 10$) ve 200000 ($=20000 \times 10$) 8 değişkenli Boole fonksiyonun kriptografik özelliklerine göre sınıflandırılması Çizelge 4.4'te verilmiştir.

Çizelge 4.4. Farklı maksimum nesil sayıları için 8 değişkenli Boole fonksiyonun kriptografik özelliklerine göre dağılımları.

**Maksimum Nesil
Sayısı: 5000**

<i>NL</i>	<i>AI</i>	<i>d</i>	#
112	16	7	1
112	24	6	83
112	24	7	4616
112	32	5	1
112	32	6	6
112	32	7	1007
114	16	7	1
114	24	7	2981
114	32	7	1967
116	24	7	38386
116	32	6	178
116	32	7	773

(a)

**Maksimum Nesil
Sayısı: 10000**

<i>NL</i>	<i>AI</i>	<i>d</i>	#
112	16	6	1
112	16	7	6
112	24	6	135
112	24	7	11135
112	32	6	13
112	32	7	2419
114	16	7	1
114	24	7	6123
114	32	7	3741
116	24	6	1
116	24	7	74576
116	32	6	378
116	32	7	1471

(b)

**Maksimum Nesil
Sayısı: 15000**

<i>NL</i>	<i>AI</i>	<i>d</i>	#
112	16	7	13
112	24	6	212
112	24	7	14824
112	32	6	27
112	32	7	2989
114	24	7	8747
114	32	7	5719
116	16	7	1
116	24	7	114536
116	32	6	507
116	32	7	2425

(c)

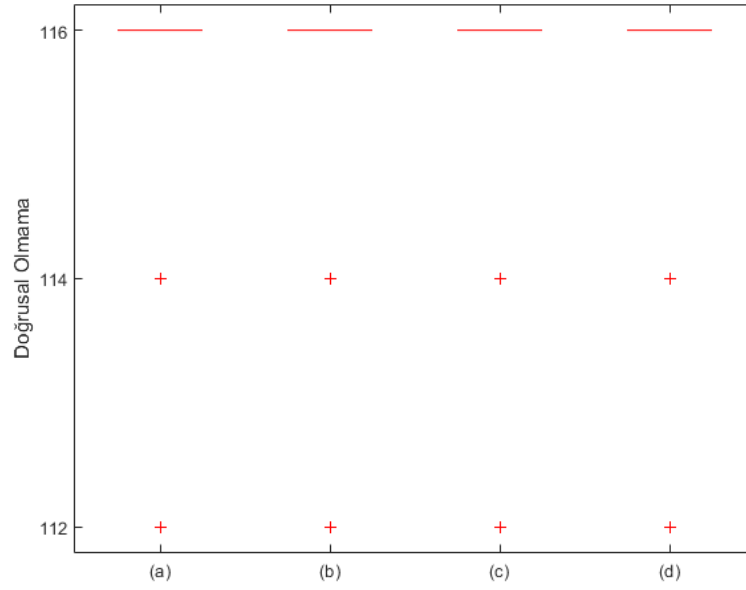
**Maksimum Nesil
Sayısı: 20000**

<i>NL</i>	<i>AI</i>	<i>d</i>	#
112	16	6	3
112	16	7	13
112	24	6	334
112	24	7	20859
112	32	6	36
112	32	7	4295
114	16	7	1
114	24	7	11550
114	32	7	7293
116	16	7	2
116	24	7	152105
116	32	6	731
116	32	7	2778

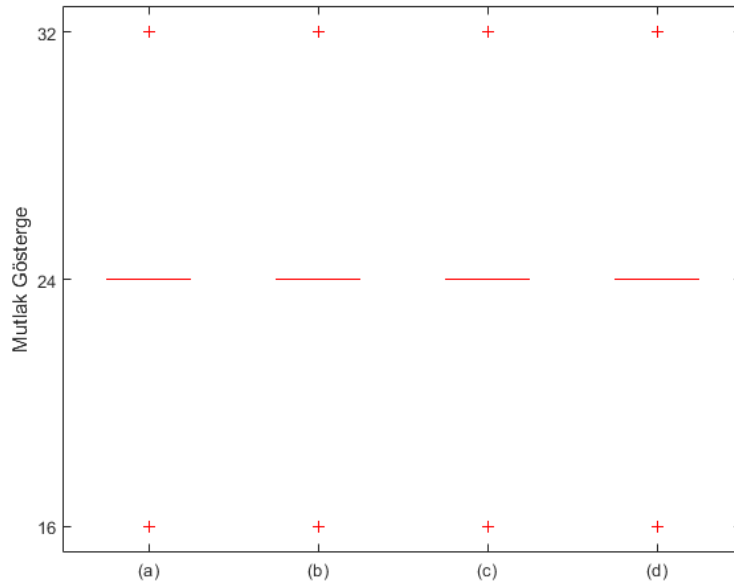
(d)

Çizelge 4.4'ten, her bir maksimum nesil sayısı için en çok üretilen Boole fonksiyonun 116 doğrusal olmama değerine sahip olduğu görülmektedir. Bununla birlikte, bu doğrusal olmama değerinin yanı sıra mutlak gösterge ve cebirsel derece bakımından da en iyi değerlere sahip Boole fonksiyonların (diğer bir ifadeyle,

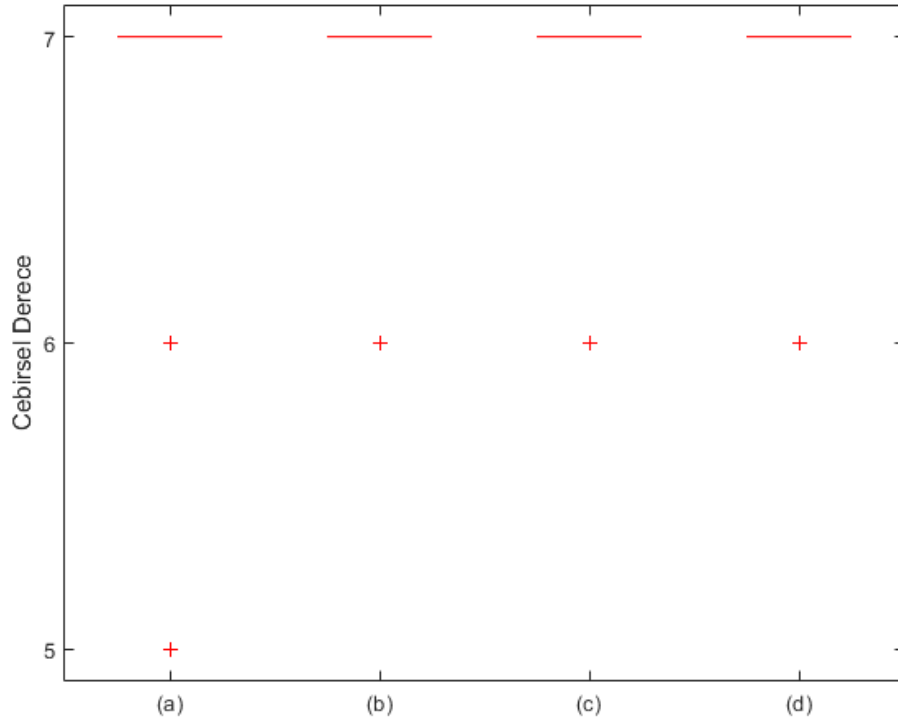
doğrusal olmama değeri 116, mutlak gösterge değeri 16 ve cebirsel derecesi 7 olan Boole fonksiyonların) maksimum nesil sayısının 15000 ve 20000 olduğu durumlarda üretildiği gözlenmektedir. Çizelge 4.4'teki dağılımlara karşılık gelen kutu grafikleri Şekil 4.13-4.15'te verilmektedir. Kutu grafikleri açısından dağılımlar ele alındığında, maksimum nesil sayısının belirgin bir farka neden olmadığı görülmektedir.



Şekil 4.13. Çizelge 4.4'teki dağılımların doğrusal olmama için aynı sırada karşılık gelen kutu grafikleri.



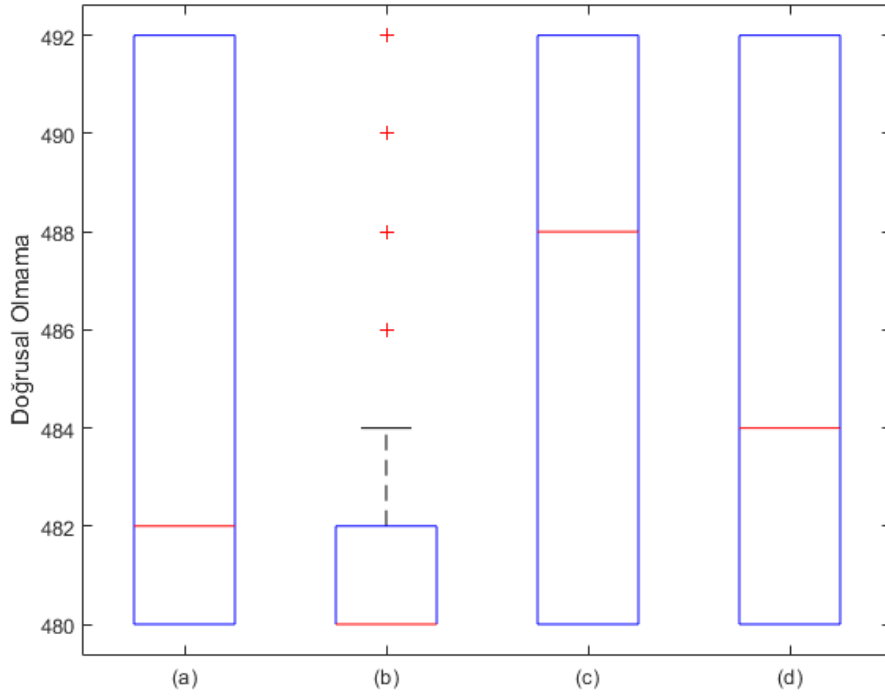
Şekil 4.14. Çizelge 4.4'teki dağılımların mutlak gösterge için aynı sırada karşılık gelen kutu grafikleri.



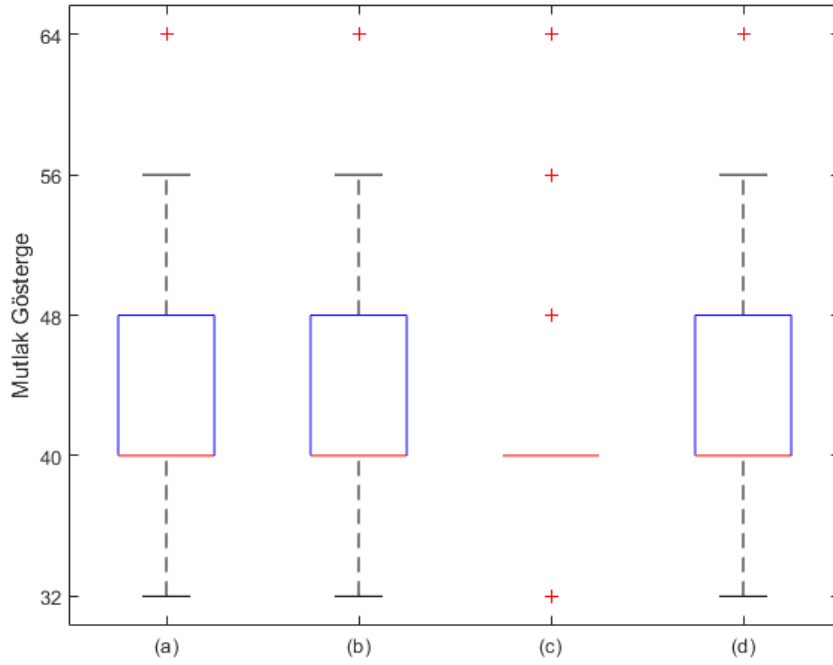
Şekil 4.15. Çizelge 4.4'teki dağılımların cebirsel derece için aynı sırada karşılık gelen kutu grafikleri.

