**T.C.**

**FIRAT ÜNİVERSİTESİ**

**FEN BİLİMLERİ ENSTİTÜSÜ**

****

**KAOTİK YER DEĞİŞTİRME KUTULARININ PERFORMANS İYİLEŞTİRMESİ İÇİN YENİ ALGORİTMALARIN GELİŞTİRİLMESİ**

**Yaşar Selim BAHÇECİ**

Yüksek Lisans Tezi

YAZILIM MÜHENDİSLİĞİ ANABİLİM DALI

AĞUSTOS 2020

**T.C.**

**FIRAT ÜNİVERSİTESİ**

**FEN BİLİMLERİ ENSTİTÜSÜ**

Yazılım Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

**KAOTİK YER DEĞİŞTİRME KUTULARININ PERFORMANS**

****

**İYİLEŞTİRMESİ İÇİN YENİ ALGORİTMALARIN GELİŞTİRİLMESİ**

Tez Yazarı

**Yaşar Selim BAHÇECİ**

Danışman

Doç. Dr. Fatih ÖZKAYNAK

AĞUSTOS 2020

ELAZIĞ

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  | **T.C.** |  |  |
|  |  |  | **FIRAT ÜNİVERSİTESİ** |  |  |
|  |  |  | **FEN BİLİMLERİ ENSTİTÜSÜ** |  |  |
|  |  |  | Yazılım Mühendisliği Anabilim Dalı |  |  |
|  |  |  | Yüksek Lisans Tezi |  |  |
| Başlığı: | |  |  | |  |
| Kaotik Yer Değiştirme Kutularının Performans İyileştirmesi için Yeni | | |  |
|  |  | Algoritmaların Geliştirilmesi | |  |  |
| Yazarı: | | Yaşar Selim BAHÇECİ | |  |  |
| İlk Teslim Tarihi: | | 14.07.2020 | |  |  |
| Savunma Tarihi: | | 13.08.2020 | |  |  |
|  |  |  |  |  |  |
|  |  |  | **TEZ ONAYI** |  |  |
|  |  |  | Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına göre hazırlanan bu tez | |  |
|  |  |  | aşağıda imzaları bulunan jüri üyeleri tarafından değerlendirilmiş ve akademik | |  |
|  |  |  | dinleyicilere açık yapılan savunma sonucunda OYBİRLİĞİ ile kabul edilmiştir. | |  |
|  |  |  |  | *İmza* |  |
| Danışman: | |  | Doç. Dr. Fatih ÖZKAYNAK | Onayladım |  |
|  |  |  | Fırat Üniversitesi Yazılım Mühendisliği |  |  |
|  | |  |  |  |  |
| Başkan: | |  | Prof. Dr. Erkan TANYILDIZI | Onayladım |  |
|  |  |  | Fırat Üniversitesi Yazılım Mühendisliği |  |  |
|  | |  |  |  |  |
| Üye: | |  | Dr. Öğr. Üyesi Fatih TOPALOĞLU | Onayladım |  |
|  |  |  | Turgut Özal Üniversitesi Bilgisayar Mühendisliği |  |  |
|  |  |  |  |  |  |



Bu tez, Enstitü Yönetim Kurulunun ......./......../20....... tarihli toplantısında tescillenmiştir.

*İmza*

Prof. Dr. Soner ÖZGEN

Enstitü Müdürü

**BEYAN**

Fırat Üniversitesi Fen Bilimleri Enstitüsü tez yazım kurallarına uygun olarak hazırladığım “Kaotik Yer Değiştirme Kutularının Performans İyileştirmesi için Yeni Algoritmaların Geliştirilmesi” Başlıklı Yüksek Lisans Tezimin içindeki bütün bilgilerin doğru olduğunu, bilgilerin üretilmesi ve sunulmasında bilimsel etik kurallarına uygun davrandığımı, kullandığım bütün kaynakları atıf yaparak belirttiğimi, maddi ve manevi desteği olan tüm kurum/kuruluş ve kişileri belirttiğimi, burada sunduğum veri ve bilgileri unvan almak amacıyla daha önce hiçbir şekilde kullanmadığımı beyan ederim.

13.08.2020

**Yaşar Selim BAHÇECİ**

****

**ÖNSÖZ**

Günümüzde bilgi güvenliğinin önemi giderek artmaktadır. Bilgi güvenliği için kriptolojik algoritmalar önem arz etmektedir. Bu amaçla kullanılan kaotik yer değiştirme kutularının performans iyileştirmesi için böyle bir çalışmaya gerek duyduk ve bu çalışmada yer değiştirme kutularının performans iyileştirmesi için yeni bir son işlem tekniği önerilmiştir.

Bu çalışmada ve lisansüstü öğrenimim süresince sürekli bana destek olan ve beni cesaretlendiren danışmanım Doç. Dr. Fatih ÖZKAYNAK’ a ve Tez yazımı süresince bana destek olan Arş. Gör. Yılmaz AYDIN’ a sonsuz teşekkürlerimi sunarım.

Bu tez çalışması, Fırat Üniversitesi Bilimsel Araştırma Projeleri Koordinasyon Birimi (FÜBAP) tarafından **TEKF.19.18** protokol numaralı proje ile desteklenmiştir.



**Yaşar Selim BAHÇECİ**

ELAZIĞ, 2020

iv

**İÇİNDEKİLER**

Sayfa

[ÖNSÖZ](#page5) [İV](#page5)

[İÇİNDEKİLER](#page6) [V](#page6)

[ÖZET](#page7) [Vİ](#page7)

[ABSTRACT](#page8) [Vİİ](#page8)

[ŞEKİLLER LİSTESİ](#page9) [Vİİİ](#page9)

[TABLOLAR LİSTESİ](#page10) [İX](#page10)

[EKLER LİSTESİ](#page11) [X](#page11)

[SİMGELER VE KISALTMALAR](#page12) [Xİ](#page12)

[**1. GİRİŞ**](#page13)[**1**](#page13)

****

[**2. YER DEĞİŞTİRME KUTULARI**](#page15)[**3**](#page15)

[2.1.](#page17) [Yer Değiştirme Kutu Tasarım Teknikleri](#page17) [5](#page17)

[2.2.](#page17) [Kaos Tabanlı Kriptoloji](#page17) [5](#page17)

[2.3.](#page18) [Kaotik Yer Değiştirme Kutuları](#page18) [6](#page18)

[**3. MATERYAL VE METOT**](#page20)[**8**](#page20)

[3.1.](#page20) [Performans İyileştirmesi için Önerilen Algoritma I](#page20) [8](#page20)

[3.2.](#page23) [Performans İyileştirmesi için Önerilen Algoritma II](#page23) [11](#page23)

[3.2.1. Kaos Tabanlı İdeal Entropi Kaynağının Üretilmesi](#page23) [11](#page23)

[3.2.2. Kaos Tabanlı İdeal Entropi Kaynağından Yer Değiştirme Kutularının Üretilmesi](#page26) [14](#page26)

[3.2.3. Zig Zag Dönüşüm Yöntemi ile Yer Değiştirme Kutularının Üretilmesi](#page27) [15](#page27)

[3.3.](#page28) [Performans İyileştirmesi için Önerilen Algoritma III](#page28) [16](#page28)

[**4. KAOS TABANLI YENİ BİR YDK TASARIM ALGORİTMASI**](#page32)[**20**](#page32)

[4.1.](#page32) [Nose–Hoover Kaotik Sistemi](#page32) [20](#page32)

[4.2.](#page33) [YDK Tasarım Yaklaşımı](#page33) [21](#page33)

[**5. BULGULAR VE TARTIŞMA**](#page36)[**24**](#page36)

[5.1.](#page37) [Algoritma I Performans Analizleri](#page37) [25](#page37)

[5.2.](#page38) [Algoritma II Performans Analizleri](#page38) [26](#page38)

[5.3.](#page41) [Algoritma III Performans Analizleri](#page41) [29](#page41)

[5.4.](#page44) [Nose–Hoover Kaotik Sistemini Temel Alan Yer Değiştirme Kutusu için Performans Analizleri . 32](#page44)

[**6. SONUÇLAR**](#page47)[**35**](#page47)

[ÖNERİLER](#page49) [37](#page49)

[KAYNAKLAR](#page50) [38](#page50)

[**EKLER**](#page56)[**44**](#page56)

[**ÖZGEÇMİŞ**](#page69)

v

**ÖZET**

Kaotik Yer Değiştirme Kutularının Performans İyileştirmesi için Yeni Algoritmaların Geliştirilmesi

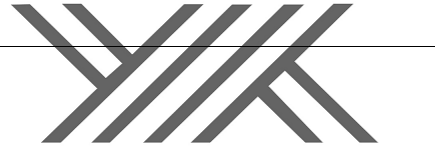
**Yaşar Selim BAHÇECİ**

Yüksek Lisans Tezi

FIRAT ÜNİVERSİTESİ

Fen Bilimleri Enstitüsü

Yazılım Mühendisliği Anabilim Dalı



Ağustos 2020, Sayfa: xi + 56

Kriptolojik protokol tasarımında yer değiştirme kutuları önemli bir yere sahiptir. Yer değiştirme kutularının oluşturulması için kullanılan yaygın yöntemlerden biri rastgele seçim tabanlı tasarımlardır. Rastgele seçim için literatürdeki en etkili yöntem olarak kaos tabanlı tasarımlar ön plana çıkmaktadır. Bu tez çalışmasında geliştirilen yeni yöntemler ile kaos tabanlı yer değiştirme kutu tasarımların performans metriklerinin iyileştirilebileceği gösterilmiştir.

Yer değiştirme kutularında performans analizi için kullanılabilecek çeşitli ölçütler olmasına rağmen en belirgin özelliklerden biri doğrusal olmama ölçütüdür. Bu tez çalışmasında geliştirilen yöntemler ile doğrusal olmama ölçütünün iyileştirilmesi hedeflenmiştir. Doğrusal olmama ölçütünün önemi kriptolojik protokoller için sağlanması zorunlu karıştırma gereksinimi ile ilişkilidir. Bir kriptolojik protokolde karıştırma gereksiniminin tam olarak karşılanabilmesi için doğrusal olmama ölçütü yüksek tasarımlara ihtiyaç duyulmaktadır. Kaos tabanlı yer değiştirme kutu tasarımlarının doğrusal olmama ölçütünün cebirsel tabanlı tasarımlara göre daha kötü olduğu bilinmektedir. Tez çalışması boyunca geliştirilen yöntemler ile bu problemin giderilmesi amaçlanmıştır.

Tez çalışması sonucunda dört farklı algoritma geliştirilerek kaos tabanlı yer değiştirme kutularının doğrusal olmama ölçütünün iyileştirilebileceği gösterilmiştir. Elde edilen bu sonuçlar blok şifreleme algoritmalarından anahtar üreteçlerine, görüntü şifreleme algoritmalarından özet fonksiyonlarına kadar geniş bir uygulama alanında kaos tabanlı yer değiştirme kutularının başarılı şekilde kullanılabileceğini göstermiştir.

**Anahtar Kelimeler:** Kaos, Kriptoloji, Blok şifreler, Yer değiştirme kutusu

vi

**ABSTRACT**

“Development of New Algorithms for Performance Improvement of Chaotic Substitution Boxes

**Yaşar Selim BAHÇECİ**

Master's Thesis

FIRAT UNIVERSITY

Graduate School of Natural and Applied Sciences



Department of Software Engineering

August 2020, Pages: xi + 56

Substitution boxes have an important place in cryptological protocol design. One of the common methods used to create substitution boxes is random selection based designs. Chaos-based designs come to the fore as the most effective method in the literature for random selection. It has been shown that performance metrics of chaos-based substitution box designs can be improved with new methods developed in this thesis study.

Although there are various criteria that can be used for performance analysis in substitution boxes, one of the most obvious features is the nonlinearity criterion. The methods developed in this thesis study aimed to improve the nonlinearity criterion. The importance of the nonlinearity criterion is related to the need for mixing required for cryptological protocols. In a cryptological protocol, in order to fully meet the need for mixing, designs with high nonlinearity are required. It is known that non-linear criteria of chaos-based substitution box designs are worse than algebraic-based designs. It is aimed to overcome this problem with the methods developed throughout the thesis study.

As a result of the thesis, four different algorithms have been developed and it has been shown that non-linearity of chaos-based substitution boxes can be improved. These results show that chaos-based substitution boxes can be used successfully in a wide range of applications from block cipher algorithms to key generators, image cipher algorithms to summary functions.

**Keywords:** Chaos, Cryptology, Block encryption, Substitution box

vii

**ŞEKİLLER LİSTESİ**

Sayfa

[**Şekil 3.1.** Çalışmada önerilen detayları Tablo 3.1’de verilen sekiz son işlem algoritmasının çıktıları](#page21)[**9**](#page21)

[**Şekil 3.2**. YDK oluşturmak için kullanılan algoritma](#page22)[**10**](#page22)

[**Şekil 3.3**. Lojistik haritanın çatallaşma diyagramı](#page24)[**12**](#page24)

[**Şekil 3.4**. Kaos tabanlı ideal entropi kaynağı elde etmek için kullanılan yöntemin akış şeması](#page25)[**13**](#page25)

[**Şekil 3.5.** YDK tasarım süreci](#page27)[**15**](#page27)

[**Şekil 3.6.** Zig-Zag dönüşüm işlemi](#page28)[**16**](#page28)

[**Şekil 3.7.** Önerilen yöntemin akış şeması](#page29)[**17**](#page29)

[**Şekil 3.8.** Fisher-Yates yönteminin akış şeması](#page29)[**17**](#page29)

[**Şekil 4.1.** Nose–Hoover sisteminin faz uzayı analizi](#page33)[**21**](#page33)

****

[**Şekil 4.2.** Önerilen yöntemin algoritması](#page34)[**22**](#page34)

viii

**TABLOLAR LİSTESİ**

Sayfa

[**Tablo 2.1.** Kaotik sistemlere ait matematiksel modeller](#page15)[**3**](#page15)

[**Tablo 2.2**. YDK yapılarının genel bir sınıflandırılması](#page19)[**7**](#page19)

[**Tablo 3.1**. Önerilen son işlem teknikleri](#page20)[**8**](#page20)

[**Tablo 3.2.** Ayrık zamanlı kaotik sistem YDK yapısı](#page22)[**10**](#page22)

[**Tablo 3.3**. Sürekli zamanlı kaotik sistem YDK yapısı](#page23)[**11**](#page23)

[**Tablo 3.4.** Doğrusal olmama ölçütü 105 ve üstü XOR dağılımı ise 10 olan YDK yapıları](#page27)[**15**](#page27)

[**Tablo 3.5.** Doğrusal olmama ölçütü 105 ve üstü XOR dağılımı ise 10 olan değişen YDK yapıları](#page28)[**16**](#page28)

[**Tablo 3.6.** Fisher-Yates yönteminin adım adım çalışması](#page30)[**18**](#page30)

[**Tablo 3.7.** Orijinal YDK yapısı](#page30)[**18**](#page30)

****

[**Tablo 3.8.** Değiştirilen YDK yapısı](#page31)[**19**](#page31)

[**Tablo 4.1.** Önerilen YDK yapısı](#page34)[**22**](#page34)

[**Tablo 4.2.** YDK yapısının performans analizleri](#page35)[**23**](#page35)

[**Tablo 5.1.** AES YDK yapısının kriptolojik özellikleri](#page36)[**24**](#page36)

[**Tablo 5.2.** Önerilen son işlem teknikleri ile gözlemlenen performans iyileştirmeleri](#page37)[**25**](#page37)

[**Tablo 5.3.** Orijinal entropi kaynağından üretilen YDK yapılarının performans karşılaştırmaları](#page38)[**26**](#page38)

[**Tablo 5.4.** Zig-zag son işlem tekniği uygulanmış YDK yapılarının performans karşılaştırmaları](#page40)[**28**](#page40)

[**Tablo 5.5.** Orijinal YDK yapısının performans karşılaştırmaları](#page42)[**30**](#page42)

[**Tablo 5.6.** Fisher-Yates yöntemi ile değiştirilen YDK yapısının performans karşılaştırmaları](#page43)[**31**](#page43)

[**Tablo 5.7.** Nose–Hoover kaotik sistemini temel alan YDK için performans analizleri](#page44)[**32**](#page44)

[**Tablo 5.8.** Nose–Hoover kaotik sistemini temel alan YDK için performans karşılaştırmaları](#page45)[**33**](#page45)

ix

**EKLER LİSTESİ**

Sayfa

[**Ek- 1:**](#page56)[**Zig-zag algoritmasının temsili gösterimi ve kodu**](#page56)[**44**](#page56)

[**Ek- 2:**](#page57)[**Orijinal YDK Tablosu**](#page57)[**45**](#page57)

[**Ek- 3:**](#page63)[**Değişen YDK Tablosu**](#page63)[**51**](#page63)

****

x

**SİMGELER VE KISALTMALAR**

**Kısaltmalar**

|  |  |
| --- | --- |
| AES | : Geliştirilmiş Şifreleme Standardı |
| BBK | : Bit Bağımsızlık Kriteri |
| DES | : Veri Şifreleme Standardı |
| IDEA | : Uluslararası Veri Şifreleme Algoritması |
| KÇK | : Katı Çığ Kriteri |
| LAT | : Doğrusal Yaklaşım Tablosu |
| RSÜ | : Rastgele Sayı Üreteci |
| SPN | : Koyma Değiştirme Ağları |
| YDK | : Yer Değiştirme Kutusu |



xi

1. **GİRİŞ**

Bir araştırmacı için en önemli yetenek problem çözme kabiliyetidir. Ancak gerçek dünya problemlerine çözüm bulmak her zaman tahmin edildiği kadar kolay olmamaktadır. Bu yüzden araştırmacılar gerçek dünya varlıklarını temsil edecek sistemler üzerine yoğunlaşmaktadır. Bu kapsamda kaotik sistemler giderek önem kazanmıştır. Son yirmi yılda bilim ve mühendislikteki birçok uygulamada kaotik sistemler yaygın şekilde kullanılmıştır. Özellikle modelleme, oyun teorisi, sezgisel yaklaşımlar ve bilgi güvenliği alanındaki birçok uygulamanın gereksinim duyduğu rastgelelik kaynağının üretilmesi kaotik sistemlerin en başarılı uygulama alanlarından biri olmuştur [1, 2].