4.4.2. 10 Değişkenli Boole Fonksiyonlar

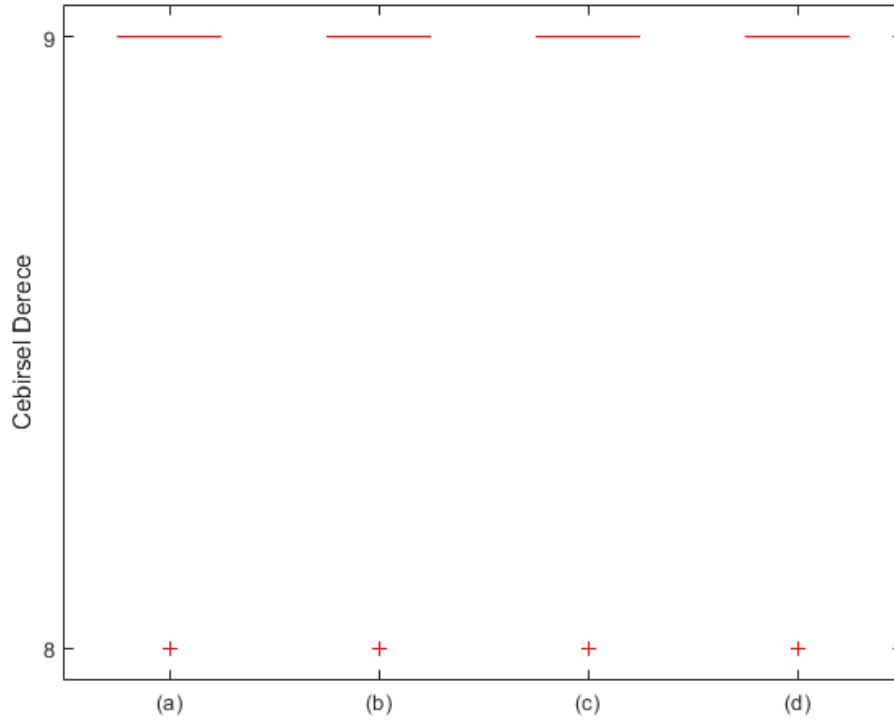
Maksimum nesil sayısına göre, en iyi nesil çıktısı olarak üretilen sırasıyla 50000 ($=5000 \times 10$), 100000 ($=10000 \times 10$), 150000 ($=15000 \times 10$) ve 200000 ($=20000 \times 10$) 10 değişkenli Boole fonksiyonun kriptografik özelliklerine göre sınıflandırması yapılmış ve bulunan sonuçların doğrusal olmama, mutlak gösterge ve cebirsel derece özellikleri için kutu grafikleri sırasıyla Şekil 4.16, Şekil 4.17 ve Şekil 4.18'de verilmiştir. Şekil 4.16'dan maksimum nesil sayısının 15000 ve üzeri olduğu durumlarda doğrusal olmama değeri yüksek Boole fonksiyonların, Şekil 4.17'den ise maksimum nesil sayısının 15000 olduğu durumda mutlak gösterge değeri düşük olan Boole fonksiyonların daha fazla üretildiği görülmektedir. Maksimum nesil sayısının cebirsel derece sonuçlarına istatistiksel olarak etkisinin olmadığı Şekil 4.18'den gözlenmektedir.



Şekil 4.16. Maksimum nesil sayısının (a) 5000, (b) 10000, (c) 15000 ve (d) 20000 olduğu durumlar için doğrusal olmama özelliğine göre elde edilen kutu grafikleri.



Şekil 4.17. Maksimum nesil sayısının (a) 5000, (b) 10000, (c) 15000 ve (d) 20000 olduğu durumlar için mutlak gösterge özelliğine göre elde edilen kutu grafikleri.



Şekil 4.18. Maksimum nesil sayısının (a) 5000, (b) 10000, (c) 15000 ve (d) 20000 olduğu durumlar için cebirsel derece özelliğine göre elde edilen kutu grafikleri.

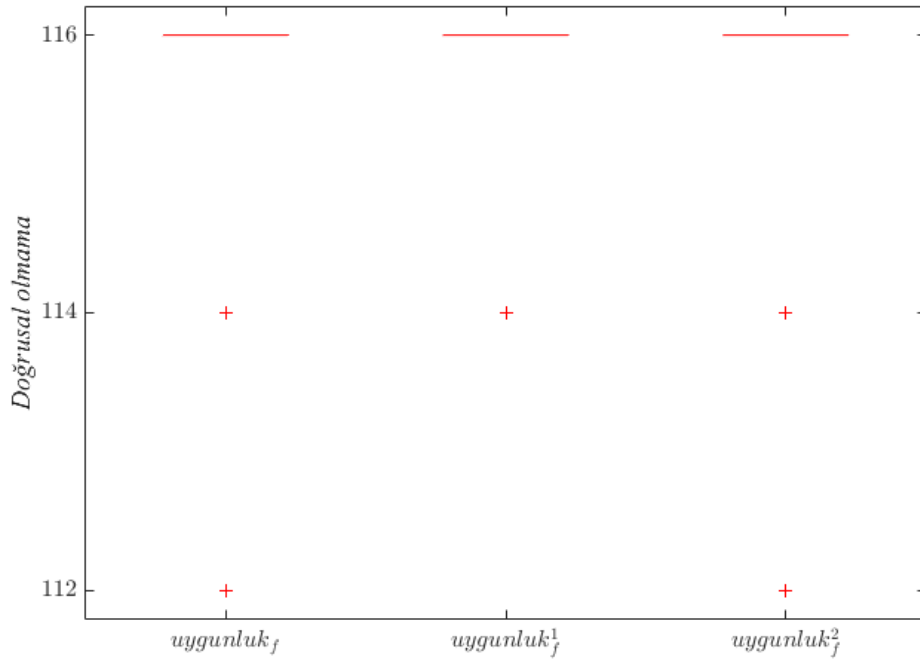
4.5. BAŞARIM DEĞERLENDİRMESİ

Bir önceki bölümde ele alınan parametrelerin ince ayarının yanı sıra, uygunluk fonksiyonunun seçimi GA'nın başarımında ve çözümlerin kalitesinde önemli bir rol oynamaktadır. Literatürde, Clark'ın maliyet/uygunluk fonksiyonu [34] Boole fonksiyonlarını evrimleştirmek için en yaygın kullanılanlardan biridir; ancak, deneysel olarak ayarlanması gereken parametrelere sahiptir. Bizim uygunluk fonksiyonumuz (Eşitlik 2.8 ile verilen $uygunluk_f$) herhangi bir deneysel parametre gerektirmedikten, burada algoritmamızın başarımı deneysel parametreler içermeyen (aşağıda verilen) iki farklı uygunluk fonksiyonu kullanılarak değerlendirilmiştir.

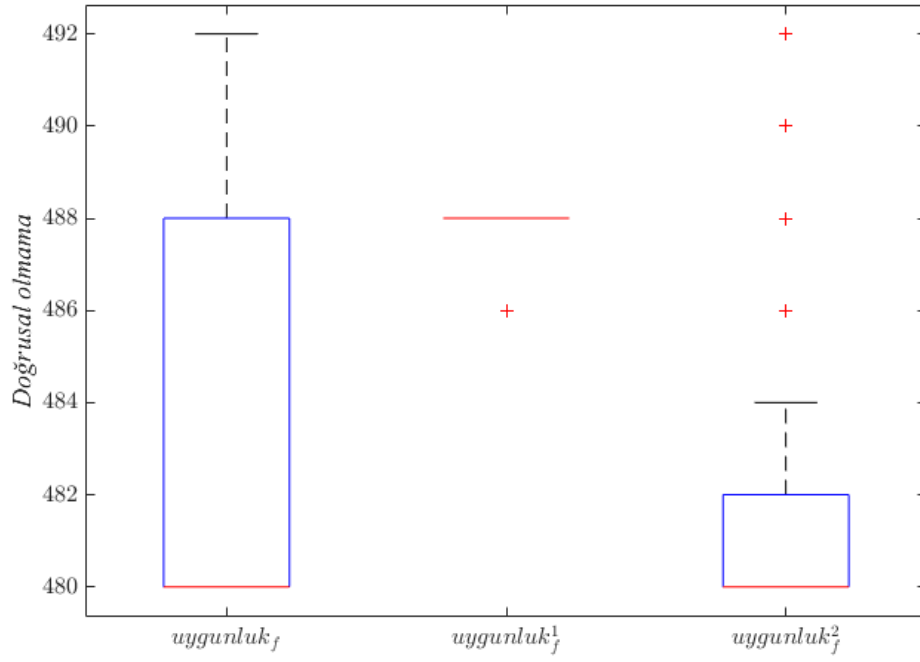
$$uygunluk_f^1 = NL_f \quad (4.1)$$

$$uygunluk_f^2 = \sum_{w \in GF(2)^n} W_f(w)^4 \quad (4.2)$$

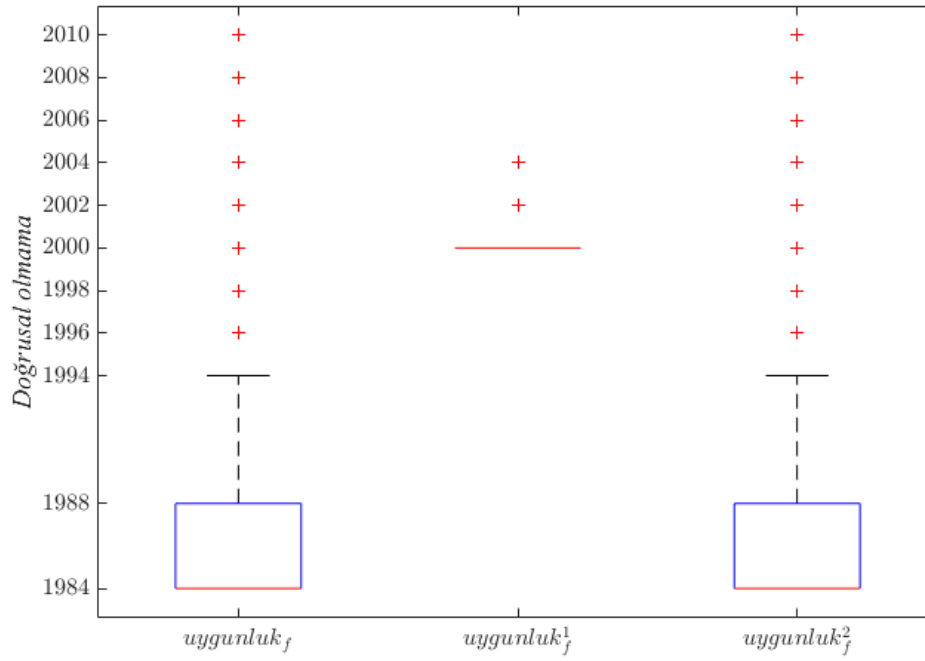
Uygunluk fonksiyonu $uygunluk_f^1$ basitçe f 'nin doğrusal olmama değeriye, diğer uygunluk fonksiyonu $uygunluk_f^2$ Clark'ın uygunluk fonksiyonu ile karşılaştırılarak en iyi çözümlere ulaşmada verimli olduğu [22] çalışmasında gösterilmiş olan f 'nin ikinci dereceden Gowers normudur. Şekil 4.19-4.24'te, 8, 10 ve 12 değişkenli durumlar için bahsedilen üç uygunluk fonksiyonunun karşılaştırma sonuçları kutu grafiği şeklinde sunulmuştur. Şekil 4.19-4.21'de (Şekil 4.22-4.24'te) gösterilen kutu grafikleri, GA'nın her biri 20000 iterasyonla 20 kez çalıştırılmasıyla oluşturulan 400000 dengeli Boole fonksiyonunun doğrusal olmama (mutlak gösterge) dağılımını temsil etmektedir.



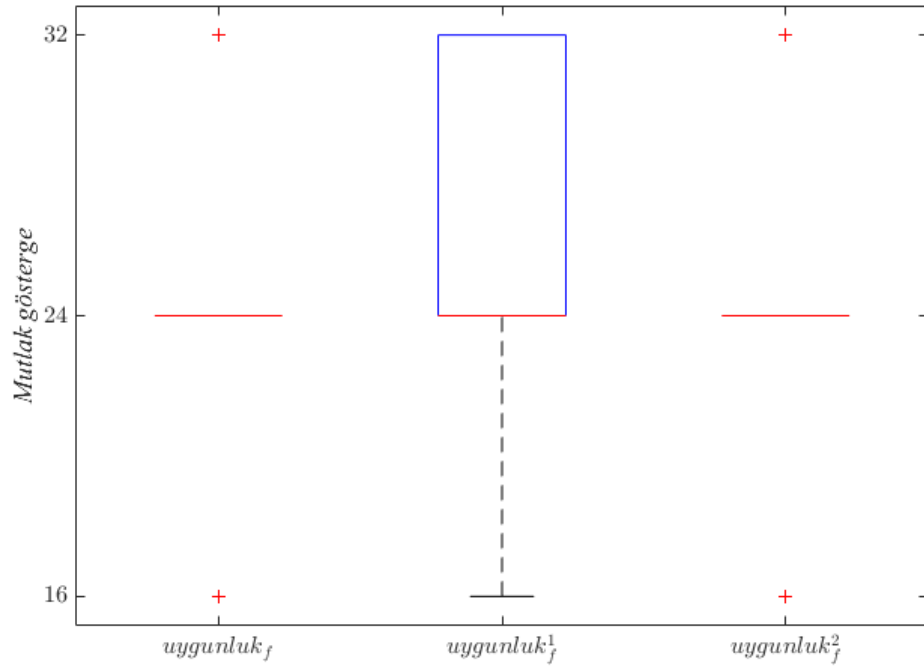
Şekil 4.19. 8 değişkenli Boole fonksiyonlar durumunda doğrusal olmama dağılımı.



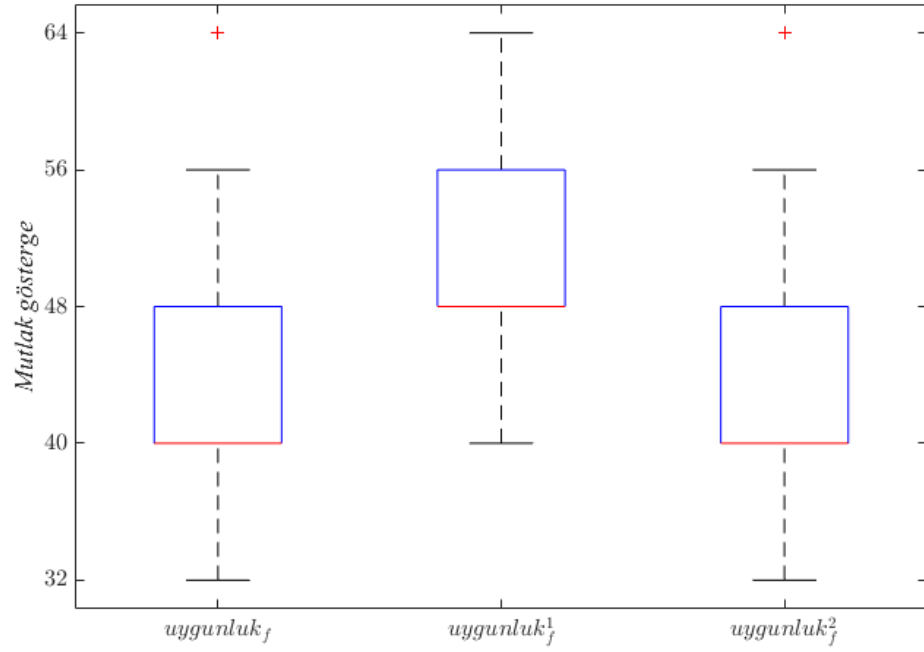
Şekil 4.20. 10 değişkenli Boole fonksiyonlar durumunda doğrusal olmama dağılımı.



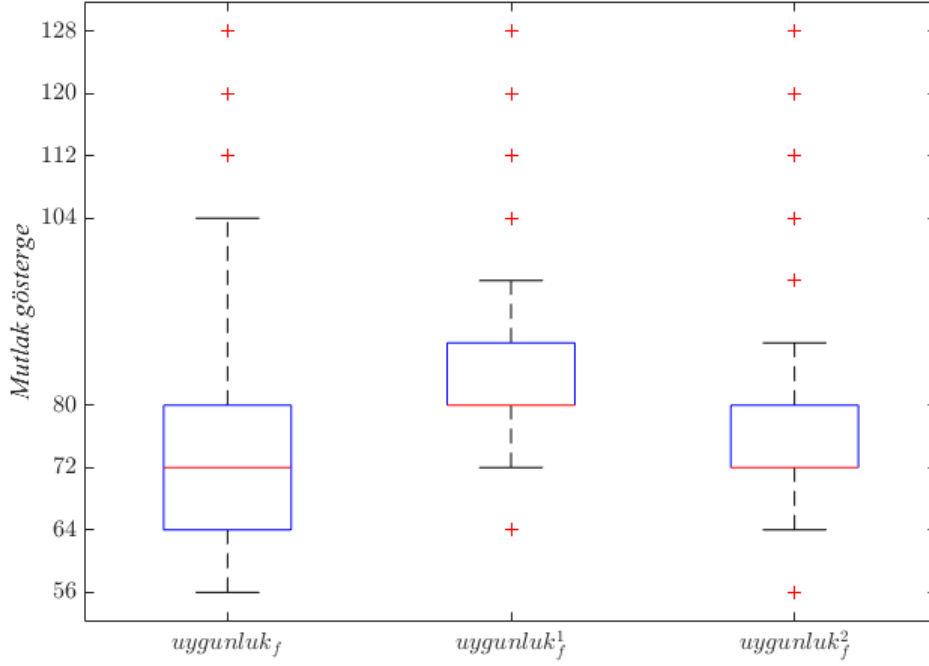
Şekil 4.21. 12 değişkenli Boole fonksiyonlar durumunda doğrusal olmama dağılımı.



Şekil 4.22. 8 değişkenli Boole fonksiyonlar durumunda mutlak gösterge dağılımı.



Şekil 4.23. 10 değişkenli Boole fonksiyonlar durumunda mutlak gösterge dağılımı.



Şekil 4.24. 12 değişkenli Boole fonksiyonlar durumunda mutlak gösterge dağılımı.

Şekil 4.19’den, $uygunluk_f$ veya $uygunluk_f^2$ kullanıldığında, kutu çizimi dağılımlarının aynı olduğu ve GA’nın 112, 114 ve 116 doğrusal olmama değerleri elde ettiği görülmektedir. Ek olarak, $uygunluk_f^1$ ’in kullanıldığı GA’nın bunlar arasındaki en düşük doğrusal olmama değerini (112) üretmediğini gözlenmektedir. Şekil 4.20, $uygunluk_f$ veya $uygunluk_f^2$ ’nin kullanıldığı GA’nın 492 doğrusal olmama değerine ulaştığını ($uygunluk_f$ ile bu doğrusal olmama değerinin daha sık üretildiğine dikkat edilmelidir) ve $uygunluk_f^1$ ’in kullanıldığı GA tarafından elde edilen en iyi doğrusal olmama değerinin 488 olduğunu göstermektedir. 12 değişken durumunda, Şekil 4.21’den anlaşıldığı gibi, elde edilen en yüksek doğrusal olmama değerinin 2010 olduğunu gösteren kutu grafiği dağılımları $uygunluk_f$ veya $uygunluk_f^2$ için aynıdır; ancak, en iyi elde edilen doğrusal olmama değeri $uygunluk_f^1$ için 2004’tür.

Şekil 4.22-4.24’te sunulan kutu grafiği dağılımları göz önüne alındığında, hem $uygunluk_f$ hem de $uygunluk_f^2$ ’nin 8 ve 10 değişkenli Boole fonksiyonları için en düşük mutlak gösterge değerleri olan sırasıyla 16 ve 32 değerlerine sahip aynı kutu grafiklerini verdiğini görüyoruz. Buna ek olarak, $uygunluk_f$ ve $uygunluk_f^2$ ’nin 10 ve 12 değişkenli durumlar için sırasıyla 32 ve 56 olan daha iyi mutlak gösterge değerleri üreterek $uygunluk_f^1$ ’den den daha iyi başarımlar gösterdiğini gözlemliyoruz. Bununla

birlikte, 8 değişkenli durum için $uygunluk_f^1$ 'in kullanıldığı GA, $uygunluk_f$ veya $uygunluk_f^2$ 'nin kullanıldığı GA'ya kıyasla daha sık (en düşük olan) 16 mutlak gösterge değerini üretmekte ve benzer şekilde 12 değişkenli durum için $uygunluk_f$ 'nin kullanıldığı GA, $uygunluk_f^2$ 'nin kullanıldığı GA'ya kıyasla daha sık (en düşük olan) 56 mutlak gösterge değerini üretmektedir.

Şekil 4.19-4.24'teki kutu grafiği dağılımlarından, $uygunluk_f$ 'nin kullanıldığı GA'nın 10 değişkenli durum için 492 doğrusal olmama değerini ve 12 değişkenli durum için 56 mutlak gösterge değerini daha sık üretmesine rağmen, yalnızca en iyi elde edilen sonuçları dikkate aldığımızda $uygunluk_f^2$ 'nin kullanıldığı GA ile benzer başarımla sergilediği sonucuna varılabilir. Ayrıca, her ikisi de 10 ve 12 değişkenli durumlar için $uygunluk_f^1$ 'in kullanıldığı GA'ya kıyasla daha iyi doğrusal olmama ve mutlak gösterge değerleri üretmektedir.

Şekil 4.19-4.24'teki kutu grafikleri ile temsil edilen doğrusal olmama ve mutlak gösterge değerlerinin dağılımlarının ortalamaları ve standart sapmaları Çizelge 4.5 ve Çizelge 4.6'da verilmiştir. Görüldüğü üzere, 10 ve 12 değişkenli durumlarda, $uygunluk_f$ için elde edilen ortalama doğrusal olmama (mutlak gösterge) değeri, $uygunluk_f^2$ için elde edilenden daha büyüktür (daha azdır). Ayrıca, $uygunluk_f^2$ ile karşılaştırıldığında, $uygunluk_f$ doğrusal olmama ve mutlak gösterge dağılımları için daha büyük standart sapmalar vermektedir. Dolayısıyla, bu durumlar için $uygunluk_f$ ile sağlanan istatistiksel parametreler, $uygunluk_f^2$ ile sağlananlardan daha iyi görünmektedir. 8 değişkenli durumda, hem doğrusal olmama hem de mutlak gösterge değerleri için, $uygunluk_f$ 'ye karşılık gelen standart sapmalar $uygunluk_f^2$ 'ye karşılık gelenlerden daha büyük olsa da, $uygunluk_f$, $uygunluk_f^2$ 'ye kıyasla daha kötü ortalama değerler verir. $uygunluk_f^1$ için bulunan ortalama doğrusal olmama (mutlak gösterge) değerlerine baktığımızda, bunların diğer doğrusal olmama (mutlak gösterge) dağılımlarının ortalamalarından daha iyi (daha kötü) olduğunu gözlemliyoruz. Dikkat edilmelidir ki $uygunluk_f^1$ çok küçük standart sapma değerleri verdiğinden (sadece 8 değişkenli durumdaki mutlak gösterge değerlerinin dağılımı hariç), $uygunluk_f$ veya $uygunluk_f^2$ ile ulaşılan doğrusal olmama ve mutlak gösterge değerlerinin $uygunluk_f^1$ ile elde edilme olasılığı daha düşük olarak görülebilir.