Kaos doğrusal olmayan dinamik sistemlerde bulunan gerekirci (deterministlik) ve rastgele benzeri bir süreçtir. Kaotik sistemler periyodik değildir ve sınırlı olmalarına rağmen bir değere yakınsamazlar. Kaotik sistemlerin en önemli özelliği başlangıç koşulları ve kontrol parametrelerine oldukça bağımlı olmasıdır. Kaosun doğası görünürde rastgele ve tahmin edilemezdir. Ayrıca kendi içerisinde bir düzene sahiptir. Hatta çoğu kez düzen içinde düzensizlik ya da düzensizlik içinde düzen olarak da tanımlanmaktadır. Matematiksel olarak, basit gerekirci dinamik bir sistemin rastgeleliği olarak tanımlanabilir. Kaotik davranış az rastlanan bir olgu değildir. Matematikten biyolojiye, ekonomiden elektronik devrelere, mühendislikten sosyal bilimlere, insan vücudunun davranışından vahşi nüfusun dağılımına kadar çok geniş bir alanda bu davranışa rastlanmaktadır.



Kriptoloji en basit anlamda güvenli veri iletişimini sağlamayı amaçlayan bir bilim dalıdır. Bir kriptolojik protokolün güvenli olarak nitelendirilebilmesi için iki temel gereksinimin sağladığının garanti edilmesi beklenmektedir. Bu gereksinimler yayılma ve karıştırma özellikleridir. Yayılma özelliği saldırganın istatistiki analizler kullanarak algoritmanın gizli anahtarını elde etmesini önlemeyi amaçlamaktadır. Yayılma özelliğini sağlanmak için genellikle orijinal verinin pozisyonun kaydırıldığı, yer değiştirildiği veya bir fonksiyon yardımıyla haritalandığı yöntemler kullanılmaktadır. Orijinal verinin değişiminde kullanılan bu yöntemler doğrusal bir yapıya sahip olduğu için saldırgan tarafından kolaylıkla tahmin edilebilir. Bu yüzden yayılma gereksinimi ile birlikte güçlü bir karıştırma işleminin sağlanması gereklidir. Çünkü karıştırma özelliği algoritmanın gizli anahtarı ile şifreli veri arasındaki ilişkinin ifade edilmesini zorlaştırmaktadır [3, 4].

Karıştırma özelliğini sağlamak için en etkili yaklaşımlardan biri güçlü bir entropi kaynağının elde edilmesidir. Ancak kriptolojik uygulamalarda bu zor bir görevdir. Tasarımda meydana gelebilecek bir kusur tüm algoritmanın güvenliğini etkileyecektir. Özellikle kriptolojik uygulamalar için fiziksel kaynakları temel alan tasarımlara gereksinim duyulmaktadır. Literatürde bu fiziksel kaynakları temel alan popüler yaklaşımlardan biri de kaos tabanlı rastgelelik üreteçleridir [5-7].

Kaotik sistemler kriptolojik rastgeleliğin elde edilmesi için güçlü bir adaydır. Bu yüzden kaotik sistemlerin sahip olduğu dinamikleri kullanarak çeşitli kriptolojik protokollerin tasarlanması aktif bir araştırma alanıdır. Bu araştırma alanında iki disiplinin bir arada kullanıldığı en başarılı örneklerinden biri de kaos tabanlı yer değiştirme kutu (YDK) yapılarının tasarımı olmuştur [1, 8].

**Problemin Tanımı:** Kaos tabanlı YDK yapılarırastgeleseçim prensibini temel alan birtasarım yaklaşımı kullanılarak elde edilmektedir. Son zamanda yapılan çalışmalar bu yapıların özellikle yan kanal saldırıları gibi uygulamaya yönelik kripto analiz senaryolarını önlemek için daha başarılı olabileceğini göstermiştir. Ancak rastgele seçim tabanlı tasarımlar uygulama saldırılarına karşı daha dirençli olmasına rağmen YDK performans ölçütleri bakımından matematiksel temelli tasarımlara göre daha kötüdür. Tez çalışması bu problemi çözmek için kullanılabilecek son işlem algoritmalarını araştırmayı amaçlamaktadır.

**Problemin Önemi:** Kaos temelli YDK yapılarının performans iyileştirmeleri yapılabilirsebu yapıların pratik uygulamalarda kullanılabilirliği gösterilmiş olacaktır. Bu durumda hem yan kanal saldırısı gibi uygulamaya yönelik kripto analiz teknikleri için bir önlem geliştirilecek hem de matematiksel tasarımlara alternatif yeni tasarımların önü açılabilecektir.



**Amaç:** YDK tasarımlarının başarısını değerlendirmek için çeşitli metrikler bulunmaktadır.Yapılan analizler bu metrikler içerisinde doğrusal olmama (nonlinearity) ölçütünün performans karşılaştırması yapmak için daha elverişli olduğunu göstermektedir. Bu yüzden tez çalışmasının amacı geliştirilecek çeşitli son işlem algoritmaları yardımı ile kaos temelli YDK yapılarının doğrusal olmama ölçütünün iyileştirebileceğini araştırılmasıdır.

Bu doğrultuda tezin geri kalan kısmı aşağıdaki gibi organize edilmiştir. İkinci bölümde YDK yapıları ve kriptoloji bilimi açısından önemine değinilmiştir. Bu bölümde öncelikle YDK yapıları hakkında genel bilgiler verilmiştir. Ardından kaos temelli YDK yapıları hakkında genel bir literatür özeti sunulmuştur. Üçüncü bölümde tez kapsamında geliştirilen yöntemlerin detayları açıklanmıştır. Üçüncü bölüm, dört alt bölümden oluşmaktadır. İlk üç alt bölümde YDK performans iyileştirmesi için önerilen algoritmalar sunulmuştur. Son alt bölümde ise literatürde ilk defa kullanılan bir kaotik sistemi temel alan YDK yapısının tasarımına ilişkin detaylar verilmiştir. Dördüncü bölümde önerilen yöntemlerin başarısı gerçekleştirilen analiz sonuçları yorumlanarak tartışılmıştır. Son bölümde elde edilen sonuçlar özetlenmiş ileriye yönelik yapılabilecek çalışmalara ilişkin önerilerde bulunulmuştur.

2

1. **YER DEĞİŞTİRME KUTULARI**

Gerçek dünya olaylarının sebepleri ve sonuçları arasındaki ilişki çok karmaşık bir yapıya sahiptir. Kaotik sistemlerde tam olarak bu karmaşık ilişkiyi temel almaktadır. Bir çok doğrusal olmayan sistemin, zaman içindeki değişiminin düzensiz olması ve tahmin edilememesi kaos olarak adlandırılmıştır. Kaotik sistemlerde; sistemin başlangıç koşulları ve kontrol parametrelerinde meydana gelebilecek en küçük bir değişiklik çok farklı çıktıların elde edilmesine sebep olmaktadır. Çoğu zaman bu olgu kelebek etkisi olarak bilinmektedir. Bir kelebeğin kanat çırpması ile meydana gelebilecek çok küçük bir değişimin bir kasırgayı tetikleyebileceğini ortaya koymaktadır. Kaotik sistemlerde çıktıların kestiriminin imkansız olduğu ifade edilmektedir. Bir başka ifade ile bir kaotik sistem olasılıksal bir sisteme benzemektedir. Fakat düzensizliğin kaynağı kestirilemeyen dış etkiler değil de sistemin gerçek dinamikleridir.



Ayrık zamanlı, sürekli zamanlı, zaman gecikmeli, uzamsal ve hiper kaotik gibi çeşitli kaotik sistem sınıfları bulunmaktadır. Bu kaotik sistem sınıflarının sahip oldukları matematiksel modeller göz önüne alınarak basitten karmaşığa doğru sıralanmıştır. Bu çalışmada diğer kaotik sistem sınıflarına kıyasla daha basit bir yapıya sahip olduğu için ayrık zamanlı sistemler üzerinden ilerlenmiştir. Bu tercihin en önemli sebebi sözde rasgele sayı üretecinin karmaşıklığını mümkün olduğunca düşük tutarak etkililiği sağlamaktır. Çalışmada dört farklı ayrık zamanlı kaotik sistem kullanılmıştır. Bu kaotik sistemlere ait matematiksel modeller Tablo 2.1’ de verilmiştir.

**Tablo 2.1.** Kaotik sistemlere ait matematiksel modeller

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Kaotik Sistem** | **Matematiksel Model** | | | | | | |  |  |
|  |  |  |  | | | |  |  |  |  |
|  | Lojistik harita | *Xn+1* | *= A Xn (1 - Xn)* | | | | |  |  |  |
|  |  |  |  | | | |  | |  |  |
|  | Çadır harita | *Xn+1* | *= A min (Xn, 1 - Xn)* | | | | | |  |  |
|  |  |  |  | | | |  |  |  |  |
|  | Sine Harita | *Xn+1* | *= A sin ( Xn)* | | | | |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | Çember Harita | Ɵ |  | *=* Ɵ |  | *+ Ω -* |  | (2 Ɵ |  | ) |
|  |  |  |
|  |  | +1 | |  |  | 2 |  |  |
|  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

Kriptoloji, haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan, temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür. Blok şifreleme sistemleri modern kriptoloji uygulamalarında önemli bir rol oynamaktadır. Bir blok şifreleme sistemi bir şifreleme algoritmasından daha fazla öneme sahiptir. Özet fonksiyonlarının tasarımı, mesaj yetkilendirme kodları, anahtar tasarım protokolleri veya sözde rastgele üreteçler gibi birçok kriptolojik temelde kullanılmaktadır. Modern kriptolojide önemli bir yer turan blok şifreleme sistemlerinin güvenli bir şekilde tasarlanabilmesi için şifreleme mimarisinde kullanılan

yer değiştirme kutularının önemi büyüktür. YDK DES, IDEA, AES gibi geleneksel blok şifreleme sistemlerindeki karıştırma özelliğini sağlayan doğrusal olmayan tek bileşendir [1].

Blok şifreleme sistemlerindeki doğrusal olmayan tek birleşenin YDK yapılarının olmasından dolayı blok şifreleme sistemlerine yapılan saldırılar genellikle YDK yapılarını hedef almaktadır. Bu yüzden iyi bir YDK tasarlamak için başarılı kriterler nedir sorusu sorulmalıdır. Kriptolojik olarak iyi YDK tasarımları yapabilmek için çeşitli ölçümler geliştirilmiştir. Bu ölçümler zamanla geliştirilen saldırılar (doğrusal, diferansiyel ve Davies saldırıları gibi) ile birlikte değişmiştir. YDK tasarımlarının kriptolojik uygulamalar için sağlaması gereken bazı özellikler aşağıda kısaca açıklanmıştır. Bu özelikler:

* **Giriş-çıkış bağımsızlığı:** Giriş değerlerinin bilinmesi, çıkış değerlerinin bilinmezliğinideğiştirmez [9, 10].
* **Çıkış-giriş bağımsızlığı:** Bazı çıkış değerlerinin bilinmesi, giriş değerlerininbilinmezliğini değiştirmez [9, 10].
* **Çıkış çıkış bağımsızlığı:** Çıkış bitleri ile ilgili kısmi bir bilgi, diğer bilinmeyen çıkışbitlerinin bilinmezliğini değiştirmez [9, 10].
* **Doğrusal olmama:** YDKyapılarının en önemli özelliğidir.YDK’ ın doğrusal eşitliklerhalinde ifade edilmesini engelleyen özelliktir. Bu doğrusal eşitlikler, YDK’ ın bulunduğu kriptolojik sistemleri kırmada kullanılır. Bu nedenle doğrusal olmama özelliği yüksek olan YDK tasarımları kullanılmalıdır [10, 11].
* **Bilgi bütünlüğü:** Kam ve Davida bilgi bütünlüğünü, “Her olası giriş değeri için her çıkışbiti, giriş bitlerinin sadece uygun bir bölümüne değil, tüm olası giriş değerlerine bağımlıdır.” olarak tanımlamıştır [12, 13].
* **Çığ kriteri:** Fesitel tarafındanYDKyapıları ve SPN (Substitution Permutation Network)tabanlı blok şifreler için tasarlanmış bir ölçümdür. Bir f boolean fonksiyonu için giriş bitinin bir biti değiştiğinde, çıkış bitlerinin yarısının değişip değişmediğini ölçmeye çalışmaktadır [12-14].
* **Katı çığ kriteri:** Webster ve Taveres tarafından bütünlük ve çığ kriterleri birleştirilerekgeliştirilmiş bir özelliktir. Bir boolean fonksiyonu için olmak üzere eğer giriş biti i’yi değiştirmek için çıkış biti j’nin kesinlikle ½ olasılığında değişmesine neden oluyorsa katı çığ kriterini (Katı Çığ Kriteri) sağlar [12-14].
* **Tersi alınabilir:** Bu kriter YDKyapılarının arzulanan bir özelliğidir. BirYDKyapısınıngiriş ve çıkış değerleri arasında birebir haritalama mevcutsa tersi alınabilir. Eğer bir YDK yapısının tersi alınamıyorsa giriş değerlerinden daha az sayıda çıkış değerleri vardır. Böyle bir durumda çıkış değerlerinde giriş değerlerine göre daha az bilinmezlik olur [9].



4

* Bu özelliklerle bağlantılı olmakla birlikte ek olarak geliştirilen YDK yapısının doğrusal ve diferansiyel kripto analize karşı ne kadar dirençli olduğunu göstermek için doğrusal yaklaşım tablosu (Lineer Approximation Table - LAT) ve fark dağılım tablosu (XOR tablosu) da kullanılmaktadır [14-15].

**2.1.** **Yer Değiştirme Kutu Tasarım Teknikleri**

YDK yapılarının tasarımı için literatürde birçok yöntem önerilmiştir. Bu yöntemler üç ana kategoride toplanmaktadır: cebirsel tabanlı yöntemler, sözde rastgele tabanlı yöntemler ve sezgisel yöntemler [16-20]. Modern blok şifreleme algoritmalarında genellikle güçlü cebirsel ilişkilere dayanan YDK tasarım teknikleri kullanılmaktadır. Bunlardan en yaygın şekilde bilinenleri Nyberg tarafından önerilmiş olan sonlu cisimde ters alma yöntemidir. Bu yöntem gelişkin şifreleme algoritması olarak bilinen AES [21] (Advanced Encryption Standard) blok şifreleme algoritmasının YDK tasarımında da kullanılmıştır. Ancak, hem yan kanal analizleri gibi uygulamaya yönelik saldırılar hem de cebirsel saldırılarının ortaya koyulması ile mevcut YDK tasarım tekniklerine alternatif olabilecek yeni yöntemler araştırılmaya başlanmıştır. Kaotik sistemlerin temel alındığı yeni tasarım teknikleri de bu amaca yönelik çalışmalar arasındadır [22-25, 26, 27].