Çizelge 4.5. n -değişkenli Boole fonksiyonları için dağılımları Şekil 4.19-4.24'te verilen doğrusal olmama değerlerinin ortalamaları (μ) ve standart sapmaları (σ), burada $n = 8, 10$ ve 12 'dir.

Uygunluk fonksiyonu	Ortalama (μ) ve standart sapma (σ)	$n = 8$	$n = 10$	$n = 12$
$uygunluk_f$	μ	115.2670	483.4514	1987.4868
	σ	1.4142	4.8963	7.0278
$uygunluk_f^1$	μ	115.9977	487.8096	2000.1845
	σ	0.0684	0.5870	0.5789
$uygunluk_f^2$	μ	115.3356	482.5152	1986.9790
	σ	1.3560	4.3490	6.1503

Çizelge 4.6. n -değişkenli Boole fonksiyonları için dağılımları Şekil 4.19-4.24'te verilen mutlak gösterge değerlerinin ortalamaları (μ) ve standart sapmaları (σ), burada $n = 8, 10$ ve 12 'dir.

Uygunluk fonksiyonu	Ortalama (μ) ve standart sapma (σ)	$n = 8$	$n = 10$	$n = 12$
$uygunluk_f$	μ	24.6387	43.6811	76.0864
	σ	2.1718	5.2957	12.6712
$uygunluk_f^1$	μ	27.8896	49.7244	81.5849
	σ	3.9986	4.3848	6.3888
$uygunluk_f^2$	μ	24.6021	43.6920	76.1885
	σ	2.1139	4.9239	11.1301

BÖLÜM 5

ARAMA ÇALIŞMASI

Yukarıdaki bölümde açıklanan GA, Çizelge 5.1’de özetlenen deneysel parametre değerleri kullanılarak gerçekleştirilmiştir. Kullandığımız bilgisayar sistemi Intel® Core™ i5-9400F CPU (2.9 GHz, 9MB önbellek, 6 çekirdek), 16 GB RAM ve Windows 10 Pro 64-bit işletim sistemi özelliklerine sahiptir. GA, C programlama dilinde uygulanmıştır ve 100 nesil için tipik tüketilen süreler, çalışmamızda ele aldığımız tüm değişken sayıları (n) için Çizelge 5.2’de verilmiştir. Sonuçlarımızı üretmek için yaklaşık altı ay boyunca tüm çekirdeklerle çalışan (her biri yukarıda verilen özelliklere sahip) 20 bilgisayar kullanılmıştır. Elde ettiğimiz en iyi sonuçların tüm doğruluk tabloları [35] ile verilen adresinde bulunmaktadır. Bunlar arasında, 8, 10 ve 12 değişkenli Boole fonksiyonlarının doğruluk tabloları Ek A’da verilmektedir.

Tek bir bükük fonksiyonun $2^{n/2-1}$ bitinin çevrilmesiyle elde edilen n -değişkenli dengeli Boole fonksiyonların sayısının $2^{n-1} + 2^{n/2-1}$ ’in $2^{n/2-1}$ ’li kombinasyonu olduğu açıkça görülmektedir. $N_{\text{dengeli}}(n)$ ile gösterdiğimiz bu sayı, $n = 8, 10, \dots, 26$ için Çizelge 5.2’de verilmiştir. $N_{\text{bükük}}(n)$, n -değişkenli bükük fonksiyonların sayısı olsun. $N_{\text{bükük}}(8) = 99,270,589,265,934,370,305,785,861,242,880$ ($\approx 2^{106}$) olduğu bilinmektedir [36]; ancak, $n > 8$ için $N_{\text{bükük}}(n)$ bilinmemektedir. O zaman, arama uzayı $N_{\text{bükük}}(n) \times N_{\text{dengeli}}(n)$ büyüklüğünde olduğundan, $n = 8$ durumu için arama uzayı yaklaşık 2^{147} olarak bulunur.

Arama stratejimizin verimliliğini daha iyi anlamak için, özellik olarak 8 değişkenli Boole fonksiyonları durumunu ele alalım. Kaba kuvvet bir arama kullanarak, doğruluk tablosu onaltılık tabanda gösterim ile aşağıdaki gibi verilen rastgele seçilmiş MM tipi bükük bir f fonksiyonundan elde edilen mümkün olan en iyi doğrusal olmama değerine sahip tüm dengeli Boole fonksiyonları üretilmiştir.

3C3C5A5A33CC669900000FF066665AA5
0F0F3CC369693333699655555AA00FF

Çizelge 5.1. Deneysel parametre değerleri.

Parametre	Değer
Başlangıç popülasyonu büyüklüğü	1000
Elitizm yaklaşımı uygulandıktan sonra kalan birey sayısı	100
Turnuvaya katılan birey sayısı	3
Ana popülasyon büyüklüğü	40
Çaprazlama olasılığı	1
Mutasyon olasılığı (n : Giriş değişkenlerinin sayısı)	$2/2^n$
Maksimum nesil sayısı	100 - 20,000

Çizelge 5.2.100 nesil için tüketilen süreler ve dengeli fonksiyonların sayısı.

N	Tüketilen süreler	$N_{\text{dengeli}}(n)$
8	3 sn.	2^{41}
10	5 sn.	2^{100}
12	10 sn.	2^{234}
14	32 sn.	2^{536}
16	1 dk. 52 sn.	2^{1204}
18	7 dk. 33 sn.	2^{2668}
20	34 dk. 56 sn.	2^{5853}
22	2 sa. 37 dk. 52 sn.	$2^{12,735}$
24	14 sa. 18 dk. 10 sn.	$2^{27,524}$
26	42 sa. 50 dk. 36 sn.	$2^{59,150}$

Sonuç olarak, bu dengeli fonksiyonların sayısının 6,346,334,872 olduğu bulunmuş ve sınıflandırmaları Çizelge 5.3'te verilmiştir (Çizelge 5.3'te kriptografik özellikler (doğrusal olmama; mutlak gösterge; cebirsel derece) üçlüsü ile gösterilmiştir.). Çizelge 5.3'ten görülebileceği gibi, mümkün olan en iyi profil (116; 16; 7)'dir ve bu profile sahip 34.336 dengeli Boole fonksiyonu vardır. $\lim_{z \rightarrow \infty} \left(1 - \frac{1}{z}\right)^z = 1/e$ olduğundan, böyle bir fonksiyon yaklaşık olarak $\binom{136}{8}/34.336 (> 2^{26})$ denemede $1-1/e (> 1/2)$ olasılıkla rastgele arama algoritmasıyla elde edilebilir. GA'yı (başlangıç popülasyonunu oluşturmak için) yukarda verilen f bükük fonksiyonunu kullanarak ve maksimum nesil sayısını 20.000 seçerek gerçekleştirdiğimiz zaman, 50 çalıştırmada $10^6 (= 20,000 \times 50 < 2^{20})$ nesil çıktısından dördünün en iyi profile sahip olduğu

gözenmiştir. Bu da arama yöntemimizin rastgele arama yöntemine göre üstünlüğünü göstermektedir.

Çizelge 5.3. Bükük fonksiyonun komşuluğunda doğrusal olmama değeri 116 olan dengeli Boole fonksiyonlarının sınıflandırılması

$(NL_f; \Delta_f; d_f)$	#
(116;16;6)	22,720
(116;16;7)	34,336
(116;24;6)	1,006,138,800
(116;24;7)	1,906,929,536
(116;32;6)	2,090,955,784
(116;32;7)	1,342,253,696

Şimdi örnek olarak doğrusal olmama değeri 116, mutlak gösterge değeri 16 ve cebirsel derecesi 7 olan 8 değişkenli dengeli bir Boole fonksiyonu oluşturalım. Her $x \in GF(2)^4$ için $l_\omega(x) = \omega \cdot x$ eşitliği ile tanımlanan fonksiyon, $\omega \in GF(2)^4$ tarafından belirlenen doğrusal bir fonksiyon olsun ve $f = [l_{\omega^{(1)}}(x), l_{\omega^{(2)}}(x), \dots, l_{\omega^{(16)}}(x)]$ Boole fonksiyonu, $\omega^{(1)}, \omega^{(2)}, \dots, \omega^{(16)}$ tarafından belirlenen farklı doğrusal fonksiyonların birleşimi olarak görülebilen MM tipi bir bükük fonksiyon olsun. Çizelge 5.4'te verilen $\omega^{(i)}$ vektörlerine, $i = 1, 2, \dots, 16$, karşılık gelen $l_{\omega^{(i)}}$ doğrusal fonksiyonlarının oluşturduğu f bükük fonksiyonunu ele alalım. f bükük fonksiyonun toplamda 8 tane olan $l_{\omega^{(5)}}(1, 0, 1, 0)$, $l_{\omega^{(5)}}(1, 1, 1, 1)$, $l_{\omega^{(6)}}(0, 0, 0, 0)$, $l_{\omega^{(6)}}(1, 1, 0, 0)$, $l_{\omega^{(16)}}(0, 1, 0, 0)$, $l_{\omega^{(16)}}(0, 1, 0, 1)$, $l_{\omega^{(16)}}(0, 1, 1, 0)$ ve $l_{\omega^{(16)}}(0, 1, 1, 1)$ bitlerinin tümleyeni alındığında (116; 16; 7) profiline sahip 8 değişkenli dengeli Boole fonksiyonu elde edilir.

Çizelge 5.4. f bükük fonksiyonunu üreten $\omega^{(i)}$ vektörleri, $i = 1, 2, \dots, 16$.

$\omega^{(1)} = (0, 1, 1, 0)$	$\omega^{(5)} = (0, 0, 0, 0)$	$\omega^{(9)} = (0, 1, 0, 0)$	$\omega^{(13)} = (1, 1, 1, 1)$
$\omega^{(2)} = (0, 1, 0, 1)$	$\omega^{(6)} = (1, 1, 0, 0)$	$\omega^{(10)} = (1, 1, 1, 0)$	$\omega^{(14)} = (0, 0, 0, 1)$
$\omega^{(3)} = (1, 0, 1, 0)$	$\omega^{(7)} = (0, 0, 1, 1)$	$\omega^{(11)} = (0, 1, 1, 1)$	$\omega^{(15)} = (1, 0, 0, 1)$
$\omega^{(4)} = (1, 0, 1, 1)$	$\omega^{(8)} = (1, 1, 0, 1)$	$\omega^{(12)} = (0, 0, 1, 0)$	$\omega^{(16)} = (1, 0, 0, 0)$

BÖLÜM 6

PARÇACIK SÜRÜ OPTİMİZASYONU ALGORİTMASI

Optimizasyon, belirli bir seçenekler kümesi arasından en iyi alternatifi veya alternatifleri seçme sanatı veya belirli bir fonksiyonun kendi tanım alanında ulaşabileceği en büyük veya en küçük olası değeri bulma sürecidir. Optimize edilecek fonksiyon doğrusal veya doğrusal olmayan olabilir. Gerçek hayattaki birçok problemin çözümünü elde etmek, sağlam optimizasyon tekniklerinin yardımı olmadan mümkün değildir. Sağlam teknikler, optimizasyonun matematiksel teorisinden yola çıkılarak tasarlanmıştır. PSO önemli sağlam optimizasyon tekniklerinden biridir. PSO, sosyal etkileşim metaforuna dayanan yeni bir küresel optimizasyon yöntemidir [37, 38]. PSO, bilim ve mühendisliğin tüm alanlarında uygulama alanı bulmaktadır [39].

PSO algoritması çok sayıda aday çözüme sahip olarak başlar. Bu parçacıklar, en uygun çözümü (küresel en iyi çözüm) bulmak için arama uzayında sürekli olarak hareket ettirilir [40]. Bu süreçte, her parçacık arama uzayındaki hareketini belirler. Bunu, mevcut konumunu geçmişteki en iyi konum ile birleştirerek yapar. Sürü içerisinde yer alan tüm parçacıklar, uygunluk (fitness function) fonksiyonuna göre değerlendirilmektedir. Uygunluk fonksiyonu, elde edilen çözümün ne kadar iyi olduğunu belirlemek için kullanılan bir değerlendirme fonksiyonudur. Arama uzayındaki her bir parçacığın en iyi kendi çözümü (p_{best}) ve tüm parçacıkların en iyi çözümü (g_{best}) değerleri dikkate alınarak yenilenmektedir. Bulunan değerler elde edildikten sonra; parçacığın konumu ile hızı sırayla mevcut denklemlere göre yenilenir.

Algoritma, durdurma koşulu sağlanana kadar tekrarlanan dört ana adım aşağıdaki gibi özetlenebilir:

- Arama uzayındaki tüm parçacıklara başlangıçta rastgele konumlar ve hızlar atanır.
- Her bir parçacığın uygunluğunu değerlendirilir.
- Bireysel ve küresel en iyi pozisyonlar güncellenir.
- Her bir parçacığın hızı ve konumunu güncellenir.

Bu sürecin en önemli kısmı olan parçacık hızı güncelleme denklemi aşağıda verilmiştir:

$$V_i^{(k+1)} = w * V_i^{(k)} + c_1 * r_1 * (x_{i,best}^{(k)} - x_i^{(k)}) + c_2 * r_2 * (x_{gbest}^{(k)} - x_i^{(k)}) \quad (6.1)$$

$$x_i^{(k+1)} = x_i^{(k)} + V_i^{(k+1)} \quad (6.2)$$

Hız güncelleme denklemi üç kısma ayrılmaktadır. Birinci kısım hız değerinin atalet ağırlığını ifade eder. w aynı zamanda eylemsizlik ağırlığı olarak da bilinir ve genellikle 0.1 ile 1 aralığında değişmektedir. Parçacıkların hız değerlerinde ani değişiklikler olmaması istenmektedir ve parçacıklar bir önceki hızlarına göre hız güncellemesi yapmalıdırlar. Eğer bu şekilde bir ilerleme olmadığı takdirde parçacıklar çözüm uzayında ani yön değişiklikleri yaparlar ve bunun sonucunda uygun bir arama gerçekleştiremeyeceklerdir. İkinci ve üçüncü kısımda bulunan r_1 ve r_2 katsayıları rastgele sayılardır ve her iterasyonda yenilenir. r_1 ve r_2 katsayıları 0-1 aralığında değişmektedir. Burada aynı zamanda bulunan c_1 ve c_2 olarak isimlendirilen sabitler pozitif yönde hızlandırma katsayılarıdır ve genellikle $c_1 = c_2 = 0.5 - 1.0 - 1.5 - 2.0$ olarak problemin durumuna seçilebilir. İkinci kısmın (kişisel hafıza bölümü) görevi; parçacıkların konumlarının geçmişte elde ettikleri en iyi konuma (p_{best}) doğru çekilmeleridir. Bu kısımda elde edilen değer $c_1 * r_1$ değeri ile ölçeklenmiştir. Üçüncü kısma ise sosyal hafıza kısmı adı verilmektedir. Bu kısımda parçacıklar sürünün en iyi konum değerine doğru çekilirler [38]. Bu kısımda da elde edilen değer $c_2 * r_2$ değeri ile ölçeklenmiştir. Hız güncellemelerinin sonucunda elde edilen güncel hız değerine kısıtlama getirilebilir. Bu değer sabit bir değer olabileceği gibi dinamik değişen bir değer de olabilir [41, 42]. p_{best} ve g_{best} değerleri sırasıyla Denklem 6.3 ve Denklem 6.4'te gösterilmiştir.

$$Pbest_i^{(k)} = x_{i,best}^{(k)} = \begin{cases} x_{i,best}^{(k-1)} & \text{if } f(x_i^{(k)}) \geq f(x_{i,best}^{(k-1)}) \\ x_i^{(k)} & \text{if } f(x_i^{(k)}) < f(x_{i,best}^{(k-1)}) \end{cases} \quad (6.3)$$

$$gbest^k = x_{gbest}^{(k)} = \min \left\{ f(x_{1,best}^{(k)}), f(x_{2,best}^{(k)}), \dots, f(x_{n,best}^{(k)}) \right\} \quad (6.4)$$

Burada;

$x_i^{(k)}$: parçacığın anlık konumu,

$x_i^{(k+1)}$: parçacığın bir sonraki konumu,

$V_i^{(k)}$: parçacığın anlık hızı,

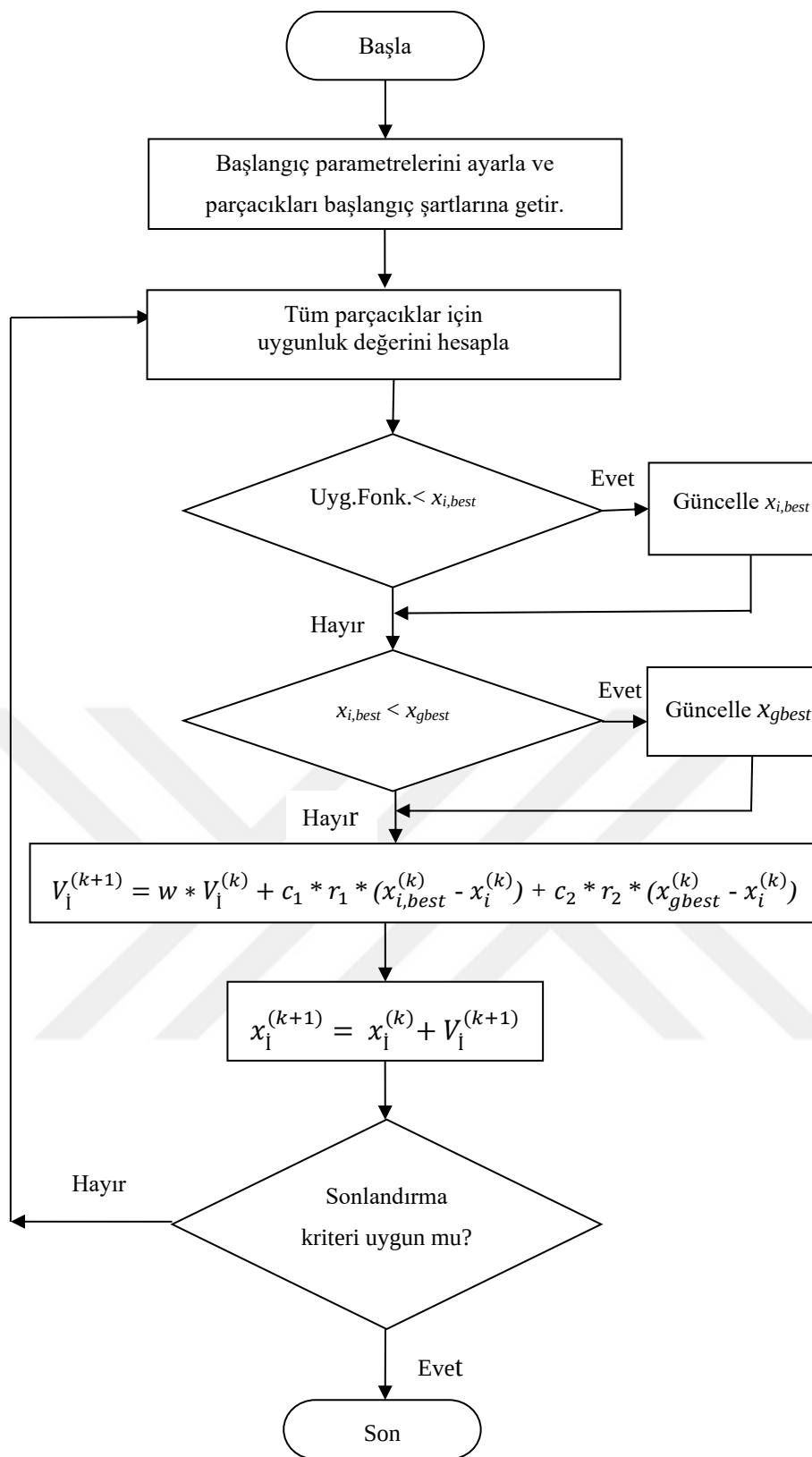
$V_i^{(k+1)}$: parçacığın bir sonraki hızı,

$V_i^{(Pbest)}$: p_{best} parçacığın hızı,

$V_i^{(gbest)}$: g_{best} parçacığının hızını temsil etmektedir.

Parçacık sürüsü optimizasyonu algoritmasının çalışma adımları aşağıdaki gibidir.

- Adım 1: Parçacıkların ilk çalışma anındaki konumları (x_i) arama uzayında rastgele olarak belirlenir.
- Adım 2: Sürüdeki tüm parçacıkların uygunluk değerleri hesaplanarak parçacıkların durumlarını değerlendirilir.
- Adım 3: Parçacık konumunun uygunluk değeri kendi yerel en iyi konumunun uygunluk değerinden daha iyi ise, parçacık konumunun yerel en iyi konumu p_{best} olarak güncellenir.
- Adım 4: Yerel en iyi parçacık vektörünün en iyi uygunluk değerine sahip parçacık global en iyi parçacık g_{best} olarak güncellenir.
- Adım 5: Denklem 6.1 ve 6.2' ye göre parçacıkların hız ve konumları güncellenir.
- Adım 6: Algoritma, durdurma kriterine ulaşıncaya kadar üçüncü adımdan itibaren tekrarlanarak devam eder.



Şekil 6.1 Parçacık Sürüsü Optimizasyonu Algoritma Yapısı

PSO algoritmasının sözde kodu (pseudo code);

For her parçacık (p) için
 Hız ve Konum değerlerini ata

```
End  
Do  
    For  $i = 1$  to  $p$   
        Uygunluk Değerini Hesapla;  
        Eğer parçacık uygunluk değeri,  $p_{best}$  parçacık uygunluk değerinden  
        daha iyi ise; bu parçacığı yeni  $p_{best}$  parçacığı olarak ata  
    End  
         $p_{best}$  parçacıklarının en iyisini  $g_{best}$  parçacığı olarak ata  
    For  $i = 1$  to  $p$   
         $p_{best}$  Değerini Güncelle;  
         $g_{best}$  Değerini Güncelle;  
        Hız ve Pozisyon Değerlerini Güncelle;  
    End  
While Sonlandırma Kriterine Ulaşıncaya Kadar
```



BÖLÜM 7

PARÇACIK SÜRÜ OPTİMİZASYONU

7.1. PARÇACIK SÜRÜ OPTİMİZASYONU KAVRAMLARI

PSO, kuşların ve balıkların sosyal davranışlarından esinlenen popülasyon tabanlı bir stokastik (değişken ve rastlantısal) optimizasyon algoritmasıdır [39]. PSO, optimizasyon ve arama problemlerine yaklaşık çözümler bulmak için yaygın olarak kullanılmaktadır. PSO'nun temel kavramları şu şekilde sıralanabilir:

7.1.1 Parçacıklar

PSO'da, optimizasyon problemine yönelik potansiyel bir çözüm "parçacık" olarak temsil edilir. Her parçacığın arama uzayında bir konumu ve bir hızı vardır ve sırasıyla Denklem 6.5 ve Denklem 6.6'da gösterilmiştir. Bir parçacığın konumu, optimizasyon probleminin olası bir çözümüne karşılık gelir.

$$X_i = X_{min} + (X_{max} - X_{min}) * random() \quad (6.5)$$

$$V_i = V_{max} * random() \quad (6.6)$$

V_{max} : Hız değişkeninin alabileceği en büyük değer.

7.1.2. Sürü

Bir grup parçacık topluca "sürü" olarak adlandırılır. Sürü, parçacıklarının konumlarını ve hızlarını yinelemeli olarak güncelleyerek arama uzayını araştırır.