Kaos tabanlı YDK tasarım çalışmaları ilk olarak 2000’li yılların başlangıçlarında görülmeye başlanmıştır. Bu tasarımlarda daha basit matematiksel modellere sahip olan ayrık zamanlı kaotik haritalar kullanılarak YDK yapıları üretilmiştir. Bu grup tasarımlarda genel yaklaşım farklı kaotik haritalar kullanarak YDK performans kriterlerinin iyileştirilmesi hedeflenmiştir. İkinci grup çalışmalar 2010 yılında ortaya çıkmıştır. Bu grup çalışmaların tasarım mantığındaki ortak nokta kaotik sistem karmaşıklığını artırılarak YDK performans ölçütlerini iyileştirmektir. Dolayısıyla bu grup tasarımlarda daha karmaşık matematiksel modele sahip sürekli zamanlı kaotik sistemler kullanılmıştır. Üçüncü grup kaos tabanlı YDK tasarımlarında ise kaotik sistemin karmaşıklığını daha fazla artırabilmek için hiper kaotik veya zaman gecikmeli kaotik sistemler kullanılmıştır. Ancak son yapılan bir çalışmada kaos tabanlı YDK yapılarının performansının kaotik sistemden bağımsız olduğunu göstermiştir. Yine aynı çalışmada kaos tabanlı YDK tasarımları için doğrusal olmama performans ölçütünde ulaşılabilecek en yüksek değerin 106,75 olduğunu göstermiştir.

**2.2.** **Kaos Tabanlı Kriptoloji**

Kaos ve kriptoloji bilimleri arasındaki yakın ilişkinin ortaya koyulması kaotik sistemlerin kullanılarak kriptolojik sistemlerin güvenliğinin artırılıp artırılamayacağı düşüncesini ortaya koyulmuştur. İki disiplin arasındaki bu ilişki Shannon’un herhangi bir şifreleme sisteminin güvenilir olması için sahip olması gereken özellikler olan karıştırma (confusion) ve yayılma

5

(diffusion) özellikleri ile kaotik sistemlerin başlangıç koşullarına duyarlı olması ve doğrusal olmaması özellikleriyle örtüşmesinden ortaya çıkmaktadır.

Kaos ve kriptoloji bilimleri arasındaki güçlü ilişkinin ortaya çıkması ile birlikte 2000’li yıllardan başlamak üzere birçok kaos tabanlı YDK tasarım önerisi sunulmuştur. 2000 ile 2009 yılları arasındaki çalışmalar incelenirse bu çalışmaların ortak noktalarının çeşitli kaotik haritaları (ayrık zamanlı kaotik sistemleri) temel alarak tasarımların gerçekleştirildiği görülür. Kaotik haritaların kullanılmasındaki en önemli sebeplerden biri sürekli zamanlı kaotik sistemlerin kullanılması durumunda meydana gelebilecek sayısal kötüleşmenin bozucu etkilerinden kaçınmak olduğu belirtilmiştir. 2010 yılında yapılan çalışmada güçlü bir tasarım algoritması ile sürekli zamanlı kaotik sistemlerinde tasarımda kullanılabileceğinin gösterilmesinin ardından daha kompleks kaotik sistemler kullanılarak YDK yapılarının performansının artırılıp artırılamayacağı araştırılmıştır. Bu çalışmada ilk defa kesir dereceli kaotik sistemler kullanılarak bir YDK tasarım algoritması önerilmiştir. Önerilen algoritma ile literatürdeki diğer kaos tabanlı algoritmalardan daha iyi bir YDK tasarlanmıştır.



**2.3.** **Kaotik Yer Değiştirme Kutuları**

Bir blok şifreleme protokolünde vazgeçilmez birleşenlerden biri yer değiştirme kutularıdır. Yer değiştirme kutu tasarımı için çeşitli yöntemler bulunmaktadır. Bu tasarım teknikleri arasında en yaygın bilinen yöntem cebirsel dönüşümleri temel almaktadır. Özellikle AES şifreleme algoritmasında kullanılan Nyberg tarafından geliştirilmiş YDK tasarımı literatürde yaygın biçimde bilinmektedir. AES YDK yapısı galois cismi (GF(28)) üzerinde indirgenemez polinomlara *(x8+x4+x+1)* göre ters alınarak oluşturulmuştur. AESYDKyapısı ulaşılabilecek en iyi kriptolojiközelliklere sahiptir. Ancak sahip olduğu cebirsel ilişkiler çeşitli zafiyetlere sebep olabilmektedir. Son yıllarda geliştirilen uygulama saldırıları bu zafiyetleri kullanarak şifreleme algoritması hakkında çeşitli bilgilerin elde edilebileceğini göstermiştir. Araştırmacılar bu problemleri gidermek için yeni tasarım teknikleri üzerine odaklanmıştır. Yeni önerilen bu tasarım tekniklerinden biri de rastgele seçim tabanlı yaklaşımlardır. Kaos ve rastgelelik arasındaki ilişki kullanılarak literatürde bir çok kaos tabanlı YDK tasarımı önerilmiştir.

Literatürde ilk önerilen kaotik YDK tasarımları ayrık zamanlı kaotik sistemleri temel almaktadır. Bu tasarımlarda ayrık zamanlı kaotik sistemleri kullanmanın sebebi sistemin basit matematiksel modeli olarak açıklanmıştır. Bu tasarımların cebirsel tasarımlara alternatif olabileceğinin iddia edilmesinin ardından kaotik sistemin rastgeleliği iyileştirilerek kriptolojik özelliklerin de iyileştirilebileceği fikri öne sürülmüştür. Bu iddiayı doğrulamak için sürekli zamanlı, zaman gecikmeli ve hiper kaotik sistemleri rastgelelik kaynağı olarak kullanan yeni tasarımlar önerilmiştir. Literatürde rastgelelik kaynağının kalitesini iyileştirmek için çok farklı

6

önerilerde sunulmuştur. Literatürdeki kaos tabanlı YDK yapılarının genel bir sınıflandırılması için Tablo 2.2 verilmiştir.

**Tablo 2.2**. YDK yapılarınıngenel bir sınıflandırılması

|  |  |  |
| --- | --- | --- |
|  | **Kullanılan kaotik sistem türü** | **Çalışmalar** |
|  |  |  |
|  | Ayrık zamanlı kaotik sistemleri temel alan tasarımlar | [11, 12, 16-19, 23, 24, 30, 34, 36- |
|  |  | 39, 42, 49, 50, 53, 60, 61, 63, 73, |
|  |  | 79, 80, 82 ] |
|  |  |  |
|  | Sürekli zamanlı kaotik sistemleri temel alan tasarımlar | [31, 33, 41-46, 48, 55, 56, 63-66, |
|  |  | 69, 71, 74] |
|  |  |  |
|  | Hiper kaotik sistemleri temel alan tasarımlar | [67, 76] |
|  |  |  |
|  | Zaman Gecikmeli kaotik sistemleri temel alan tasarımlar | [18, 47] |
|  |  |  |
|  | Kesir dereceli kaotik sistemleri temel alan tasarımlar | [6, 32, 58, 62, 64, 70] |
|  |  |  |
|  | Diğer | [28, 29, 40, 57, 59, 64, 68, 75, 78, |
|  |  | 79, 81-85] |
|  |  |  |



Kaotik sistemin rastgeleliği ve YDK yapılarının kritptolojik özellikleri arasındaki doğrusal ilişkiyi ortaya koymak için Tanyıldızı ve Özkaynak [8] optimizasyon algoritmalarını kullanarak en uygun entropi kaynağını elde etmeyi amaçlamışlardır. Çalışmalarında kaotik sistemin rastgeleliğini ölçmek için ki-kare testini temel almışlardır. Ki-kare testine göre en iyi rastgelelik özelliklerine sahip kaotik entropi kaynağının nasıl üretileceğini göstermişlerdir. Bu güne kadar rastgele seçim tabanlı bir YDK yapısı için ulaşılabilecek maksimum doğrusalsızlık değerinin 106,75 olabileceği iddia edilmiştir. Bu değer teorik ve deneysel olarak daha önce yayınlanan çalışmalarda ortaya koyulmuştur. Yine Tanyıldızı ve Özkaynak ki-kare testi için ideal özelliklere sahip entropi kaynağını kullanarak maksimum doğrusalsızlık değerine sahip YDK yapılarının elde edilebileceği gösterilmiştir.

7

1. **MATERYAL VE METOT**

Bu bölüm dört alt bölümden oluşmaktadır. Her bir alt bölümde kaos temelli YDK yapılarının nasıl tasarlanabileceği ve performans metriklerinin (özellikle doğrusal olmama metriğinin) nasıl iyileştirilebileceği detaylı biçimde açıklanmıştır.

**3.1.** **Performans İyileştirmesi için Önerilen Algoritma I**

Bu bölümde önerilen son işlem algoritmasının YDK performans ölçütleri üzerindeki etkisini en iyi şekilde analiz edebilmek için AES YDK yapısına benzer olarak 16x16 boyutunda YDK yapıları temel alınmıştır. AES algoritmasının temel alınmasının sebebi 2000 yılından beri blok şifreleme algoritması standardı olarak birçok alanda yaygın şekilde kullanılmasıdır. Önerilen son işlem algoritmasının temel prensibi kaotik sistem çıkışlarını YDK değerlerine dönüştürülmesinin ardından elde edilen tablonun satır ve sütun pozisyonlarının karıştırılması prensibine dayanmaktadır [86].



Karıştırma işlemi için sekiz farklı yaklaşımın performans üzerindeki etkisi analiz edilmiştir. Karıştırma işleminde kullanılan sekiz farklı yaklaşımın detaylarına Tablo 3.1’de yer verilmiştir. Tablo 3.1’de listelenen bu son işlemlerin çalışma mantığını etkili bir şekilde ifade edebilmek için 4x4 boyutunda küçük bir YDK yapısı için sonuçlar grafiksel olarak Şekil 3.1’de gösterilmiştir.

|  |  |
| --- | --- |
|  | **Tablo 3.1**.Önerilen son işlem teknikleri |
|  |  |
| **İşlem No** | **Açıklama** |
|  |  |
| **1** | i numaralı satır (i-1) defa dairesel olarak sola kaydırılır. |
|  |  |
| **2** | i numaralı satır (i-1) defa dairesel olarak sağa kaydırılır. |
|  |  |
| **3** | i numaralı sütun (i-1) defa dairesel olarak yukarı kaydırılır. |
|  |  |
| **4** | i numaralı sütun (i-1) defa dairesel olarak aşağı kaydırılır. |

1. i numaralı satır (i-1) defa dairesel olarak sola kaydırılır. Ardından i numaralı sütun (i-1) defa dairesel olarak yukarı kaydırılır.
2. i numaralı satır (i-1) defa dairesel olarak sağa kaydırılır. Ardından i numaralı sütun (i-1) defa dairesel olarak yukarı kaydırılır.
3. i numaralı sütun (i-1) defa dairesel olarak aşağı kaydırılır. Ardından i numaralı satır (i-1) defa dairesel olarak sola kaydırılır.
4. i numaralı sütun (i-1) defa dairesel olarak aşağı kaydırılır. Ardından i numaralı satır (i-1) defa dairesel olarak sağa kaydırılır.

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
|  |  |  |  |
| 5 | 6 | 7 | 8 |
|  |  |  |  |
| 9 | 10 | 11 | 12 |
|  |  |  |  |
| 13 | 14 | 15 | 16 |
|  |  |  |  |

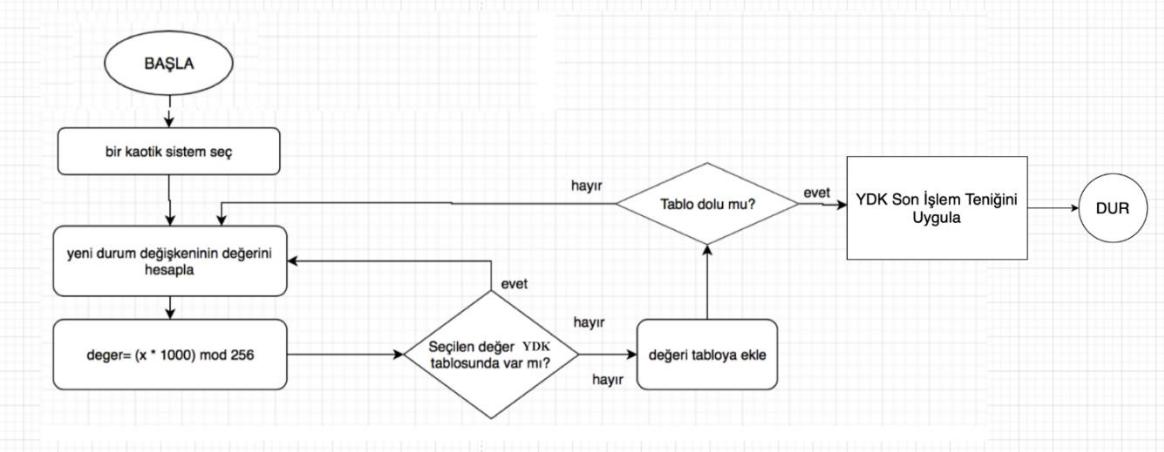
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  | (a) | Orijinal YDK | | | | |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 1 | 2 | 3 | 4 |  | 1 | 2 | 3 | 4 |  |  | 1 | | 6 | 11 | 16 |  |  | 1 |  | 14 | 11 |  | 8 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | 7 | 8 | 5 |  | 8 | 5 | 6 | 7 |  |  | 5 | | 10 | 15 | 4 |  |  | 5 |  | 2 | 15 |  | 12 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 11 | 12 | 9 | 10 |  | 11 | 12 | 9 | 10 |  |  | 9 | | 14 | 3 | 8 |  |  | 9 |  | 6 | 3 |  | 16 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| 16 | 13 | 14 | 15 |  | 14 | 15 | 16 | 13 |  |  | 13 | | 2 | 7 | 12 |  |  | 13 |  | 10 | 7 |  | 4 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  | |
|  | (b) | İşlem 1 | |  |  | (c) | İşlem 2 | |  |  |  |  | (d) | İşlem 3 | | |  |  |  | (e) | İşlem 4 | | |
|  |  |  |  |  | |  |  |  |  | | |  |  |  |  |  |  | |  | |  |  |  |
| 1 | 7 | 9 | 15 |  | 1 | 5 | 9 | 13 |  |  | | 1 | 14 | 11 | 8 |  |  | 1 |  | 14 | 11 |  | 8 |
|  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | 12 | 14 | 4 |  | 8 | 12 | 16 | 4 |  |  | | 2 | 15 | 12 | 5 |  |  | 12 |  | 5 | 2 |  | 15 |
|  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |
| 11 | 13 | 3 | 5 |  | 11 | 15 | 3 | 7 |  |  | | 3 | 16 | 9 | 6 |  |  | 3 |  | 16 | 9 |  | 6 |
|  |  |  |  |  |  |  |  |  |  |  | |  |  |  |  |  |  |  |  |  |  |  |  |
| 16 | 2 | 8 | 10 |  | 14 | 2 | 6 | 10 |  |  | | 4 | 13 | 10 | 7 |  |  | 10 |  | 7 | 4 |  | 13 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | (f) | İşlem 5 | |  |  | (g) | İşlem 6 | |  |  |  |  | (h) | İşlem 7 | | |  |  | (ı) İşlem 8 | | | |  |



**Şekil 3.1.** Çalışmada önerilen detayları Tablo 3.1’de verilen sekiz son işlem algoritmasının çıktıları

YDK yapısı oluşturulurken son işlem tekniğinin başarısını ön plana çıkarmak için mümkün olduğunca basit bir yaklaşım kullanılmaya çalışılmıştır bu yüzden çok güçlü bir tek yönlü fonksiyon olan mod fonksiyonu kullanılarak kaotik sistem çıkışları 0 ile 255 arasındaki değerlere dönüştürülmüştür. Kaotik sistemleri temel alarak YDK oluşturan algoritmanın akış şeması Şekil 3.2’de verilmiştir. Bu algoritma ve YDK değerlendirme kriteri olarak kullanılabilecek ölçümler hakkında daha detaylı bilgiler için Kaynak [26, 27, 72] incelenebilir. Kaynak [35]’deki algoritma kullanılarak elde edilen biri ayrık zamanlı diğeri sürekli zamanlı kaotik sistem için üretilen iki farklı YDK yapısı sırasıyla Tablo 3.2 ve Tablo 3.3’de verilmiştir.