7.1.3 Uygunluk Fonksiyonu

PSO, bir çözümün kalitesini değerlendiren bir uygunluk fonksiyonu gerektirir. Amaç, optimizasyon probleminin niteliğine bağlı olarak uygunluk fonksiyonunu minimize etmek veya maksimize etmektir.

7.1.4. Kişisel En İyi Değer

Parçacıklar iterasyonlar boyunca en iyi konum değerini ararlar. Her iterasyon adımı, bir parçacık, daha önce elde ettiği en iyi konum değeri ile güncel iterasyonda bulunan yeni konum değerini karşılaştırır. Eğer yeni konum değeri, o ana kadar bilinen en iyi kişisel konum değerinden daha iyi bir uygunluk sağlıyorsa, bu yeni konum değeri parçacığın yeni kişisel en iyi konumu olur. Parçacığın iterasyonlar boyunca, sürüdeki diğer parçacıklara bakmadan sadece kendi geçmişindeki değerlere bakarak bulduğu kendi en iyi değerine kişisel en iyi değer (p_{best}) denir.

7.1.5. Küresel (Global) En İyi Değer

PSO'da, sürü içindeki parçacıkların konum değerleri hesaba katıldığında elde edilen en iyi uygunluk değerine "global en iyi değer" (g_{best}) denir. Yeni iterasyonda bulunan en iyi değer g_{best} 'den daha iyi uygunluğa sahipse yeni g_{best} değeri olur.

7.1.6. Atalet Ağırlığı

Atalet ağırlığı kullanılarak, bir parçacığın bir önceki hızının yeni hızına olan etkisi kontrol altına alınır. Büyük atalet ağırlıkları, parçacığın çözüm uzayında genel aramalar yapmasını sağlar; yani, daha geniş bir alanda dolaşarak potansiyel çözümleri keşfeder. Bu durumda, parçacık, p_{best} ve g_{best} değerlerinden daha az etkilenir ve daha keşif odaklı çalışır. Öte yandan, küçük atalet ağırlıkları, parçacığın çözüm uzayında daha spesifik aramalar yapmasına neden olur. Bu durumda, parçacık, p_{best} ve g_{best} önceki deneyimlerinden daha fazla yararlanır ve en uygun çözüme daha yakın konumlara odaklanarak yakınsama yapar.

7.1.7. Hız Değeri

Hız değeri, bir parçacığın çözüm uzayında gezinmesini sağlayan en kritik etkidir. Hız değerleri pozitif ve negatif değerler olabilir, böylece parçacıklar çok yönlü bir şekilde hareket ederek arama yapabilirler. Ancak, hız değerleri kontrol edilmezse parçacıklar çözüm alanının dışına çıkabilir ve istenmeyen değerlere ulaşabilir. Bu durumu önlemek için hız değerine, V_{max} gibi kısıtlayıcı bir sınırlama getirilmiştir. V_{max} Denklem 6.7.'deki gibi hesaplanmaktadır.

$$V_{max} = (X_{max} - X_{min}) * \% R ; R \in [10 - 20] \quad (6.7)$$

Eğer bir parçacığın hız değeri limitini aşarsa bir kısıtlama getirilir.

$$V_i > V_{max} \text{ ise } V_i = V_{max}$$

$$V_i < -V_{min} \text{ ise } V_i = -V_{min}$$

7.1.8. Hızlandırma Katsayıları

Hızlandırma katsayılarından c_1 , parçacıkların bireysel en iyi konumları (p_{best} değerleri) üzerine olan etkisini kontrol ederken, c_2 parçacıkların global en iyi konumları (g_{best} değerleri) üzerine olan etkisini kontrol eden katsayılardır. Hızlandırma katsayılarının büyük olması, parçacıkların birbirinden uzaklaşıp ayrılmasına neden olabilir. Bu durumda geniş bir çözüm alanı taranabilir. Öte yandan, küçük hızlandırma katsayıları, parçacıkların hareketlerini kısıtlar ve çözüm uzayının yeterince keşfedilememesine neden olabilir. Hızlandırma katsayıları, problemin türüne bağlı olarak farklı değerler alabilir.

7.1.9 Sonlandırma Kriteri

PSO'da sonlandırma kriteri, genellikle kullanıcı tarafından belirlenen sabit bir iterasyon sayısı, reset sayısı, belirlenmiş bir çalışma zamanı veya belirlenen iterasyonun global en iyi değerleri (g_{best}) arasındaki farkın belirli bir eşik değer altına düşmesi durumu olabilir.

7.2. PARÇACIK SÜRÜ OPTİMİZASYONU ARAMA SONUÇLARI

Çalışmamızda, 8, 10 ve 12 değişkenli Boole fonksiyonları üzerinde bir dizi deney gerçekleştirilmiş olup, bu deneylerin sonuçlarına dayanarak parametre değerlerini belirlemek üzere bir parametre ayarlama aşaması gerçekleştirilmiştir. Özel olarak, her bir değişken sayısı için başlangıçta rasgele olarak parçacık sayısı 200 olarak belirlenmiştir. ve 50, 100, 150 ve 200 olan seçim büyüklükleri ile deneyler yapılmıştır. 6.1’ de verilen denklem ile c_1 , c_2 adı verilen hızlanma katsayıları sabitleri ve w atalet ağırlığı ile 18 adet tüm kombinasyonlar denenerek en iyi doğrusal olmama değerinin hangi parametreler kullanılarak elde edildiği tespit edilmiştir. Tüm kombinasyonlara ait tablo ile en iyi kombinasyon parametre tablosu Çizelge 7.1 - Çizelge 7.2’de gösterilmiştir.

PSO’nun başarısı kontrol parametrelerinin değerlerine çok yakından bağlılık göstermektedir. Bunları atalet veya eylemsizlik ağırlığı (ω), rastgele değerler (r_1 ve r_2), hızlanma katsayıları (c_1 , c_2) olarak sıralayabiliriz. Bu amaçla, PSO kontrol parametrelerine odaklanan ve parçacık arama davranışını iyileştirmeyi amaçlayan bir çalışma yürütülerek, yerel ve global arama arasındaki denge artırılmalıdır.

Çizelge 7.1. 8, 10 ve 12 değişkenli Boole fonksiyonları için bilinen en iyi doğrusal olmama değerlerini veren tüm kombinasyonlar.

Parametreler	Tüm Kombinasyonlar
$c_1 - c_2 - w$ değerleri	(1, 1, 0.5) - (1, 1, 1) - (1, 1.5, 0.5) - (1, 1.5, 1) (1, 2, 0.5) - (1, 2, 1) - (1.5, 1, 0.5) - (1.5, 1, 1) - (1.5, 1.5, 0.5) - (1.5, 1.5, 1) - (1.5, 2, 0.5) - (1.5, 2, 1) (2, 1, 0.5) - (2, 1, 1) - (2, 1.5, 0.5) - (2, 1.5, 1) - (2, 2, 0.5) - (2, 2, 1)

Çizelge 7.2. 8 (Standart PSO), 8 (PSO Luca) - 8 (PSO Luca-Reset), 10 (PSO Luca) - 10 (PSO Luca - Reset), 12 (PSO Luca) değişkenli Boole fonksiyonları için bilinen en iyi doğrusal olmama değerlerini veren kombinasyonlar.

Değişken sayısı	En iyi Kombinasyonlar ($c_1 - c_2 - w$)
8 (Standart PSO)	(1, 1, 1) - (1.5, 1, 0.5) (1.5, 1, 1) - (1.5, 2, 0.5) (1, 2, 0.5) - (1, 2, 1)
8 (PSO Luca) - 8 (PSO Luca-Reset)	(2, 1, 0.5) (2, 2, 0.5)
10 (PSO Luca) - 10 (PSO Luca-Reset)	(1, 1, 1) - (2, 1, 0.5) (1, 1, 1) - (2, 1, 0.5)
12 (PSO Luca)	(1, 1, 1) - (2, 1, 0.5)

Çalışmamızda, dengeli Boole fonksiyonlarının doğrusal olmama özelliğini geliştirmeyi amaçladığımız için, belirtilen kombinasyonlar ilgili doğrusal olmama sonuçlarına göre değerlendirilmiştir. Bir kombinasyon, elde ettiği ortalama değer baz alındığında, kötü bir çözümün iyi çözümlerin göz ardı edilmesine neden olabileceği açıkça anlaşılmaktadır. Bu sebeple, ortalama değerler yerine, kombinasyonların ulaştıkları en üst düzey doğrusal olmama değerleri dikkate alınmıştır. Standart PSO ve PSO-Luca 8 değişkenli Boole fonksiyonları için, her parametre kombinasyonunun bilinen en iyi doğrusal olmama değeri olan 116'yı elde ettiği gözlenmiştir [43]. 10 değişkenli durum için, (1, 1, 1) - (2, 1, 0.5) kombinasyon sırasıyla bilinen en iyi doğrusal olmama değeri olan 492 değerini elde etmektedir. 12 ve değişkenli durum için, (1, 1, 1) - (2, 1, 0.5) kombinasyonları sırasıyla bilinen en iyi doğrusal olmama değeri olan 2010 değerini elde edilemeyip, bulunan değer 2002 olarak gözlemlenmiştir. Bu kombinasyonlar Çizelge 6.3 ve Çizelge 6.4' te verilmiştir.

Çizelge 7.3. PSO deneysel parametre değerleri.

Parametre	Değer
Başlangıç popülasyonu	Rasgele – 200
n değişkeni değerleri	8 - 10 - 12
W	0.5 - 1.0
c_1 ve c_2	1.0 - 1.5 - 2.0
r_1 ve r_2	Rasgele
V_{min} ve V_{max}	-3.0 - 3.0
Parçacık popülasyonu	50, 100, 200
İterasyon sayısı	2000,.....,20000
Durdurma kriteri	Durdurma kriteri karşılanana kadar.

Çizelge 7.5. 200 parçacık için tüketilen süreler ve dengeli fonksiyonların sayısı.

N	Tüketilen süreler	$N_{dengeli} (n)$
8 (Standart PSO)	240 sn.	2^{41}
8 (PSO-Luca)	78 sn.	2^{41}
8 (PSO-Luca-Reset)	170 sn.	2^{41}
10 (Standart PSO)	11 dk 55 sn.	2^{100}
10 (PSO-Luca)	165 sn.	2^{100}
10 (PSO-Luca-Reset)	18 dk 38sn.	2^{100}
12 (Standart PSO)	53 dk 33sn.	2^{234}
12 (PSO-Luca)	14 dk 15 sn.	2^{234}
12 (PSO-Luca-Reset)	23 dk.32 sn.	2^{234}

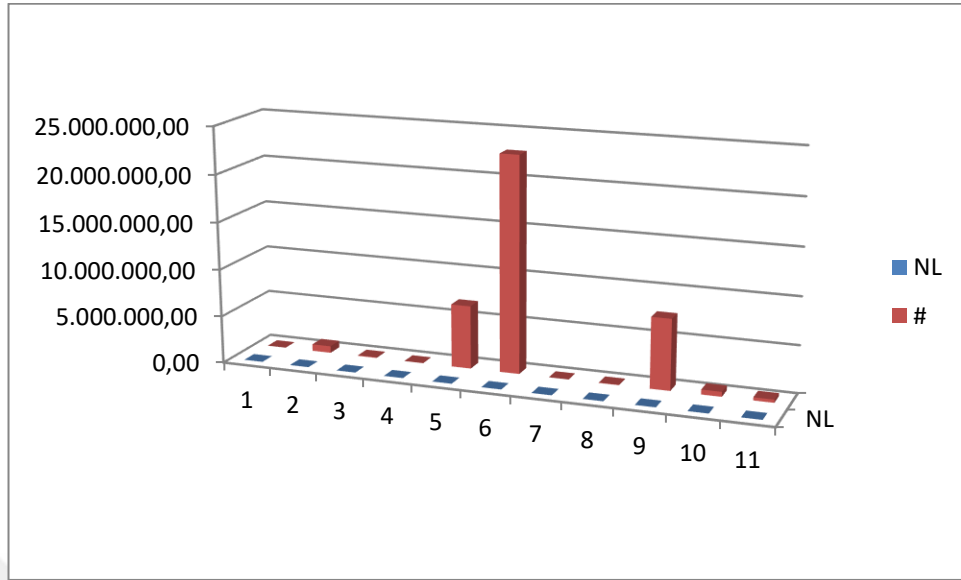
Sıfırlama adımının uygulandığı ve uygulanmadığı durumlarda, en iyi nesil çıktısı olarak üretilen 200000 ($=20000 \times 10$) 8 değişkenli Boole fonksiyonun kriptografik özelliklerine göre sınıflandırılması Çizelge 7.4'te verilmiştir.