9



**Şekil 3.2**.YDK oluşturmak için kullanılan algoritma



**Tablo 3.2.** Ayrık zamanlıkaotik sistemYDK yapısı

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **0** | 100 | 169 | 155 | 98 | 235 | 49 | 152 | 73 | 19 | 81 | 36 | 43 | 9 | 216 | 62 | 195 |
|  | **1** | 18 | 247 | 147 | 105 | 29 | 137 | 75 | 232 | 57 | 237 | 173 | 16 | 224 | 163 | 82 | 165 |
|  | **2** | 35 | 162 | 97 | 21 | 225 | 193 | 63 | 4 | 74 | 54 | 68 | 61 | 218 | 177 | 146 | 71 |
|  | **3** | 77 | 66 | 238 | 83 | 122 | 240 | 151 | 139 | 133 | 25 | 205 | 161 | 220 | 183 | 254 | 39 |
|  | **4** | 33 | 154 | 243 | 17 | 55 | 191 | 182 | 106 | 255 | 78 | 96 | 58 | 233 | 171 | 221 | 253 |
|  | **5** | 40 | 129 | 46 | 28 | 87 | 67 | 119 | 53 | 174 | 244 | 234 | 101 | 142 | 89 | 126 | 229 |
|  | **6** | 190 | 24 | 236 | 166 | 104 | 145 | 23 | 136 | 56 | 198 | 90 | 197 | 181 | 201 | 217 | 204 |
|  | **7** | 65 | 143 | 22 | 84 | 91 | 131 | 251 | 214 | 112 | 207 | 231 | 48 | 252 | 248 | 228 | 102 |
|  | **8** | 37 | 189 | 69 | 60 | 168 | 20 | 245 | 116 | 10 | 76 | 227 | 156 | 188 | 44 | 196 | 113 |
|  | **9** | 95 | 246 | 42 | 215 | 167 | 223 | 175 | 128 | 7 | 14 | 230 | 239 | 209 | 250 | 5 | 88 |
|  | **A** | 202 | 51 | 164 | 120 | 158 | 206 | 213 | 38 | 0 | 72 | 138 | 186 | 176 | 125 | 3 | 2 |
|  | **B** | 222 | 184 | 70 | 212 | 47 | 121 | 144 | 134 | 117 | 132 | 123 | 85 | 50 | 199 | 13 | 208 |
|  | **C** | 118 | 80 | 111 | 109 | 200 | 45 | 178 | 6 | 30 | 93 | 160 | 64 | 241 | 79 | 11 | 194 |
|  | **D** | 12 | 210 | 130 | 110 | 108 | 185 | 107 | 124 | 226 | 41 | 242 | 1 | 192 | 114 | 149 | 148 |
|  | **E** | 187 | 115 | 99 | 94 | 31 | 203 | 157 | 179 | 86 | 52 | 141 | 26 | 59 | 15 | 180 | 140 |
|  | **F** | 127 | 159 | 34 | 135 | 249 | 8 | 92 | 211 | 27 | 153 | 170 | 172 | 103 | 150 | 32 | 219 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

10

**Tablo 3.3**.Sürekli zamanlı kaotik sistem YDK yapısı

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
|  | **0** | 100 | 169 | 235 | 49 | 9 | 19 | 73 | 152 | 43 | 98 | 195 | 105 | 147 | 16 | 224 | 162 |
|  | **1** | 57 | 81 | 163 | 137 | 36 | 21 | 61 | 165 | 232 | 62 | 216 | 75 | 237 | 54 | 18 | 254 |
|  | **2** | 133 | 97 | 83 | 151 | 238 | 218 | 183 | 240 | 29 | 74 | 173 | 33 | 55 | 17 | 205 | 66 |
|  | **3** | 4 | 154 | 25 | 129 | 58 | 39 | 146 | 67 | 78 | 161 | 220 | 106 | 40 | 229 | 35 | 221 |
|  | **4** | 191 | 177 | 190 | 24 | 139 | 53 | 82 | 126 | 253 | 71 | 166 | 119 | 225 | 46 | 96 | 247 |
|  | **5** | 56 | 198 | 90 | 182 | 68 | 171 | 84 | 89 | 63 | 102 | 231 | 155 | 197 | 255 | 201 | 217 |
|  | **6** | 145 | 251 | 244 | 77 | 142 | 22 | 207 | 65 | 243 | 174 | 167 | 91 | 23 | 181 | 101 | 193 |
|  | **7** | 14 | 87 | 230 | 37 | 112 | 227 | 252 | 245 | 143 | 28 | 164 | 76 | 209 | 136 | 131 | 48 |
|  | **8** | 223 | 189 | 236 | 158 | 2 | 168 | 250 | 10 | 206 | 234 | 125 | 38 | 188 | 3 | 122 | 69 |
|  | **9** | 116 | 138 | 50 | 228 | 199 | 88 | 5 | 20 | 214 | 13 | 70 | 104 | 117 | 175 | 44 | 72 |
|  | **A** | 212 | 60 | 184 | 42 | 64 | 156 | 186 | 132 | 51 | 222 | 204 | 202 | 0 | 239 | 111 | 176 |
|  | **B** | 45 | 93 | 130 | 144 | 246 | 215 | 30 | 123 | 113 | 80 | 11 | 248 | 47 | 95 | 241 | 12 |
|  | **C** | 210 | 233 | 118 | 178 | 121 | 6 | 124 | 213 | 226 | 134 | 149 | 208 | 85 | 109 | 1 | 203 |
|  | **D** | 7 | 192 | 187 | 41 | 128 | 194 | 26 | 200 | 196 | 110 | 108 | 159 | 94 | 160 | 179 | 86 |
|  | **E** | 107 | 242 | 31 | 120 | 114 | 140 | 115 | 34 | 15 | 59 | 185 | 135 | 52 | 8 | 180 | 148 |
|  | **F** | 27 | 249 | 153 | 92 | 141 | 127 | 211 | 170 | 79 | 157 | 150 | 103 | 172 | 99 | 32 | 219 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |



**3.2.** **Performans İyileştirmesi için Önerilen Algoritma II**

Bu bölümde önerilen yöntemin en önemli özelliği ideal entropi kaynağı kullanılarak üretilen YDK yapılarının önerilen son işlem tekniği ile yeniden konumlandırılmasıdır. Kaynak [8]’de optimizasyon algoritmaları aracılığı ile kaotik sistemler için ideal entropi kaynağını üretecek başlangıç koşulları ve kontrol parametrelerinin nasıl seçilebileceği gösterilmiştir. Bu bölümde öncelikle en uygun başlangıç koşulları ve kontrol parametre değerlerinin nasıl belirlenebileceği açıklanmıştır. Ardından bu ideal entropi kaynağını yer değiştirme kutularına dönüştürmek için önerilen yöntemin ayrıntıları verilmiştir. Son olarak son işlem algoritması olarak kullanılan zig-zag yönteminin detaylarına yer verilmiştir.

**3.2.1.** **Kaos Tabanlı İdeal Entropi Kaynağının Üretilmesi**

Kaos ve rastgelelik arasındaki heyecan verici ilişki literatürde çok yaygın şekilde kullanılmıştır. Ancak kaos tabanlı rastgelelik üreteçleri için literatürde önemli bir eksiklik bulunmaktadır: Doğrusal olmayan bir sistemin kaotik davranış gösterebilmesi için başlangıç koşulları ve kontrol parametrelerinin uygun şekilde seçilmesi gerekmektedir. Genellikle doğrusal olmayan sistemlerin kaotik davranış gösterdiği başlangıç koşulları ve kontrol parametrelerinin alabileceği değer aralıkları iki rasyonel sayı aralığındadır. Literatürde önerilen kaos tabanlı

11

rastgelelik üreteçlerinde başlangıç koşulları ve kontrol parametrelerinin bu aralıkta herhangi bir değer seçilerek tasarımların gerçekleştirildiği bilgisi paylaşılmıştır. Ancak bu seçimlerin rastgelelik üzerindeki etkisi incelenmemiştir. Örneğin matematiksel modeli Denklem 3.1’de verilen en yaygın kaotik sistemlerden biri olan lojistik harita isimli doğrusal olmayan sistemin çatallaşma (bifurcation) diyagramı Şekil 3.3’de verilmiştir. Denklem 3.1’de x0 değeri sistemin başlangıç koşulu a parametresi ise doğrusal olmayan sistemin kontrol parametresidir. Şekil 3.3’den görülebileceği gibi a parametresinin 1 ile 3 arasındaki değerlerinde sistem kaotik değildir ve tek bir denge noktası vardır, sistem bu noktaya yaklaşarak orada sabit kalır. a parametresinin 3 ile 3,5 arasındaki değerleri için iki denge noktası vardır ve herhangi birine yaklaşarak orada sabit kalır. Fakat 3,5 değerinden sonra sistem kaosa girmiştir ve davranışı kestirilemez. Bu kestirilemez davranış rastgelelik için önemli olduğundan literatürdeki birçok kaos tabanlı rastgelelik üreteç tasarımında xn değerinin [0 - 1] aralığında a değerinin ise [3,5 - 4] arasında seçilmesi istenmiştir. Ancak her iki parametrenin tanımlı olduğu aralıkta sonsuz adet seçim yapılabilir. Yapılabilecek bu seçimlerin etkisinin incelenmemiş olması önemli bir eksikliktir. Bu çalışmanın amacı bu problemleri optimizasyon algoritmaları yardımıyla adresleyebilmektir.

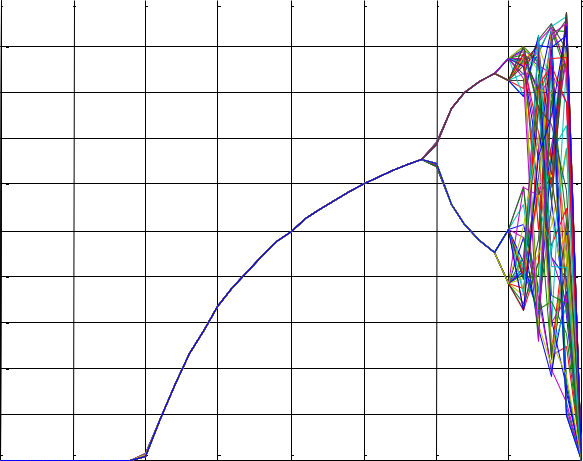


|  |  |
| --- | --- |
| +1 = ∗ ∗(1− ) | (3.1) |

|  |
| --- |
| xn |

lojistik haritanin çatallasma diyagrami

1 



0.9



0.8



0.7



0.6



0.5



0.4



0.3



0.2



0.1



|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 0 |  |  |  |  |  |  |  |  |
| 0 | 0.5 | 1 | 1.5 | 2 | 2.5 | 3 | 3.5 | 4 |
|  |  |  |  | a |  |  |  |  |



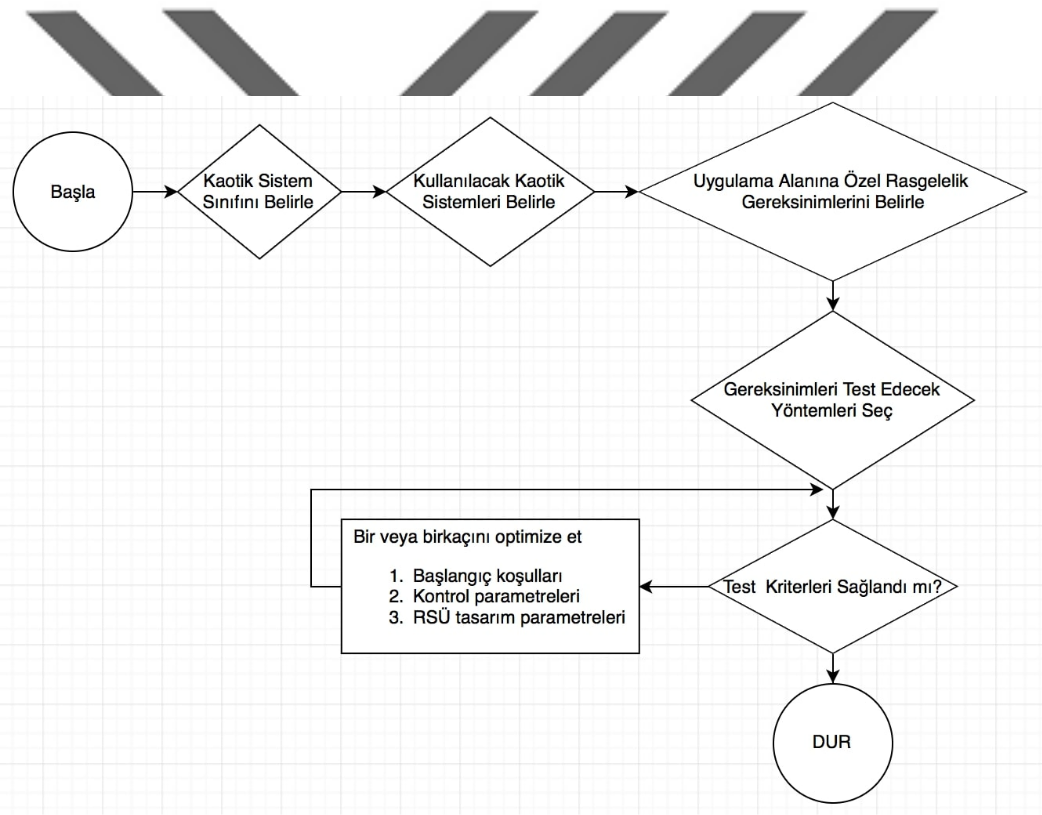
**Şekil 3.3**.Lojistik haritanın çatallaşma diyagramı

Optimizasyon, bir problem için, verilen şartlar altında tüm çözümler arasından en iyi çözümü̈ elde etme işidir. Optimizasyonun performansını etkileyen ve kontrolümüz altında değerleri olan değişkenlere karar değişkenleri denir. Karar değişkenlerinin amaç üzerindeki etkilerinin

12

analitik olarak gösterilmesiyle amaç fonksiyonu oluşturulur. Çoğu durumda, karar değişkenlerinin sadece belirli değerleri kullanılmalıdır. Karar değişkenlerinin değerleri üzerindeki bu sınırlandırmalara sınırlayıcılar denir. O halde farklı bir ifadeyle optimizasyon, karar değişkenlerinin mümkün olan tüm kombinasyonları arasından verilen tüm sınırlayıcıları sağlayan ve amaç fonksiyonunu en iyi hale getiren (maksimizasyon ya da minimizasyon) kombinasyonun bulunması işidir.

Kaynak [8]’de rastgelelik gereksinimlerini amaç fonksiyonu olarak kullanıp; karar değişkenlerindeki sınırlayıcılar için ise rastgelelik testlerinden faydalanarak farklı rastgelelik gereksinimlerine sahip uygulamalara özgü belirlenen gereksinimleri en iyi şekilde sağlayan kaotik sistem veya sistemlerin başlangıç koşulları ve kontrol parametrelerini belirleyerek rastgelelik üretecinin tasarımı gerçekleştirilmiştir. Önerilen yöntemin akış şeması Şekil 3.4’de verilmiştir. Belirlenen akış şemasının bir uygulaması aşağıda adım adım açıklanmıştır.



**Şekil 3.4**. Kaos tabanlıideal entropikaynağı elde etmek için kullanılan yöntemin akış şeması

13

Adım 1. Kullanılacak Kaotik Sistem Sınıfının Belirlenmesi: Bu çalışmada en basit matematiksel modele sahip kaotik sistem sınıfı olan ayrık zamanlı kaotik sistem sınıfı seçilmiştir.

Adım 2. Kullanılacak Kaotik Sistemlerin Belirlenmesi: Literatürde birçok ayrık zamanlı kaotik sistem bulunmaktadır. Çalışmada dört farklı ayrık zamanlı kaotik sistem kullanılmıştır. Bu sistemler lojistik, çadır (tent), sine ve çember (circle) haritalardır.

Adım 3. Uygulama Alanına Özel Rastgelelik Gereksinimlerini Belirle: Sözde rastgele sayı üreteçleri için istatistiksel rastgelelik yeterli olmaktadır. Bu durumda iyi istatistiksel özellikler göstermesi gereksiniminin sağlanması yeterli olacaktır.

Adım 4. Gereksinimlerin Sağlandığını Test Edecek Kriterleri Seç: İyi istatistiksel özelliklerin sağladığının kontrol edilmesi yeterli olacaktır. Bu aşamada mümkün olduğu kadar basit olması için ki-kare testi rasgelelik testi olarak kullanılmıştır.