Çizelge 7.5. Sıfırlama adımının (a) uygulandığı ve (b) uygulanmadığı durumlar için 8 değişkenli 38699837 Boole fonksiyonu ile 8 değişkenli 4514024 Boole fonksiyonu kriptografik özelliklerine göre dağılımları.

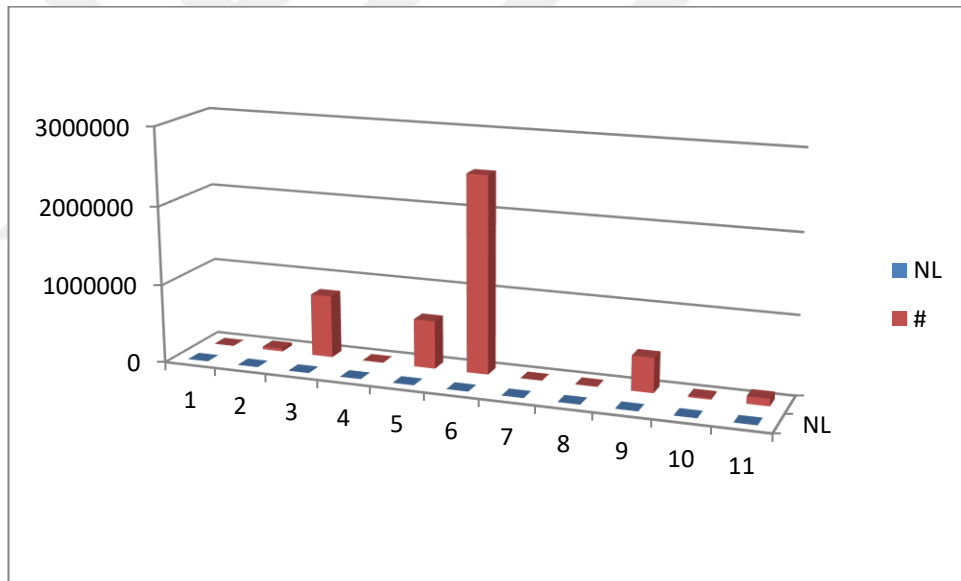
<i>NL</i>	<i>AI</i>	<i>d</i>	#	<i>NL</i>	<i>AI</i>	<i>d</i>	#
112	24	6	2245	112	16	6	277
112	24	7	712133	112	24	6	36987
112	32	5	65771	112	24	7	797307
112	32	6	12015	112	32	6	3741
114	24	7	6685653	112	32	7	610720
114	32	7	22838683	114	24	7	2503967
116	16	7	688	116	16	7	716
116	24	6	40101	116	24	6	4029
116	24	7	7494567	116	24	7	443524
116	32	6	518538	116	32	6	18919
116	32	7	329443	116	32	7	93837

(a)
(b)

Çizelge 7.5'ten anlaşıldığı üzere, sıfırlama adımının uygulandığı durumda, doğrusal olmama değeri 116 olan Boole fonksiyonları daha fazla üretilmiş ve aynı zamanda en iyi mutlak gösterge değeri olan 16 elde edilmiştir. Cebirsel derecesi 6 olan Boole fonksiyonları, bu adımın uygulandığı durumda üretilmiş olsa da, bu fonksiyonların sayısının oldukça sınırlı olduğuna dikkat edilmelidir. Bu sonuçlar, Çizelge 6.5'teki dağılımlara karşılık gelen grafikler Şekil 6.2 ve Şekil 6.3'ten de gözlenebilmektedir.



Şekil 7.1 Parçacık Sürüsü Optimizasyonu Sıfırlama Adım Grafiği



Şekil 7.2 Parçacık Sürüsü Optimizasyonu Sıfırlama Adımı Uygulanmayan Grafik

Çizelge 7.6. Sıfırlama adımının (PSO Luca-Reset) uygulandığı ve (PSO Luca) uygulanmadığı en iyi durumlar için 10 ve 12 değişkenli Boole fonksiyonlarının kriptografik özelliklerine göre dağılımları.

N	$c_1 - c_2 - w$	$NL- AI- d$	#
10 (Standart PSO)	1 - 1 - 1	490 - 40 - 9	1013/391278
		492 - 40 - 9	358/391278
10 (PSO Luca)	1 - 1 - 1	492 - 40 - 9	374/1219262
		492 - 48 - 8	199/1219262
10 (PSO Luca-Reset)	2 - 1 - 0.5	490 - 40 - 9	689/1330251
		492 - 40 - 9	517/1330251
12 (Standart PSO)	1 - 1 - 1	2002 - 80 - 11	12224/1875458
		2002 - 88 - 11	5342/1875458
12 (PSO Luca)	1 - 1 - 1	2002 - 72 - 11	6296/1866636
		2002 - 80 - 11	14547/1866636
12 (PSO Luca-Reset)	2 - 1 - 0.5	2002 - 72 - 11	8935/1691439
		2002 - 80 - 11	13571/1691439

PSO algoritmasında $n = 8, 10$ ve 12 değerleri için elde edilen en iyi sonuçlar Çizelge 7.6'da gösterilmiştir.

BÖLÜM 8

SONUÇLAR

Çizelge 7.7’de, kriptografik özellikler (doğrusal olmama; mutlak gösterge; cebirsel derece) üçlüsü ile ifade edilerek, çift $n \in [8, 26]$ için elde ettiğimiz en iyi sonuçlar özetlenmekte ve [9], [25-27] çalışmalarındaki mevcut en iyi sonuçlarla karşılaştırılmaktadır. Görüldüğü gibi, tasarladığımız GA’nın bükük bir fonksiyonun minimum sayıda ($2^{n/2-1}$) bitinin çevrilmesiyle üretilen n değişkenli dengeli Boole fonksiyonlarına uygulanmasıyla, $n = 12, 14, \dots, 26$ için daha önce bilinmeyen ($2^{n/2}$ ’den küçük) daha iyi mutlak gösterge değerleri elde edilmiştir. Buna ek olarak, karşılık gelen doğrusal olmama değerlerinin $n = 16, 18, \dots, 26$ için $2^{n-1} - 2^{n/2}$ değerini aştığı görülmektedir. Sonuçlarımız ayrıca $n = 8, 10, \dots, 16$ için, bükük bir fonksiyona en yakın mesafede olan ve bilinen en iyi doğrusal olmama değerine sahip dengeli Boole fonksiyonlarının örneklerini göstermektedir. Bildiğimiz kadarıyla, mutlak gösterge değerleri üzerinde aşikâr olmayan bir alt sınır yoktur ve sadece dengeli bir Boole fonksiyonunun mutlak gösterge değerinin en düşük 8 olabileceği bilinmektedir. Bu nedenle, Çizelge 7.7’de sunulan sonuçlar [27] çalışmasındaki mutlak gösterge değerlerini iyileştirse de, özellikle büyük değişken sayıları için yeterli hesaplama gücü ile daha fazla iyileştirme elde etmek oldukça olasıdır. Öte yandan, uzun süredir devam eden bir açık problem olarak, $n \geq 8$ için $2^{n-1} - 2^{n/2} + n \lfloor n/2 \rfloor$ ’den daha büyük doğrusal olmama değerine ulaşan çift n değişkenli dengeli bir Boole fonksiyonunun var olup olmadığı hala bilinmemektedir ve bu nedenle, bu doğrusal olmama değerine ulaşmak oldukça zor görünmektedir. Örneğin, doğrusal olmama değeri 118 olan 8 değişkenli dengeli bir Boole fonksiyonunun var olup olmadığı literatürde bilinmemektedir.

Çalışmamızda, dengeli Boole fonksiyonlarının en önemli iki kriptografik özelliği olan doğrusal olmama ve mutlak gösterge ele alınmıştır. Bir Boole fonksiyonunun bir kriptosistemde kullanılabilmesi için esneklik, cebirsel bağımsızlık ve hızlı cebirsel

bağışıklık gibi diğer kriptografik özelliklerinin de dikkate alınması gerekmektedir. Arama stratejimizin, büyük fonksiyonlara olan mesafenin artırılması ve uygunluk fonksiyonunun buna göre tasarlanması ile, bahsedilen diğer kriptografik özellikleri eniyilemek için kullanılmasının mümkün olduğunu düşünülmektedir. Ancak, bu kriptografik özellikler arasında bir denge söz konusu olduğundan ve bir özelliği iyileştirmek başka bir özelliğin kötüleşmesine yol açabileceğinden, diğer kriptografik özellikleri eniyilerken Çizelge 7.7’de sunulan en iyi kriptografik özelliklerin kötüleşmesi oldukça olasıdır. Örneğin, esneklik derecesi 1 olan Boole fonksiyonlar için bilinen en iyi mutlak gösterge değerlerine sahip iki sınıfın inşa edildiği [44] çalışması ile karşılaştırıldığında, Çizelge 7.1’de elde ettiğimiz mutlak gösterge değerlerinin daha iyi olduğu görülebilir.

Çizelge 7.7. Elde ettiğimiz en iyi GA profillerin literatürdeki en iyi sonuçlarla karşılaştırılması (Herhangi bir f Boole fonksiyonun profili $(NL_f; \Delta_f; d_f)$ üçlüsü ile gösterilmektedir.).

Kaynak	$n = 8$	$n = 10$	$n = 12$	$n = 14$
[25]	(116; 16; 7)	(488; 40; 9)	(2002; 64; 11)	(8102; 104; 13) (8104; 112; 13)
[9]	-	(488; 24; 9)	-	-
[27]	-	-	(1996; 56; 11)	(8106; 96; 13)
[20]	(116; 24; 7)	(488; 40; 9)	(2002; 72; 11)	-
[22]	(116; 24; -)	(488; 40; -)	(2002; 72; -)	-
Sonuçlar	(116; 16; 7)	(480; 24; 6) (492; 40; 9)	(1984; 40; 7) (1984; 48; 11) (2010; 80; 11)	(8064; 88; 13) (8120; 144; 12)

Kaynak	$n = 16$	$n = 18$	$n = 20$
[26]	-	(130,664; 480; 17)	-
[27]	(32,604; 160; 15)	(130,762; 312; 17)	(523,688; 600; 19)
Sonuçlar	(32,516; 152; 15) (32,628; 288; 14)	(130,752; 256; 17)	(523,676; 400; 19)
Kaynak	$n = 22$	$n = 24$	$n = 26$
[26]	(2,095,484; 1880; 21)	-	(33,547,436; 7856; 25)
[27]	(2,096,020; 1224; 21)	(8,386,392; 2360; 23)	(33,550,064; 4584; 25)
Sonuçlar	(2,095,958; 592; 21)	(8,386,318; 904; 23)	(33,549,996; 1360; 25)

Çizelge 7.8. Elde ettiğimiz en iyi PSO profillerin literatürdeki en iyi sonuçlarla karşılaştırılması (Herhangi bir f Boole fonksiyonun profili $(NL_f; \Delta_f; d_f)$ üçlüsü ile gösterilmektedir.).