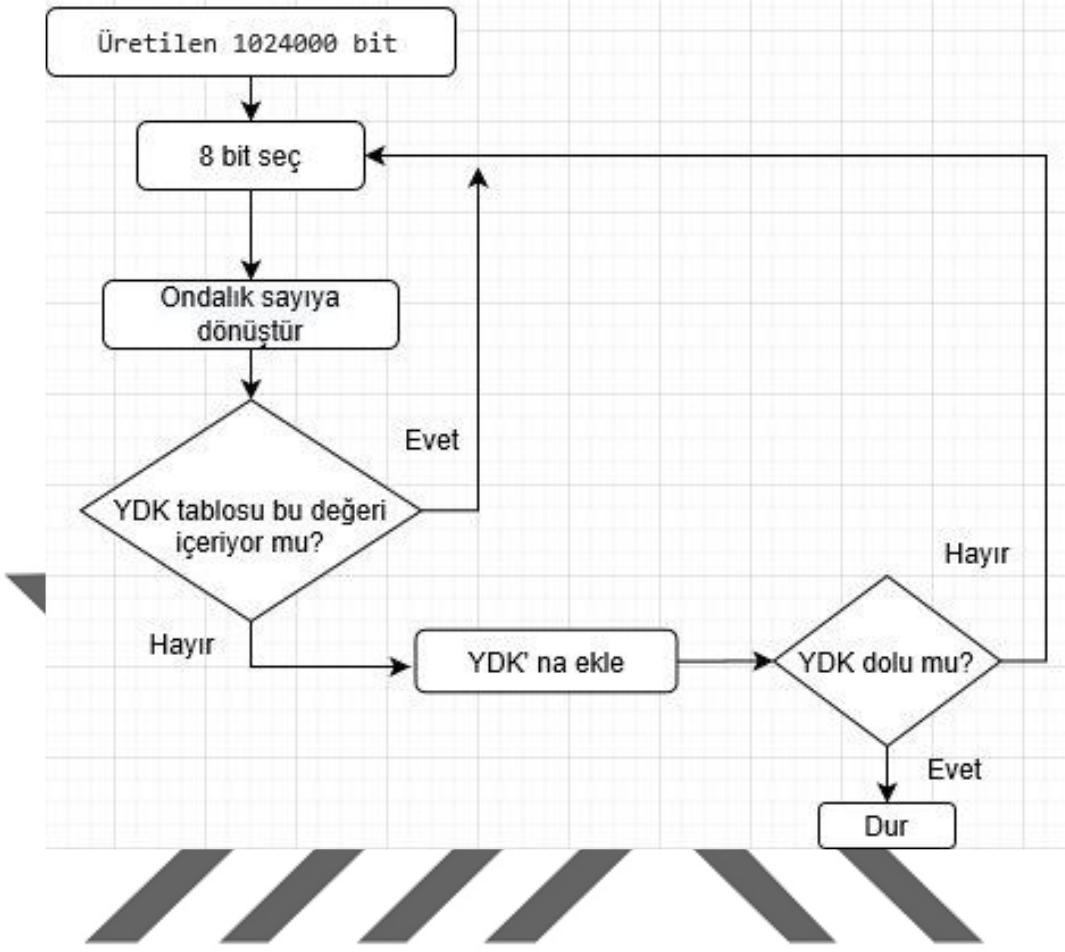
Adım 5. RSÜ Tasarım Mantığına Karar Verilmesi: Literatürde birçok farklı RSÜ tasarım mantığı bulunmaktadır. Rastgele sayıları üretmek için literatürde yaygın şekilde kullanılan bir yöntem; seçilen eşik değerine göre kaotik sistem çıkışlarını 0 veya 1 değerlerine dönüştürme işlemidir. Analizlerde eşik değeri olarak 0,5 değeri seçilmiştir. Eğer kaotik sistem çıkışı 0,5’ den küçük ise 0 bit değeri üretilir. Kaotik sistemin çıkış değeri 0,5 değerine eşit veya büyük ise 1 değeri üretilir. Yani kaotik sistem çıkışları bir entropi kaynağı olarak seçilmiş ve kaotik sistem çıkışları 0/1 bit dizisine dönüştürülerek bir rastgele sayı üreteci tasarlanmıştır.

Adım 6. Kaotik Sistemin Başlangıç Koşulları ve Kontrol Parametrelerinin Optimizasyonu: Bu aşamada amacımız üretilen bit dizisinin veya başka bir ifade ile kaos tabanlı RSÜ’ nin rastgelelik karakteristiklerini optimize edecek başlangıç koşulları ve kontrol parametrelerine karar verebilmektir.

**3.2.2. Kaos Tabanlı İdeal Entropi Kaynağından Yer Değiştirme Kutularının Üretilmesi**

İdeal entropi kaynağı belirlenmesinin ardından 1024000 adet bit elde edilmiştir. 1024000 adet bit üretilmesinin sebebi entropi kaynağının istatistiksel özelliklerinin test edilebilmesi ile ilişkilidir. Elde edilen bu entropi kaynağı Şekil 3.5’de akış şeması verilen algoritma kullanılarak 219 adet YDK yapısına dönüştürülmüştür. Üretilen YDK sayısı fazla olduğu için sadece doğrusal olmama ölçütü 105 ve üstü, XOR dağılımı ise 10 olan tabloya Tablo 3.4’ de yer verilmiştir.

14



**Şekil 3.5.** YDK tasarım süreci

**Tablo 3.4.** Doğrusal olmama ölçütü 105 ve üstü XOR dağılımı ise 10 olan YDK yapıları

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Doğrusalsızlık** | | **Bit Bağımsızlık** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  | **YDK** |  | **Kriteri** | |
|  |  |  |  |  |  |  | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |
|  |  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |
|  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | **YDK56** | 100 | 108 | 105 | 103,29 | 0,5002 | 0,5071 | 0,625 | 0,4219 | 10 |
|  | **YDK122** | 102 | 108 | 105 | 104,29 | 0,4962 | 0,5037 | 0,5938 | 0,4062 | 10 |
|  | **YDK168** | 102 | 108 | 105 | 103,57 | 0,4978 | 0,5002 | 0,6094 | 0,3906 | 10 |
|  | **YDK177** | 98 | 108 | 105 | 101,93 | 0,4983 | 0,4949 | 0,6094 | 0,3906 | 10 |
|  | **YDK178** | 102 | 108 | 105 | 104,21 | 0,4999 | 0,5054 | 0,5781 | 0,4219 | 10 |
|  | **YDK200** | 100 | 108 | 105,25 | 103,36 | 0,4999 | 0,5002 | 0,6094 | 0,4062 | 10 |
|  | **YDK210** | 102 | 108 | 105 | 103,5 | 0,4962 | 0,4998 | 0,5781 | 0,375 | 10 |
|  |  |  |  |  |  |  |  |  |  |  |

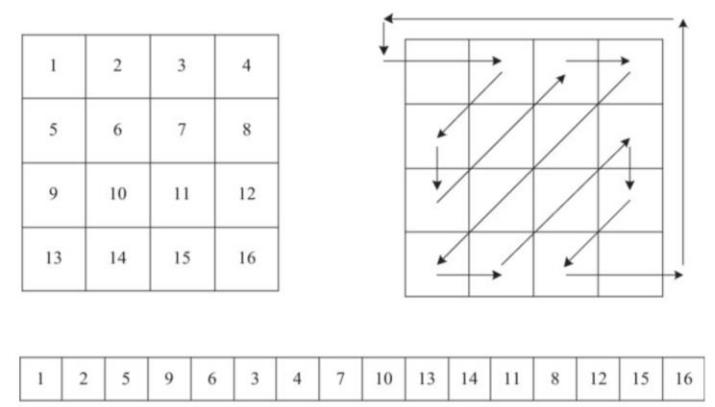
**3.2.3.** **Zig Zag Dönüşüm Yöntemi ile Yer Değiştirme Kutularının Üretilmesi**

Üretilen 219 adet YDK yapısı Şekil 3.6’da gösterilen biçimde yeniden konumlanarak

orijinal 219 adet YDK yapısından değiştirilmiş ve yeni 219 adet YDK yapısı elde edilmiştir. Zig-

15

zag dönüşüm işleminin çalışma mantığı Şekil 3.6’da görselleştirilmiştir. Ayrıca kod parçacığı ve temsili gösterimi Ek-1’de sunulmuştur.



**Şekil 3.6.** Zig-Zag dönüşüm işlemi



Toplam 438 farklı tablo elde edilmiştir, anlamlı olması bakımında yüksek performans ölçütlerine sahip YDK yapıları Tablo 3.5’ de verilmiştir.

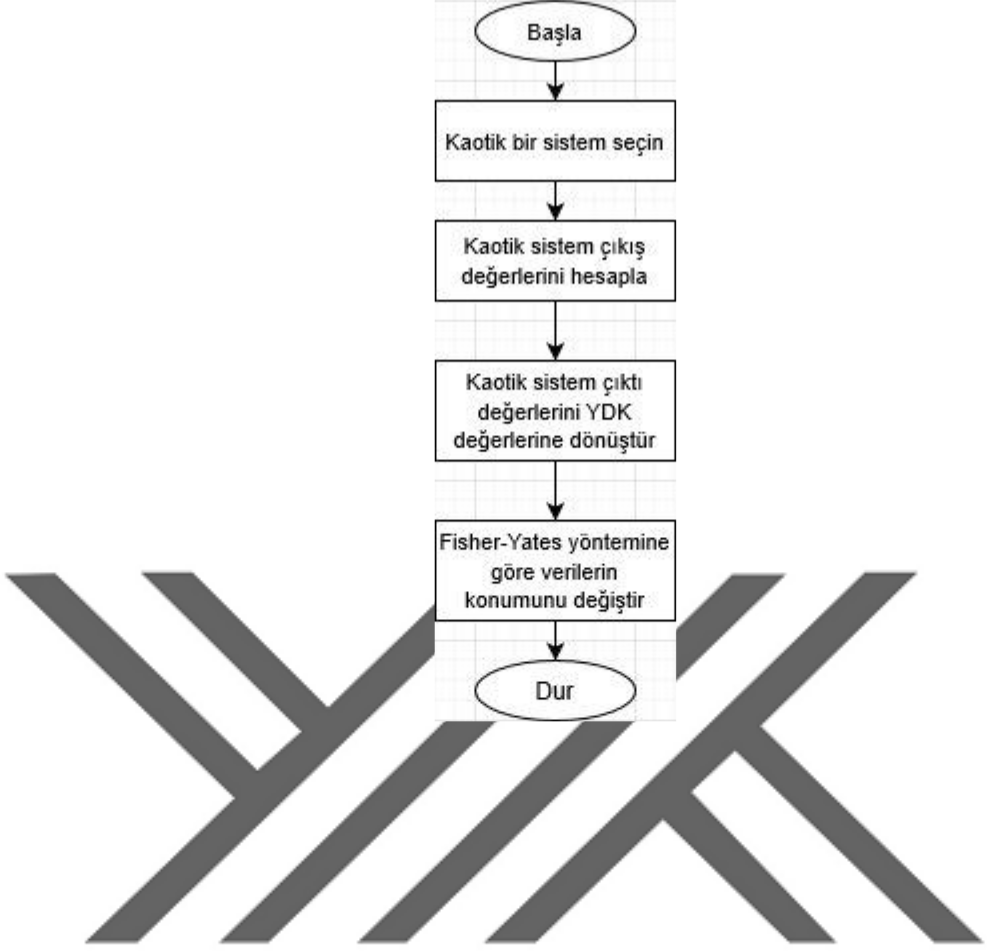
**Tablo 3.5.** Doğrusal olmama ölçütü 105 ve üstü XOR dağılımı ise 10 olan değişen YDK yapıları

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  | **Doğrusalsızlık** | | **Bit Bağımsızlık** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  | **YDK** |  | **Kriteri** | |
|  |  |  |  |  |  |  | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |
|  |  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |
|  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | **YDK\_23** | 102 | 110 | 105,75 | 103,93 | 0,4972 | 0,5073 | 0,5781 | 0,3906 | 10 |
|  | **YDK\_54** | 104 | 108 | 105,5 | 102,93 | 0,5026 | 0,5054 | 0,5938 | 0,3906 | 10 |
|  | **YDK\_58** | 102 | 108 | 105,25 | 103,21 | 0,4971 | 0,5 | 0,6094 | 0,4219 | 10 |
|  | **YDK\_71** | 100 | 108 | 105,75 | 104,79 | 0,4995 | 0,488 | 0,6094 | 0,4062 | 10 |
|  |  |  |  |  |  |  |  |  |  |  |

**3.3.** **Performans İyileştirmesi için Önerilen Algoritma III**

Bu bölümde önerilen algoritma Fisher Yates isimli dizi karma algoritması kullanılarak YDK doğrusalsızlık metriğinin iyileştirmesini amaçlamaktadır. Algoritmanın akış şeması Şekil 3.7’ de verilmiştir [87].

16



**Şekil 3.7.** Önerilen yöntemin akış şeması

Önerilen algoritmanın özgün yönü Fisher Yates isimli dizi karma algoritmasıdır. Bu algoritmanın çalışma mantığı Şekil 3.8’ de gösterilen akış şeması ile açıklanmaya çalışılmıştır.



**Şekil 3.8.** Fisher-Yates yönteminin akış şeması

17

Fisher Yates algoritmasının çalışma mantığı adım adım Tablo 3.6’ da basitleştirilmiş bir örnek kullanılarak gösterilmiştir. Aşağıdaki örnekte 8 elemanlı bir dizinin karma süreci adım adım gösterilmiştir.

**Tablo 3.6.** Fisher-Yates yönteminin adım adım çalışması

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Aralık** | **Rulo** |  |  | **Çizgi** | | | | | | **Sonuç** |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | 12345678 | | | | | | | |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | **1-8** | 3 | 1 2 | | ~~3~~ | 45678 | | | | | 3 |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | **1-7** | 4 | 1 2 | | ~~3~~ | 4 | ~~5~~ | 6 7 8 | | | 3 5 |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | **1-6** | 5 | 1 2 | | ~~3~~ | 4 | ~~5~~ | 6 | ~~7~~ | 8 | 3 5 7 |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | **1-5** | 3 | 1 2 | | ~~3~~ | ~~4~~ | ~~5~~ | 6 | ~~7~~ | 8 | 3574 |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | **1-4** | 4 | 1 2 | | ~~3~~ | ~~4~~ | ~~5~~ | 6 | ~~7~~ | ~~8~~ | 35748 |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | **1-3** | 1 | ~~1~~ | 2 | ~~3~~ | ~~4~~ | ~~5~~ | 6 | ~~7~~ | ~~8~~ | 357481 |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  | **1-2** | 2 | ~~1~~ | 2 | ~~3~~ | ~~4~~ | ~~5~~ | ~~6~~ | ~~7~~ | ~~8~~ | 3574816 |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  | ~~1~~ | ~~2~~ | ~~3~~ | ~~4~~ | ~~5~~ | ~~6~~ | ~~7~~ | ~~8~~ | 35748162 |
|  |  |  |  |  |  |  |  |  |  |  |  |



Tablo 3.7’ de orijinal YDK yapısı verilmiştir. Tablo 3.8‘ de ise önerilen yöntem kullanılarak değiştirilen YDK yapısına yer verilmiştir.

**Tablo 3.7.** Orijinal YDK yapısı

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| **0** | 145 | 154 | 48 | 51 | 61 | 124 | 18 | 83 | 110 | 122 | 227 | 179 | 67 | 206 | 74 | 163 |
| **1** | 42 | 155 | 195 | 248 | 139 | 181 | 114 | 247 | 92 | 82 | 29 | 96 | 34 | 236 | 229 | 75 |
| **2** | 241 | 17 | 91 | 39 | 101 | 28 | 221 | 129 | 147 | 24 | 216 | 250 | 188 | 109 | 217 | 239 |
| **3** | 173 | 1 | 57 | 87 | 50 | 135 | 117 | 86 | 190 | 8 | 200 | 253 | 210 | 7 | 197 | 168 |
| **4** | 166 | 211 | 38 | 119 | 15 | 137 | 182 | 35 | 134 | 228 | 183 | 202 | 37 | 138 | 214 | 120 |
| **5** | 71 | 123 | 240 | 99 | 141 | 191 | 43 | 40 | 108 | 209 | 94 | 249 | 151 | 66 | 152 | 69 |
| **6** | 22 | 63 | 121 | 242 | 140 | 98 | 45 | 235 | 95 | 107 | 133 | 255 | 150 | 102 | 161 | 2 |
| **7** | 125 | 178 | 104 | 105 | 12 | 32 | 41 | 118 | 88 | 184 | 84 | 225 | 233 | 245 | 21 | 112 |
| **8** | 177 | 185 | 127 | 153 | 212 | 157 | 187 | 169 | 237 | 158 | 254 | 243 | 113 | 25 | 89 | 219 |
| **9** | 44 | 80 | 54 | 30 | 116 | 27 | 223 | 244 | 146 | 132 | 10 | 78 | 193 | 164 | 49 | 203 |
| **A** | 246 | 59 | 198 | 230 | 85 | 11 | 199 | 55 | 9 | 194 | 31 | 20 | 159 | 73 | 13 | 167 |
| **B** | 213 | 53 | 36 | 126 | 165 | 115 | 70 | 162 | 215 | 175 | 77 | 174 | 46 | 128 | 220 | 4 |
| **C** | 251 | 160 | 65 | 208 | 5 | 130 | 143 | 3 | 192 | 93 | 189 | 33 | 136 | 23 | 52 | 106 |
| **D** | 204 | 0 | 64 | 172 | 196 | 207 | 103 | 232 | 131 | 176 | 148 | 186 | 72 | 149 | 60 | 252 |
| **E** | 90 | 100 | 97 | 180 | 201 | 79 | 224 | 231 | 111 | 226 | 14 | 171 | 205 | 19 | 170 | 218 |
| **F** | 47 | 142 | 238 | 234 | 81 | 26 | 156 | 16 | 222 | 58 | 68 | 144 | 6 | 62 | 56 | 76 |

18

**Tablo 3.8.** Değiştirilen YDK yapısı

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| **0** | 132 | 94 | 162 | 67 | 139 | 241 | 137 | 32 | 27 | 107 | 64 | 165 | 63 | 255 | 41 | 227 |
| **1** | 163 | 205 | 77 | 206 | 230 | 127 | 244 | 130 | 81 | 170 | 171 | 122 | 203 | 210 | 158 | 24 |
| **2** | 113 | 101 | 238 | 1 | 95 | 252 | 78 | 75 | 195 | 190 | 229 | 29 | 2 | 51 | 123 | 240 |
| **3** | 124 | 91 | 202 | 199 | 208 | 209 | 76 | 221 | 152 | 136 | 180 | 233 | 68 | 79 | 191 | 153 |
| **4** | 186 | 141 | 133 | 176 | 150 | 52 | 5 | 88 | 142 | 129 | 104 | 20 | 177 | 207 | 131 | 23 |
| **5** | 38 | 102 | 126 | 220 | 90 | 98 | 164 | 242 | 82 | 72 | 135 | 55 | 231 | 160 | 185 | 21 |
| **6** | 45 | 99 | 62 | 9 | 211 | 197 | 103 | 112 | 54 | 46 | 80 | 234 | 222 | 71 | 40 | 167 |
| **7** | 47 | 92 | 155 | 118 | 96 | 245 | 178 | 58 | 115 | 193 | 11 | 219 | 31 | 100 | 173 | 179 |
| **8** | 16 | 214 | 28 | 43 | 56 | 156 | 19 | 6 | 7 | 120 | 93 | 109 | 236 | 42 | 175 | 174 |
| **9** | 189 | 105 | 128 | 14 | 83 | 18 | 61 | 108 | 144 | 201 | 84 | 33 | 154 | 119 | 183 | 125 |
| **A** | 10 | 237 | 235 | 159 | 225 | 134 | 106 | 65 | 215 | 166 | 147 | 196 | 87 | 148 | 114 | 213 |
| **B** | 111 | 121 | 59 | 66 | 184 | 73 | 34 | 168 | 35 | 232 | 182 | 60 | 53 | 138 | 216 | 17 |
| **C** | 116 | 187 | 254 | 44 | 146 | 194 | 74 | 13 | 70 | 181 | 217 | 247 | 248 | 15 | 8 | 212 |
| **D** | 228 | 223 | 169 | 249 | 246 | 161 | 198 | 204 | 89 | 36 | 117 | 151 | 0 | 218 | 12 | 37 |
| **E** | 50 | 172 | 226 | 48 | 85 | 253 | 69 | 145 | 30 | 49 | 22 | 157 | 4 | 110 | 86 | 39 |
| **F** | 25 | 149 | 57 | 188 | 3 | 243 | 250 | 192 | 143 | 200 | 97 | 239 | 140 | 26 | 224 | 251 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |



19

1. **KAOS TABANLI YENİ BİR YDK TASARIM ALGORİTMASI**

Bu bölümde YDK tasarımı için literatürde ilk defa kullanılan bir kaotik sistem temel alınarak yeni bir YDK tasarımı gerçekleştirilmiştir. Bu bölüm iki alt bölümden oluşmaktadır. İlk bölümde Nose–Hoover kaotik sisteminin detaylarına yer verilmiştir. İkinci alt bölümde ise YDK yapısının nasıl elde edildiği açıklanmıştır.

**4.1.** **Nose–Hoover Kaotik Sistemi**

Bu bölümde Nose–Hoover kaotik sistemi temel alınarak geliştirilen yeni bir yer değiştirme kutu yapısının detaylarına yer verilmiştir. Geliştirilen yöntemin özgün yönü, YDK yapılarının başarısını ölçmek için kullanılan değerlendirme kriterleri analiz edildiğinde elde edilen başarılı analiz sonuçları, önerilen yeni kaos tabanlı YDK yapısının diğer üçüncü dereceden kaos tabanlı YDK yapılarına alternatif olabileceğini göstermiş olmasıdır [88].



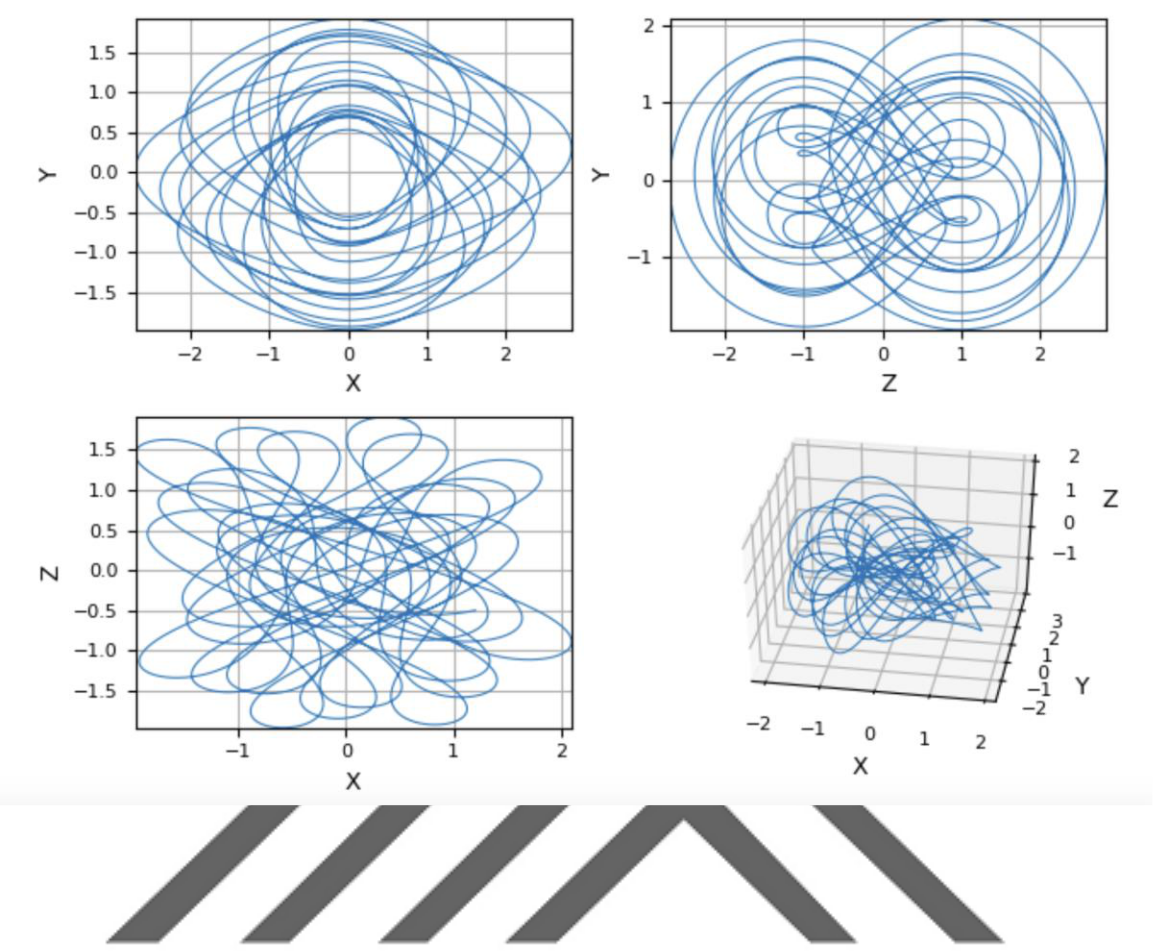
İkinci bölümde daha önce açıklandığı gibi kaotik sistemler genellikle iki ana kategori içerisinde sınıflandırılmaktadır. Bu kategoriler ayrık ve sürekli zamanlı kaotik sistemlerdir. Ayrık zamanlı kaotik sistemler daha basit matematiksel yapıya sahipken sürekli zamanlı sistemler daha karmaşıktır. Çünkü sürekli zamanlı bir sistemde kaotik davranışın gözlemlenebilmesi için sistemin en az üçüncü dereceden bir sistem olması gerekmektedir. Bu yüzden literatürde Lorenz, Chen, Rossler ve Chua devresi gibi birçok üçüncü dereceden kaotik sistem kullanılarak kriptolojik tasarımlar geliştirilmiştir. Bu bölümde önerilen yöntemde ise bu sistemlere alternatif olabilecek bir diğer kaotik sistem olan Nose–Hoover sistemi temel alınarak bir tasarım yapılmıştır.

Nose–Hoover sisteminde yukarıda sayılan sistemler gibi üçüncü dereceden bir sistemdir. Adi diferansiyel denklemler kullanılarak tanımlanmaktadır. Sistemin matematiksel modeli Denklem 4.1’ de verilmiştir. Denklem 4.1’ de ifade edildiği sistemin üç başlangıç koşulu bulunmaktadır. Diğer üçüncü dereceden kaotik sistemlerden farklı olarak Nose–Hoover sistemi herhangi bir kontrol parametresine sahip değildir.

|  |  |
| --- | --- |
| *dx/dt = y* |  |
| *dy/dt = y \* z – x* | (4.1) |
| *dz/dt = 1 – y\*y* |  |

Nose–Hoover sisteminin durum değişkenlerinin değişimini gösteren faz uzayı grafikleri Şekil 4.1’ de gösterilmiştir.

20

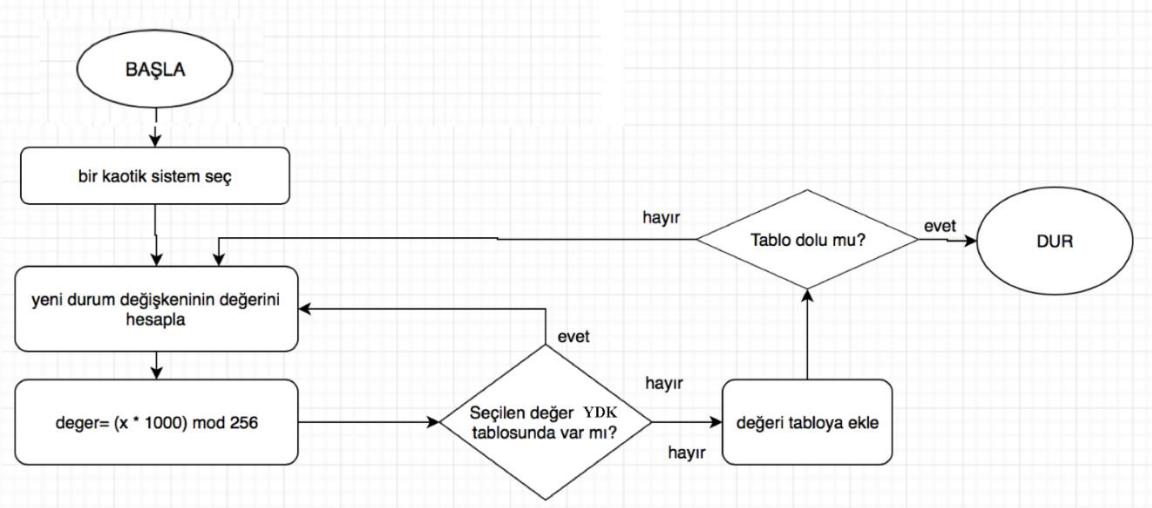


**Şekil 4.1.** Nose–Hoover sisteminin faz uzayı analizi

**4.2.** **YDK Tasarım Yaklaşımı**

Önerilen yöntemin temel amaçlarından biri üçüncü dereceden diğer kaotik sistemlere alternatif olabilecek yeni bir YDK yapısı önermek olduğu için Kaynak [35]’de önerilen yöntem temel alınarak YDK yapısı oluşturulmuştur. Yöntemin detayları için Şekil 4.2 incelenebilir. Bu yöntemde sadece kaotik sistem olarak Nose–Hoover sistemi kullanılmıştır. Bu yöntemle elde edilen YDK yapısı Tablo 4.1’ de verilmiştir.

21



**Şekil 4.2.** Önerilen yöntemin algoritması



**Tablo 4.1.** Önerilen YDK yapısı

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **A** | **B** | **C** | **D** | **E** | **F** |
| **0** | 19 | 100 | 82 | 169 | 62 | 29 | 131 | 137 | 16 | 49 | 240 | 105 | 155 | 43 | 152 | 73 |
| **1** | 36 | 171 | 57 | 18 | 237 | 81 | 247 | 136 | 98 | 9 | 195 | 97 | 228 | 17 | 235 | 165 |
| **2** | 224 | 218 | 193 | 232 | 177 | 229 | 147 | 227 | 35 | 71 | 46 | 54 | 216 | 58 | 238 | 53 |
| **3** | 23 | 175 | 139 | 75 | 151 | 33 | 129 | 163 | 252 | 248 | 96 | 61 | 225 | 254 | 68 | 40 |
| **4** | 21 | 250 | 176 | 78 | 253 | 4 | 200 | 183 | 162 | 66 | 145 | 188 | 243 | 28 | 166 | 64 |
| **5** | 255 | 22 | 133 | 161 | 39 | 55 | 197 | 191 | 143 | 173 | 104 | 63 | 206 | 83 | 233 | 50 |
| **6** | 220 | 106 | 154 | 205 | 146 | 181 | 24 | 67 | 25 | 90 | 48 | 111 | 239 | 77 | 101 | 226 |
| **7** | 74 | 164 | 102 | 204 | 44 | 14 | 87 | 217 | 236 | 91 | 168 | 158 | 120 | 65 | 122 | 119 |
| **8** | 142 | 10 | 76 | 244 | 189 | 37 | 222 | 207 | 56 | 246 | 174 | 84 | 214 | 60 | 230 | 42 |
| **9** | 79 | 182 | 221 | 126 | 1 | 2 | 198 | 38 | 245 | 180 | 251 | 116 | 88 | 89 | 134 | 5 |
| **A** | 231 | 112 | 190 | 69 | 201 | 0 | 72 | 215 | 31 | 167 | 234 | 113 | 209 | 199 | 109 | 186 |
| **B** | 196 | 95 | 178 | 86 | 52 | 20 | 132 | 128 | 41 | 7 | 13 | 156 | 202 | 3 | 123 | 212 |
| **C** | 12 | 213 | 160 | 223 | 51 | 93 | 70 | 203 | 242 | 110 | 15 | 125 | 118 | 30 | 80 | 184 |
| **D** | 187 | 47 | 115 | 208 | 45 | 121 | 210 | 6 | 194 | 108 | 144 | 117 | 138 | 85 | 211 | 148 |
| **E** | 141 | 192 | 107 | 103 | 124 | 172 | 11 | 241 | 219 | 130 | 159 | 185 | 26 | 170 | 149 | 27 |
| **F** | 127 | 34 | 99 | 153 | 135 | 140 | 179 | 114 | 59 | 157 | 94 | 92 | 8 | 249 | 32 | 150 |
|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

22

Yukarıda Tablo 4.1’ de verilen YDK yapısının performans analizleri için Tablo 4.2 incelenebilir.

**Tablo 4.2.** YDK yapısının performans analizleri

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **Doğrusalsızlık** | **Katı Çığ Kriteri** | **Bit Bağımsızlık Kriteri** | | **Giriş / Çıkış XOR** |
|  | **Ortalaması** | **Ortalaması** |  |  | **Dağılımı** |
|  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  | **BBK-** | **Mak.** | **Mak.** |
|  |  |  | **KÇK** |  |  |
|  |  |  |  |  |  |
|  | 104,25 | 0,5044 | 0,502 | 103,93 | 10 |
|  |  |  |  |  |  |



23

1. **BULGULAR VE TARTIŞMA**

En genel ifade ile bir kriptolojik YDK yapısının tasarımı Denklem 5.1’ de verildiği gibi doğrusal olmayan bire bir ve örten bir fonksiyon tasarımı ile ilişkilidir. Denklem 5.1’ de ifade edildiği gibi YDK büyüklüğüne bağlı olarak 0 ile n arasındaki sayılar yine 0 ile n arasındaki sayılara dönüştürülerek karıştırma özelliğinin sağlanması garanti edilmeye çalışılmaktadır. YDK yapılarının kriptolojik özelliklerini değerlendirmek için fonksiyonun bire bir ve örten (bijektive) olmasının yanı sıra doğrusal olmama, giriş çıkış bağımsızlığı, katı çığ kriteri ve diferansiyel kripto analizle ilişkili olan XOR dağılım tablosu gibi kriterler bulunmaktadır [26, 27, 72].

|  |  |
| --- | --- |
| *S(n):[0:n]→[0:n]* | (5.1) |



YDK tasarımı blok şifreleme algoritmalarının tarihsel gelişiminde önemli bir rol oynamıştır. Data Encryption Standart (DES) algoritmasında kullanılan YDK yapısının tasarım prensiplerinin açıklanmamış olması, diferansiyel saldırılara karşı dirençli olmadığının gösterilmesi araştırmacıları yeni bir blok şifreleme algoritması tasarım sürecine yönlendirmiş ve 2000’li yılların başında AES algoritması ortaya çıkmıştır. AES algoritmasında kullanılan YDK yapısı Nyberg tarafından indirgenemez polinomlarda ters haritalama yöntemi kullanılarak tasarlanmıştır. DES YDK yapısının problemlerini gideren bu tasarım güçlü matematiksel fonksiyonlara dayandığı için kriptolojik özellikler bakımından herhangi bir zayıflık içermediği görülmüştür. AES YDK yapısının kriptolojik özellikleri Tablo 5.1’ de verilmiştir [26, 27]

**Tablo 5.1.** AES YDK yapısının kriptolojik özellikleri

|  |  |
| --- | --- |
| **Kriptolojik Özellik** | **Değer** |
| Doğrusal Olmama (nonlinearity) | 112 |
| Katı Çığ Kriteri (KÇK) | 0,5 |
| Giriş/Çıkış Bitleri - nonlinearity | 112 |
| Giriş/Çıkış Bitleri - KÇK | 0,5 |
| XOR Dağılım Tablosu | 4 |

Bir YDK yapısının başarısını değerlendirmek için genellikle beş kriter kullanılmaktadır. Bu kriterler birebir ve örten olması (bijective property), doğrusal olmama (nonlinearity) özelliği, giriş çıkış bitlerinin bağımsızlığı kriteri (Bit Independence Criterion /BIC), katı çığ kriteri (strict avalance criterion) ve giriş/çıkış XOR dağılımı (input/output XOR distribution) kriterleridir. YDK üretimi için kullanılan yöntem bijective özelliğini otomatik olarak sağladığı için Tablo 5.1’ de bu özelliğe yer verilmemiştir. Doğrusal olmama değerinin maksimum değeri kaos tabanlı YDK yapıları için 106,75 olduğu bilinmektedir. Önerilen yeni YDK yapısı bu değere çok yakındır. Katı

çığ kriteri için en uygun değer 0,5’dir. Bu ölçüt içinde çok yakın sonuçların elde edildiği gözlemlenmiştir. BIC ölçümü önceki iki kriter ile bağlantılıdır ve bu kriter de başarılı biçimde sağlanmıştır. Son değerlendirme kriteri için ise kaos tabanlı tasarımlarda ulaşılabilecek minimum değer 10’dur. Analiz sonuçları bu kriterinde sağlandığını göstermiştir.