Kaynak	$n = 8$	$n = 10$	$n = 12$
[25]	(116; 16; 7)	(488; 40; 9)	(2002; 64; 11)
[9]	-	(488; 24; 9)	-
[27]	-	-	(1996; 56; 11)
[20]	(116; 24; 7)	(488; 40; 9)	(2002; 72; 11)
[22]	(116; 24; -)	(488; 40; -)	(2002; 72; -)
Sonuçlar	(116; 16; 7)	(490; 40; 9)	(2002; 72; 11)
	(116; 24; 7)	(492; 40; 9)	(2002; 80; 11)

Luca'nın [21] PSO ile bulduğu en iyi doğrusal olmama değerleri (116, 6, 32) (480, 80, 9) (1972, 208, 11); PSO çalışmamızla iyileştirilmiştir.

Çizelge 7.9. Elde ettiğimiz en iyi GA ve PSO profillerin karşılaştırılması (Herhangi bir f Boole fonksiyonun profili $(NL_f; \Delta_f; d_f)$ üçlüsü ile gösterilmektedir.).

Kaynak	$n = 8$	$n = 10$	$n = 12$
GA Sonuçlar	(116; 16; 7)	(480; 24; 6)	(1984; 40; 7)
		(492; 40; 9)	(1984; 48; 11)
			(2010; 80; 11)
PSO Sonuçlar	(116; 16; 7)	(490; 40; 9)	(2002; 72; 11)
	(116; 24; 7)	(492; 40; 9)	(2002; 80; 11)
En İyi Sonuçlar	(116; 16; 7)	(492; 40; 9)	(2010; 80; 11)

KAYNAKLAR

1. Shannon, C. E. "Communication theory of secrecy systems", *The Bell System Technical Journal*, 28(4):656-715 (1949).
2. Aumasson, J.-P., Fischer, S., Khazaei, S., Meier, W., Rechberger, C., "New Features of Latin Dances: Analysis of Salsa, ChaCha, and Rumba", *Fast Software Encryption*, 470-488,(2008).
3. Banik, S., Maitra, S., Sarkar, S., "A Differential Fault Attack on the Grain Family of Stream Ciphers", *Cryptographic Hardware and Embedded Systems – CHES* , 122-139,(2012).
4. Meier, W., Staffelbach, O. "Fast correlation attacks on certain stream ciphers", *Journal of Cryptology*, 1(3):159-176 (1989).
5. Massey, J. "Shift-register synthesis and BCH decoding", *IEEE Transactions on Information Theory*, 15(1):122-127 (1969).
6. Matsui, M., "Linear Cryptanalysis Method for DES Cipher", *Advances in Cryptology — EUROCRYPT '93*, 386-397,(1994).
7. Biham, E., Shamir, A. "Differential cryptanalysis of DES-like cryptosystems", *Journal of Cryptology*, 4(1):3-72 (1991).
8. Carlet, C. Boolean Functions for Cryptography and Error-Correcting Codes. In: Boolean Models and Methods in Mathematics, Computer Science, and Engineering. Crama, Y., Hammer, P. L. (editors), *Cambridge University Press. Cambridge*, 257-397 (2010).

9. Kavut, S., Maitra, S., Yucel, M. D. "Search for Boolean Functions With Excellent Profiles in the Rotation Symmetric Class", *IEEE Transactions on Information Theory*, 53(5):1743-1751 (2007).
10. Patterson, N. J., Wiedemann, D. H. "The covering radius of the (215, 16) Reed-Muller code is at least 16276", *IEEE Trans Inf Theory*, 29(3):354-355 (1983).
11. Hou, X.-d. "On the norm and covering radius of the first-order Reed-Muller codes", *IEEE Transactions on Information Theory*, 43(3):1025-1027 (1997).
12. Dobbertin, H., "Construction of bent functions and balanced Boolean functions with high nonlinearity", *Fast Software Encryption*, 61-74,(1995).
13. Millan, W., Clark, A., Dawson, E., "An effective genetic algorithm for finding highly nonlinear boolean functions", *Information and Communications Security*, 149-158,(1997).
14. Millan, W., Clark, A., Dawson, E., "Smart hill climbing finds better boolean functions", *In Workshop on Selected Areas in Cryptology - Workshop Record*, pages 50-63, (1997).
15. Millan, W., Clark, A., Dawson, E., "Heuristic design of cryptographically strong balanced Boolean functions", *Advances in Cryptology — EUROCRYPT'98*, 489-499,(1998).
16. Clark, J. A., Jacob, J. L., "Two-Stage Optimisation in the Design of Boolean Functions", *Information Security and Privacy*, 242-254,(2000).
17. Clark, J. A., Jacob, J. L., Stepney, S., Maitra, S., Millan, W., "Evolving Boolean Functions Satisfying Multiple Criteria", *Progress in Cryptology — INDOCRYPT*, 246-259,(2002).

18. Kavut, S., Yücel, M. D., "Improved Cost Function in the Design of Boolean Functions Satisfying Multiple Criteria", ***Progress in Cryptology - INDOCRYPT*** , 121-134,(2003).
19. Burnett, L. D., "Heuristic optimization of Boolean functions and substitution boxes for cryptography", ***Queensland University of Technology***, (2005).
20. Izbenko, Y., Kovtun, V., Kuznetsov, A., "The Design of Boolean Functions by Modified Hill Climbing Method", ***Sixth International Conference on Information Technology: New Generations***, Las Vegas, NV, USA, 356-361,(2009).
21. Mariot, L., Leporati, A. Heuristic Search by Particle Swarm Optimization of Boolean Functions for Cryptographic Applications. In: Proceedings of the Companion Publication of the 2015 ***Annual Conference on Genetic and Evolutionary Computation. Madrid, Spain: Association for Computing Machinery***, 1425–1426 (2015).
22. Behera, P. K., Gangopadhyay, S. "An improved hybrid genetic algorithm to construct balanced Boolean function with optimal cryptographic properties", ***Evolutionary Intelligence***, 15(1):639-653 (2022).
23. Chen, V. Y., "The Gowers norm in the testing of Boolean functions", Doctoral dissertation, ***Massachusetts Institute of Technology***, Massachusetts (2009).
24. Zhang, X. M., Yheng, Z., "GAC – the criterion for global avalanche characteristics of cryptographic functions", ***Journal for Universal Computer Science***, 1 (5): 316-333 (1995).
25. Burnett, L., Millan, W., Dawson, E., Clark, A., "Simpler methods for generating better Boolean functions with good cryptographic properties", ***Australasian Journal of Combinatorics***, 29: 231-248 (2004).

26. Tang D., Maitra S., “Construction of n -variable ($n \equiv 2 \pmod{4}$) balanced Boolean functions with maximum absolute value in autocorrelation spectra $< 2^{n/2}$ ”, ***IEEE Transactions on Information Theory***, 64 (1): 393-402 (2018).
27. Kavut, S., Maitra, S., Tang, D., “Construction and search of balanced Boolean functions on even number of variables towards excellent autocorrelation profile”, ***Designs, Codes and Cryptography***, 87: 261-276 (2019).
28. Dillon, J. F., “Elementary Hadamard difference sets”, Ph.D. dissertation, ***University of Maryland***, Maryland (1974).
29. Djurasevic, M., Jakobovic, D., Mariot, L., Picek, S., “A survey of metaheuristic algorithms for the design of cryptographic Boolean functions”, ***Cryptography and Communications*** (2023).
30. Cusick, T. W., Stănică, P., “Cryptographic Boolean functions and applications”, ***Elsevier, Academic Press***, Cambridge (2009).
31. Yücel, M. D., “Alternative nonlinearity criteria for Boolean functions”, Memorandum No. 2001-1, ***Middle East Technical University***, Ankara (2001).
32. Holland, J. H., “Adaptation in natural and artificial systems”, ***University of Michigan Press***, Michigan (1975).
33. McFarland, R. L., “A family of noncyclic difference sets”, ***Journal of Combinatorial Theory - Series A***, 15: 1-10 (1973).
34. Clark, J. A., Jacob, J. L., Stepney, S., Maitra, S., Millan, W., “Evolving Boolean functions satisfying multiple criteria”, ***Indocrypt 2002***, LNCS, vol. 2551, 246-259 (2002).
35. İnternet: GitHub, “Balanced Boolean functions on even number of variables achieving absolute indicator less than $2^{n/2}$ ”, ***https://github.com/Selcuk-kripto/imp_AC*** (2023).

36. Langevin, P., Leander, G., “Counting all bent functions in dimension eight 99270589265934370305785861242880”, *Designs, Codes and Cryptography*, 59: 193-205 (2011).
37. Zhang, Y.; Wang, S.; Ji, G. “A Comprehensive Survey on Particle Swarm Optimization Algorithm and Its Applications”, *Math. Probl. Eng.* 1–38, (2015).
38. R.C. Eberhart and J. Kennedy, “A New Optimizer using Particle Swarm Theory”, *In Proceedings of the Sixth International Symposium on Micromachine and Human Science*, pp. 39–43, (1995).
39. J. Kennedy and R.C. Eberhart, “Particle Swarm Optimization”, *In Proceedings of the IEEE International Joint Conference on Neural Networks*, pp. 1942–1948. IEEE Press, (1995).
40. J. Kennedy, “Small Worlds and Mega-Minds: Effects of Neighborhood Topology on Particle Swarm Performance”, *In Proceedings of the IEEE Congress on Evolutionary Computation*, vol. 3, pp. 1931–1938 (1999).
41. Valle, Y. D., Vanayagamoorthy, G. K., Mohagheghi, S., Hernandez, J. C., Harley R. G., "Particle swarm optimization: basic concepts, variants and applications in power system", *IEEE Transactions on Evolutionary Computations*, 12: 171-195 (2008).
42. Helwig, S., Neumann, F. and Wanka R., "Particle swarm optimization with velocity adaptation", *International Conference on Adaptive and Intelligent Systems, Klagenfurt*, 146-151 (2009).
43. Djurasevic, M., Jakobovic, D., Mariot, L., Picek, S., “A survey of metaheuristic algorithms for the design of cryptographic Boolean functions” . *Cryptography and Communications*”, 15: 1171-1197 (2023).
44. Li, Y., Kan, H., Peng, J., Tan, C. H., “SAO 1-resilient functions with lower absolute indicator in even variables”, *IEEE Access*, 8: 222377-222384 (2020).

EK AÇIKLAMALAR A.

**8, 10 VE 12 DEĞİŞKENLİ BOOLE FONKSİYONLARIN
DOĞRULUK TABLOLARI**

(2010; 80; 11):

[illegible]

33CC33CC33CC33CC666699999666699999669999669966669930
66999966669999665555AAAA5555AAAA3333CCCCCCCC333333
5AA5A55AA55A5AA566996699996699660000FFFFFFFFF000055
8CFF21FFFF00FF2355AAAA5555AAAA55200008000031008066
696969696969690F0F0F0F0F0F0F0F3CC33CC33CC33CC3555
3CC33CC3C33CC33CC66996699669966990FF00FF00FF00FF0699

ÖZGEÇMİŞ

Erol ÖZÇEKİÇ. İlk, orta ve liseyi Balıkesir’de okudu. Liseyi Anadolu Teknik Lisesi Bilgisayar Bölümü’nde tamamladı.1997-2001 yılında Marmara Üniversitesi Teknik Eğitim Fakültesi’nden mezun oldu. 2001 yılında Balıkesir Üniversitesi Bandırma Meslek Yüksekokulu’nda Öğretim Görevlisi olarak çalışmaya başladı. 2015 yılında Balıkesir Üniversitesi Bigadiç Meslek Yüksekokulu’na nakil oldu. Halen çalışmaya Balıkesir Üniversitesi Balıkesir Meslek Yüksekokulu Bilgisayar Programcılığı Bölümü’nde devam etmektedir. Evli ve iki çocuğu bulunmaktadır.