Bu bölümde Bölüm 3’ de önerilen her bir YDK tasarım yönteminin yukarıda listelenen performans metrikleri için elde edilen bulguları tartışılmıştır.

**5.1.** **Algoritma I Performans Analizleri**

Bölüm 3.1’de açıklanan yöntem kullanılarak öncelikle iki farklı YDK yapısı üretilmiştir (Tablo 3.2 ve Tablo 3.3 ). Bu iki YDK yapısı ile sekiz farklı son işlem algoritması kullanılarak 16 farklı YDK elde edilmiştir. Son işlemler sonucunda üretilen YDK yapılarının performans üzerinde olumlu etkileri olduğu görülmüştür. Önerilen yöntemin başarısını genelleştirmek için her bir son işlem algoritması için 20 farklı YDK yapısı kullanılarak toplam 160 YDK yapısı elde edilmiştir. Bu YDK yapılarına, önerilen son işlem teknikleri uygulanarak gözlemlenen performans iyileştirmeleri Tablo 5.2’ de verilmiştir.



**Tablo 5.2.** Önerilen son işlem teknikleri ile gözlemlenen performans iyileştirmeleri

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Doğrusal Olmama** | **Doğrusal Olmama** |  |
| **Son İşlem Tekniği** | **Ölçütü 103 ve altı** | **Ölçütü 103.5 ve üstü** | **Genel Değerlendirme** |
|  | **olan YDK’ ları için** | **olan YDK ’ları için** |  |
|  |  |  |  |
| **Son İşlem 1** | 9/10 | 3/10 | 13/20 |
| **Son İşlem 2** | 9/10 | 2/10 | 11/20 |
| **Son İşlem 3** | 10/10 | 3/10 | 13/20 |
| **Son İşlem 4** | 7/10 | 2/10 | 9/20 |
| **Son İşlem 5** | 8/10 | 1/10 | 9/20 |
| **Son İşlem 6** | 7/10 | 1/10 | 8/20 |
| **Son İşlem 7** | 5/10 | 1/10 | 6/20 |
| **Son İşlem 8** | 7/10 | 2/10 | 9/20 |
| **Genel Değerlendirme** | 62/80 (%77) | 15/80 (%18) | 77/160 (%48) |
|  |  |  |  |

25

Tablo 5.2 analiz edildiğinde aşağıdaki bulgulara ulaşılmıştır:

* Birden fazla son işlem tekniğini ardı ardına uygulamak yerine tek bir son işlem tekniğinin uygulanmasının performans artışı için daha etkili olduğu gözlemlenmiştir.
* Önerilen son işlem tekniklerinin doğrusal olmama ölçütü göreceli olarak kötü YDK yapılarında daha etkili olduğu gözlemlenmiştir.

İlerideki çalışmalarda daha fazla deneme yapılarak yöntemin başarı yüzdesinin artabileceği düşünülmektedir. Yakın zamanda yayınlanan çalışmalar bu görüşü desteklemektedir [89]

**5.2.** **Algoritma II Performans Analizleri**

Orijinal ve değiştirilmiş YDK yapıları için performans analizleri sırasıyla EK-2 ve EK-3 deki tablolarda verilmiştir.



Literatürdeki mevcut çalışmalar ile Bölüm 3.2.2 ve Bölüm 3.2.3’de listelenen YDK yapılarının performans karşılaştırmaları sırasıyla Tablo 5.3 ve Tablo 5.4’ de verilmiştir.

**Tablo 5.3.** Orijinal entropi kaynağından üretilen YDK yapılarının performans karşılaştırmaları (Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  | **Kriteri** | |  |  |  | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |
|  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |  |
|  |  |  |  |  |  |  |  |  |  |
| Kaynak [49] | 112 | 112 | 112 | 112 | 0,4992 | 0,5049 | 0,5625 | 0,4531 | 4 |
| Kaynak [50] | 112 | 112 | 112 | 112 | 0,4992 | 0,5049 | 0,5625 | 0,4531 | 4 |
| Kaynak [64] | 112 | 112 | 112 | 108 | 0,5027 | 0,5115 | 0,5469 | 0,4219 | 8 |
| Kaynak [53] | 108 | 112 | 109 | 104 | 0,5012 | 0,5012 | 0,5156 | 0,4531 | 8 |
| Kaynak [76] | 106 | 110 | 108,5 | 104 | 0,4971 | 0,5017 | 0,5938 | 0,4062 | 10 |
| Kaynak [42] | 108 | 108 | 108 | 90 | 0,495 | 0,5068 | 0,5781 | 0,4063 | 10 |
| Kaynak [55] | 104 | 110 | 108 | 112 | 0,5006 | 0,5007 | 0,5175 | 0,4258 | 12 |
| Kaynak [69] | 106 | 108 | 107,5 | 104,3 | 0,5001 | 0,4944 | 0,5731 | 0,4219 | 10 |
| Kaynak [57] | 106 | 110 | 107 | 105,5 | 0,501 | 0,5015 | 0,5625 | 0,4063 | 10 |
| Kaynak [35a] | 106 | 108 | 106,7 | 103,5 | 0,4957 | 0,4941 | 0,6094 | 0,3909 | 10 |
| Kaynak [35b] | 106 | 108 | 106,7 | 103,2 | 0,4994 | 0,4063 | 0,4971 | 0,4063 | 10 |
| Kaynak [60] | 106 | 108 | 106,7 | 104 | 0,4951 | 0,5034 | 0,625 | 0,4219 | 10 |
| Kaynak [70] | 104 | 108 | 106,7 | 103,5 | 0,504 | 0,4976 | 0,625 | 0,4062 | 10 |
| Kaynak [61] | 104 | 110 | 106,5 | 105,2 | 0,4984 | 0,512 | 0,6406 | 0,4375 | 10 |
| Kaynak [73] | 106 | 108 | 106,5 | 104,2 | 0,5003 | 0,4978 | 0,5938 | 0,4375 | 10 |
| Kaynak [66] | 104 | 110 | 106,2 | 102,3 | 0,5023 | 0,5039 | 0,5938 | 0,4219 | 10 |
| Kaynak [67] | 102 | 108 | 106 | 105,4 | 0,4968 | 0,5002 | 0,5938 | 0,4219 | 10 |
| Kaynak [71] | 104 | 110 | 106 | 103,5 | 0,4977 | 0,5012 | 0,6406 | 0,4062 | 10 |
| Kaynak [74] | 104 | 110 | 106 | 104,2 | 0,5014 | 0,5197 | 0,625 | 0,4375 | 10 |
| Kaynak [56] | 104 | 108 | 105,7 | 104 | 0,5032 | 0,4976 | 0,5938 | 0,4219 | 10 |
| Kaynak [28] | 100 | 110 | 105,5 | 107 | 0,4983 | 0,5022 | 0,5781 | 0,4063 | 32 |

26

**Tablo 5.3.** Orijinal entropi kaynağından üretilen YDK yapılarının performans karşılaştırmaları (Devamı)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  | **Kriteri** | |  |  |  | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | Kaynak [30] | 98 | 110 | 105,5 | 105,7 | 0,4994 | 0,4926 | 0,5937 | 0,4062 | 32 |
|  | Kaynak [63] | 102 | 110 | 105,5 | 104,3 | 0,4988 | 0,501 | 0,6094 | 0,4063 | 12 |
|  | Kaynak [65] | 102 | 108 | 105,3 | 104 | 0,4971 | 0,5056 | 0,5781 | 0,4375 | 10 |
|  | **YDK200** | **100** | **108** | **105,25** | **103,36** | **0,4999** | **0,5002** | **0,6094** | **0,4062** | **10** |
|  | Kaynak [51] | 102 | 108 | 105,2 | 104,3 | 0,5013 | 0,5059 | 0,5781 | 0,4063 | 12 |
|  | **YDK178** | **102** | **108** | **105** | **104,21** | **0,4999** | **0,5054** | **0,5781** | **0,4219** | **10** |
|  | **YDK56** | **100** | **108** | **105** | **103,29** | **0,5002** | **0,5071** | **0,625** | **0,4219** | **10** |
|  | Kaynak [68] | 104 | 106 | 105 | 103,4 | 0,4994 | 0,5012 | 0,5938 | 0,4063 | 10 |
|  | **YDK177** | **98** | **108** | **105** | **101,93** | **0,4983** | **0,4949** | **0,6094** | **0,3906** | **10** |
|  | **YDK168** | **102** | **108** | **105** | **103,57** | **0,4978** | **0,5002** | **0,6094** | **0,3906** | **10** |
|  | **YDK122** | **102** | **108** | **105** | **104,29** | **0,4962** | **0,5037** | **0,5938** | **0,4062** | **10** |
|  | **YDK210** | **102** | **108** | **105** | **103,5** | **0,4962** | **0,4998** | **0,5781** | **0,375** | **10** |
|  | Kaynak [44] | 100 | 107 | 104,8 | 104,7 | 0,489 | 0,499 | 0,585 | 0,429 | 12 |
|  | Kaynak [58] | 100 | 108 | 104,75 | 103,6 | 0,5009 | 0,4978 | 0,6093 | 0,4218 | 12 |
|  | Kaynak [29] | 100 | 108 | 104,7 | 105 | 0,4965 | 0,4037 | 0,5938 | 0,3906 | 32 |
|  | Kaynak [45] | 102 | 108 | 104,7 | 104,1 | 0,5021 | 0,5056 | 0,5937 | 0,3906 | 12 |
|  | Kaynak [62] | 100 | 108 | 104,7 | 103,1 | 0,4942 | 0,4982 | 0,5781 | 0,4218 | 10 |
|  | Kaynak [72] | 102 | 108 | 104,7 | 103,3 | 0,4972 | 0,5034 | 0,5938 | 0,3906 | 10 |
|  | Kaynak [75] | 102 | 108 | 104,5 | 104,6 | 0,5013 | 0,498 | 0,6406 | 0,4219 | 12 |
|  | Kaynak [40] | 102 | 106 | 104 | 103,2 | 0,4971 | 0,498 | 0,6093 | 0,375 | 10 |
|  | Kaynak [48] | 98 | 108 | 104 | 102 | 0,4967 | 0,4954 | 0,6094 | 0,2813 | 12 |
|  | Kaynak [52] | 100 | 106 | 104 | 102,5 | 0,499 | 0,4946 | 0,625 | 0,375 | 10 |
|  | Kaynak [54] | 102 | 106 | 104 | 103,5 | 0,5019 | 0,5018 | 0,5175 | 0,4825 | 10 |
|  | Kaynak [59] | 98 | 108 | 104 | 104 | 0,5078 | 0,5039 | 0,6093 | 0,4218 | 12 |
|  | Kaynak [38] | 101 | 108 | 103,8 | 102,6 | 0,4958 | 0,5058 | 0,5781 | 0,3906 | 14 |
|  | Kaynak [47] | 101 | 106 | 103,8 | 103,4 | 0,5037 | 0,5036 | 0,6328 | 0,414 | 10 |
|  | Kaynak [37] | 99 | 106 | 103,3 | 103,3 | 0,4995 | 0,4987 | 0,6015 | 0,414 | 10 |
|  | Kaynak [36] | 98 | 108 | 103,2 | 104,2 | 0,5031 | 0,5058 | 0,5975 | 0,3671 | 12 |
|  | Kaynak [41] | 100 | 106 | 103,2 | 103,7 | 0,5009 | 0,5048 | 0,5937 | 0,4218 | 10 |
|  | Kaynak [39] | 100 | 106 | 103 | 103,1 | 0,5024 | 0,5 | 0,6093 | 0,4218 | 14 |
|  | Kaynak [43] | 96 | 106 | 103 | 100,3 | 0,501 | 0,5039 | 0,625 | 0,3906 | 12 |
|  | Kaynak [46] | 98 | 108 | 103 | 104,1 | 0,4988 | 0,5012 | 0,5937 | 0,4062 | 12 |
|  | Kaynak [34] | 96 | 106 | 102,5 | 102,5 | 0,4026 | 0,5178 | 0,6719 | 0,3906 | 54 |
|  | Kaynak [32] | 98 | 108 | 102,3 | 100 | 0,4992 | 0,4836 | 0,6016 | 0,3281 | 14 |
|  | Kaynak [31] | 84 | 106 | 100 | 101,9 | 0,4962 | 0,4812 | 0,625 | 0,125 | 16 |
|  | Kaynak [33] | 84 | 106 | 100 | 101,9 | 0,4962 | 0,4812 | 0,625 | 0,125 | 16 |
|  |  |  |  |  |  |  |  |  |  |  |



27

**Tablo 5.4.** Zig-zag son işlem tekniği uygulanmış YDK yapılarının performans karşılaştırmaları (Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** | **Doğrusalsızlık** | | | **Bit Bağımsızlık** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  | **Kriteri** | |  |  |  | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |
|  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |  |
|  |  |  |  |  |  |  |  |  |  |
| Kaynak [49] | 112 | 112 | 112 | 112 | 0,4992 | 0,5049 | 0,5625 | 0,4531 | 4 |
| Kaynak [50] | 112 | 112 | 112 | 112 | 0,4992 | 0,5049 | 0,5625 | 0,4531 | 4 |
| Kaynak [64] | 112 | 112 | 112 | 108 | 0,5027 | 0,5115 | 0,5469 | 0,4219 | 8 |
| Kaynak [53] | 108 | 112 | 109 | 104 | 0,5012 | 0,5012 | 0,5156 | 0,4531 | 8 |
| Kaynak [76] | 106 | 110 | 108,5 | 104 | 0,4971 | 0,5017 | 0,5938 | 0,4062 | 10 |
| Kaynak [42] | 108 | 108 | 108 | 90 | 0,495 | 0,5068 | 0,5781 | 0,4063 | 10 |
| Kaynak [55] | 104 | 110 | 108 | 112 | 0,5006 | 0,5007 | 0,5175 | 0,4258 | 12 |
| Kaynak [69] | 106 | 108 | 107,5 | 104,3 | 0,5001 | 0,4944 | 0,5731 | 0,4219 | 10 |
| Kaynak [57] | 106 | 110 | 107 | 105,5 | 0,501 | 0,5015 | 0,5625 | 0,4063 | 10 |
| Kaynak [35a] | 106 | 108 | 106,7 | 103,5 | 0,4957 | 0,4941 | 0,6094 | 0,3909 | 10 |
| Kaynak [35b] | 106 | 108 | 106,7 | 103,2 | 0,4994 | 0,4063 | 0,4971 | 0,4063 | 10 |
| Kaynak [60] | 106 | 108 | 106,7 | 104 | 0,4951 | 0,5034 | 0,625 | 0,4219 | 10 |
| Kaynak [70] | 104 | 108 | 106,7 | 103,5 | 0,504 | 0,4976 | 0,625 | 0,4062 | 10 |
| Kaynak [61] | 104 | 110 | 106,5 | 105,2 | 0,4984 | 0,512 | 0,6406 | 0,4375 | 10 |
| Kaynak [73] | 106 | 108 | 106,5 | 104,2 | 0,5003 | 0,4978 | 0,5938 | 0,4375 | 10 |
| Kaynak [66] | 104 | 110 | 106,2 | 102,3 | 0,5023 | 0,5039 | 0,5938 | 0,4219 | 10 |
| Kaynak [67] | 102 | 108 | 106 | 105,4 | 0,4968 | 0,5002 | 0,5938 | 0,4219 | 10 |
| Kaynak [71] | 104 | 110 | 106 | 103,5 | 0,4977 | 0,5012 | 0,6406 | 0,4062 | 10 |
| Kaynak [74] | 104 | 110 | 106 | 104,2 | 0,5014 | 0,5197 | 0,625 | 0,4375 | 10 |
| **YDK\_71** | **100** | **108** | **105,75** | **104,79** | **0,4995** | **0,488** | **0,6094** | **0,4062** | **10** |
| **YDK\_54** | **104** | **108** | **105,5** | **102,93** | **0,5026** | **0,5054** | **0,5938** | **0,3906** | **10** |
| **YDK\_23** | **102** | **110** | **105,75** | **103,93** | **0,4972** | **0,5073** | **0,5781** | **0,3906** | **10** |
| **YDK\_58** | **102** | **108** | **105,25** | **103,21** | **0,4971** | **0,5** | **0,6094** | **0,4219** | **10** |
| Kaynak [56] | 104 | 108 | 105,7 | 104 | 0,5032 | 0,4976 | 0,5938 | 0,4219 | 10 |
| Kaynak [28] | 100 | 110 | 105,5 | 107 | 0,4983 | 0,5022 | 0,5781 | 0,4063 | 32 |
| Kaynak [30] | 98 | 110 | 105,5 | 105,7 | 0,4994 | 0,4926 | 0,5937 | 0,4062 | 32 |
| Kaynak [63] | 102 | 110 | 105,5 | 104,3 | 0,4988 | 0,501 | 0,6094 | 0,4063 | 12 |
| Kaynak [65] | 102 | 108 | 105,3 | 104 | 0,4971 | 0,5056 | 0,5781 | 0,4375 | 10 |
| **YDK200** | **100** | **108** | **105,25** | **103,36** | **0,4999** | **0,5002** | **0,6094** | **0,4062** | **10** |
| Kaynak [51] | 102 | 108 | 105,2 | 104,3 | 0,5013 | 0,5059 | 0,5781 | 0,4063 | 12 |
| **YDK178** | **102** | **108** | **105** | **104,21** | **0,4999** | **0,5054** | **0,5781** | **0,4219** | **10** |
| **YDK56** | 100 | 108 | 105 | 103,29 | 0,5002 | 0,5071 | 0,625 | 0,4219 | 10 |
| Kaynak [68] | 104 | 106 | 105 | 103,4 | 0,4994 | 0,5012 | 0,5938 | 0,4063 | 10 |
| **YDK177** | **98** | **108** | **105** | **101,93** | **0,4983** | **0,4949** | **0,6094** | **0,3906** | **10** |
| **YDK168** | **102** | **108** | **105** | **103,57** | **0,4978** | **0,5002** | **0,6094** | **0,3906** | **10** |
| **YDK122** | **102** | **108** | **105** | **104,29** | **0,4962** | **0,5037** | **0,5938** | **0,4062** | **10** |
| **YDK210** | **102** | **108** | **105** | **103,5** | **0,4962** | **0,4998** | **0,5781** | **0,375** | **10** |
| Kaynak [44] | 100 | 107 | 104,8 | 104,7 | 0,489 | 0,499 | 0,585 | 0,429 | 12 |
| Kaynak [58] | 100 | 108 | 104,75 | 103,6 | 0,5009 | 0,4978 | 0,6093 | 0,4218 | 12 |
| Kaynak [29] | 100 | 108 | 104,7 | 105 | 0,4965 | 0,4037 | 0,5938 | 0,3906 | 32 |
| Kaynak [45] | 102 | 108 | 104,7 | 104,1 | 0,5021 | 0,5056 | 0,5937 | 0,3906 | 12 |
| Kaynak [62] | 100 | 108 | 104,7 | 103,1 | 0,4942 | 0,4982 | 0,5781 | 0,4218 | 10 |
| Kaynak [72] | 102 | 108 | 104,7 | 103,3 | 0,4972 | 0,5034 | 0,5938 | 0,3906 | 10 |



28

**Tablo 5.4.** Zig-zag son işlem tekniği uygulanmış YDK yapılarının performans karşılaştırmaları (Devamı)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **YDK** | **Doğrusalsızlık** | | | **Bit Bağımsızlık** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  |  | **Kriteri** |  |  |  | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | Kaynak [75] | 102 | 108 | 104,5 | 104,6 | 0,5013 | 0,498 | 0,6406 | 0,4219 | 12 |
|  | Kaynak [40] | 102 | 106 | 104 | 103,2 | 0,4971 | 0,498 | 0,6093 | 0,375 | 10 |
|  | Kaynak [48] | 98 | 108 | 104 | 102 | 0,4967 | 0,4954 | 0,6094 | 0,2813 | 12 |
|  | Kaynak [52] | 100 | 106 | 104 | 102,5 | 0,499 | 0,4946 | 0,625 | 0,375 | 10 |
|  | Kaynak [54] | 102 | 106 | 104 | 103,5 | 0,5019 | 0,5018 | 0,5175 | 0,4825 | 10 |
|  | Kaynak [59] | 98 | 108 | 104 | 104 | 0,5078 | 0,5039 | 0,6093 | 0,4218 | 12 |
|  | Kaynak [38] | 101 | 108 | 103,8 | 102,6 | 0,4958 | 0,5058 | 0,5781 | 0,3906 | 14 |
|  | Kaynak [47] | 101 | 106 | 103,8 | 103,4 | 0,5037 | 0,5036 | 0,6328 | 0,414 | 10 |
|  | Kaynak [37] | 99 | 106 | 103,3 | 103,3 | 0,4995 | 0,4987 | 0,6015 | 0,414 | 10 |
|  | Kaynak [36] | 98 | 108 | 103,2 | 104,2 | 0,5031 | 0,5058 | 0,5975 | 0,3671 | 12 |
|  | Kaynak [41] | 100 | 106 | 103,2 | 103,7 | 0,5009 | 0,5048 | 0,5937 | 0,4218 | 10 |
|  | Kaynak [39] | 100 | 106 | 103 | 103,1 | 0,5024 | 0,5 | 0,6093 | 0,4218 | 14 |
|  | Kaynak [43] | 96 | 106 | 103 | 100,3 | 0,501 | 0,5039 | 0,625 | 0,3906 | 12 |
|  | Kaynak [46] | 98 | 108 | 103 | 104,1 | 0,4988 | 0,5012 | 0,5937 | 0,4062 | 12 |
|  | Kaynak [34] | 96 | 106 | 102,5 | 102,5 | 0,4026 | 0,5178 | 0,6719 | 0,3906 | 54 |
|  | Kaynak [32] | 98 | 108 | 102,3 | 100 | 0,4992 | 0,4836 | 0,6016 | 0,3281 | 14 |
|  | Kaynak [31] | 84 | 106 | 100 | 101,9 | 0,4962 | 0,4812 | 0,625 | 0,125 | 16 |
|  | Kaynak [33] | 84 | 106 | 100 | 101,9 | 0,4962 | 0,4812 | 0,625 | 0,125 | 16 |
|  |  |  |  |  |  |  |  |  |  |  |



Yukarıda Tablo 5.3 ve Tablo 5.4’ de; önerilen yapılar ile literatürdeki yapılar, doğrusal olmama ölçütüne göre sıralı bir şekilde (performansı iyiden kötüye doğru) verilmiştir. Zig-zag son işlem tekniği uygulanmadan önce ve sonraki YDK yapıları tablolarda (Tablo 5.3 ve Tablo 5.4) koyu renkle gösterilmiştir, bu tablolar incelendiğinde önerilen yapıların literatürdeki birçok çalışmadan daha iyi sonuçlar verdiği gözlemlenmiştir.

**5.3.** **Algoritma III Performans Analizleri**

Literatürdeki mevcut çalışmalar ile Bölüm 3.3’de verilen Tablo 3.7 ve Tablo 3.8’ e ilişkin performans karşılaştırmaları sırasıyla Tablo 5.5 ve Tablo 5.6’ de verilmiştir.

29

**Tablo 5.5.** Orijinal YDK yapısının performans karşılaştırmaları

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** | **Doğrusalsızlık** | | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  |  |  |  |  | **I/O XOR** |
|  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |
|  |  |  |  |  |  |  |  |  |  |
| Kaynak [49] | 112 | 112 | 112 | 112 | 0,4992 | 0,5049 | 0,5625 | 0,4531 | 4 |
| Kaynak [50] | 112 | 112 | 112 | 112 | 0,4992 | 0,5049 | 0,5625 | 0,4531 | 4 |
| Kaynak [64] | 112 | 112 | 112 | 108 | 0,5027 | 0,5115 | 0,5469 | 0,4219 | 8 |
| Kaynak [53] | 108 | 112 | 109 | 104 | 0,5012 | 0,5012 | 0,5156 | 0,4531 | 8 |
| Kaynak [76] | 106 | 110 | 108,5 | 104 | 0,4971 | 0,5017 | 0,5938 | 0,4062 | 10 |
| Kaynak [42] | 108 | 108 | 108 | 90 | 0,495 | 0,5068 | 0,5781 | 0,4063 | 10 |
| Kaynak [55] | 104 | 110 | 108 | 112 | 0,5006 | 0,5007 | 0,5175 | 0,4258 | 12 |
| Kaynak [69] | 106 | 108 | 107,5 | 104,3 | 0,5001 | 0,4944 | 0,5731 | 0,4219 | 10 |
| Kaynak [57] | 106 | 110 | 107 | 105,5 | 0,501 | 0,5015 | 0,5625 | 0,4063 | 10 |
| Kaynak [35a] | 106 | 108 | 106,7 | 103,5 | 0,4957 | 0,4941 | 0,6094 | 0,3909 | 10 |
| Kaynak [35b] | 106 | 108 | 106,7 | 103,2 | 0,4994 | 0,4063 | 0,4971 | 0,4063 | 10 |
| Kaynak [60] | 106 | 108 | 106,7 | 104 | 0,4951 | 0,5034 | 0,625 | 0,4219 | 10 |
| Kaynak [70] | 104 | 108 | 106,7 | 103,5 | 0,504 | 0,4976 | 0,625 | 0,4062 | 10 |
| Kaynak [61] | 104 | 110 | 106,5 | 105,2 | 0,4984 | 0,512 | 0,6406 | 0,4375 | 10 |
| Kaynak [73] | 106 | 108 | 106,5 | 104,2 | 0,5003 | 0,4978 | 0,5938 | 0,4375 | 10 |
| Kaynak [66] | 104 | 110 | 106,2 | 102,3 | 0,5023 | 0,5039 | 0,5938 | 0,4219 | 10 |
| Kaynak [67] | 102 | 108 | 106 | 105,4 | 0,4968 | 0,5002 | 0,5938 | 0,4219 | 10 |
| Kaynak [71] | 104 | 110 | 106 | 103,5 | 0,4977 | 0,5012 | 0,6406 | 0,4062 | 10 |
| Kaynak [74] | 104 | 110 | 106 | 104,2 | 0,5014 | 0,5197 | 0,625 | 0,4375 | 10 |
| Kaynak [56] | 104 | 108 | 105,7 | 104 | 0,5032 | 0,4976 | 0,5938 | 0,4219 | 10 |
| Kaynak [28] | 100 | 110 | 105,5 | 107 | 0,4983 | 0,5022 | 0,5781 | 0,4063 | 32 |
| Kaynak [30] | 98 | 110 | 105,5 | 105,7 | 0,4994 | 0,4926 | 0,5937 | 0,4062 | 32 |
| Kaynak [63] | 102 | 110 | 105,5 | 104,3 | 0,4988 | 0,501 | 0,6094 | 0,4063 | 12 |
| Kaynak [65] | 102 | 108 | 105,3 | 104 | 0,4971 | 0,5056 | 0,5781 | 0,4375 | 10 |
| Kaynak [51] | 102 | 108 | 105,2 | 104,3 | 0,5013 | 0,5059 | 0,5781 | 0,4063 | 12 |
| Kaynak [68] | 104 | 106 | 105 | 103,4 | 0,4994 | 0,5012 | 0,5938 | 0,4063 | 10 |
| Kaynak [44] | 100 | 107 | 104,8 | 104,7 | 0,489 | 0,499 | 0,585 | 0,429 | 12 |
| Kaynak [58] | 100 | 108 | 104,75 | 103,6 | 0,5009 | 0,4978 | 0,6093 | 0,4218 | 12 |
| Kaynak [29] | 100 | 108 | 104,7 | 105 | 0,4965 | 0,4037 | 0,5938 | 0,3906 | 32 |
| Kaynak [45] | 102 | 108 | 104,7 | 104,1 | 0,5021 | 0,5056 | 0,5937 | 0,3906 | 12 |
| Kaynak [62] | 100 | 108 | 104,7 | 103,1 | 0,4942 | 0,4982 | 0,5781 | 0,4218 | 10 |
| Kaynak [72] | 102 | 108 | 104,7 | 103,3 | 0,4972 | 0,5034 | 0,5938 | 0,3906 | 10 |
| Kaynak [75] | 102 | 108 | 104,5 | 104,6 | 0,5013 | 0,498 | 0,6406 | 0,4219 | 12 |
| Kaynak [40] | 102 | 106 | 104 | 103,2 | 0,4971 | 0,498 | 0,6093 | 0,375 | 10 |
| Kaynak [48] | 98 | 108 | 104 | 102 | 0,4967 | 0,4954 | 0,6094 | 0,2813 | 12 |
| Kaynak [52] | 100 | 106 | 104 | 102,5 | 0,499 | 0,4946 | 0,625 | 0,375 | 10 |
| Kaynak [54] | 102 | 106 | 104 | 103,5 | 0,5019 | 0,5018 | 0,5175 | 0,4825 | 10 |
| Kaynak [59] | 98 | 108 | 104 | 104 | 0,5078 | 0,5039 | 0,6093 | 0,4218 | 12 |
| Kaynak [38] | 101 | 108 | 103,8 | 102,6 | 0,4958 | 0,5058 | 0,5781 | 0,3906 | 14 |
| Kaynak [47] | 101 | 106 | 103,8 | 103,4 | 0,5037 | 0,5036 | 0,6328 | 0,414 | 10 |
| Kaynak [37] | 99 | 106 | 103,3 | 103,3 | 0,4995 | 0,4987 | 0,6015 | 0,414 | 10 |
| Kaynak [36] | 98 | 108 | 103,2 | 104,2 | 0,5031 | 0,5058 | 0,5975 | 0,3671 | 12 |
| Kaynak [41] | 100 | 106 | 103,2 | 103,7 | 0,5009 | 0,5048 | 0,5937 | 0,4218 | 10 |
| Kaynak [39] | 100 | 106 | 103 | 103,1 | 0,5024 | 0,5 | 0,6093 | 0,4218 | 14 |
| Kaynak [43] | 96 | 106 | 103 | 100,3 | 0,501 | 0,5039 | 0,625 | 0,3906 | 12 |
| Kaynak [46] | 98 | 108 | 103 | 104,1 | 0,4988 | 0,5012 | 0,5937 | 0,4062 | 12 |
| Kaynak [34] | 96 | 106 | 102,5 | 102,5 | 0,4026 | 0,5178 | 0,6719 | 0,3906 | 54 |
| Kaynak [32] | 98 | 108 | 102,3 | 100 | 0,4992 | 0,4836 | 0,6016 | 0,3281 | 14 |
| **FY\_YDK** | **98** | **106** | **101,75** | **103,36** | **0,5034** | **0,4905** | **0,5938** | **0,4062** | **10** |
| Kaynak [31] | 84 | 106 | 100 | 101,9 | 0,4962 | 0,4812 | 0,625 | 0,125 | 16 |
| Kaynak [33] | 84 | 106 | 100 | 101,9 | 0,4962 | 0,4812 | 0,625 | 0,125 | 16 |
|  |  |  |  |  |  |  |  |  |  |



30

**Tablo 5.6.** Fisher-Yates yöntemi ile değiştirilen YDK yapısının performans karşılaştırmaları

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** | **Doğrusalsızlık** | | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  |  |  |  |  | **I/O XOR** |
|  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |
|  |  |  |  |  |  |  |  |  |  |
| Kaynak [49] | 112 | 112 | 112 | 112 | 0,4992 | 0,5049 | 0,5625 | 0,4531 | 4 |
| Kaynak [50] | 112 | 112 | 112 | 112 | 0,4992 | 0,5049 | 0,5625 | 0,4531 | 4 |
| Kaynak [64] | 112 | 112 | 112 | 108 | 0,5027 | 0,5115 | 0,5469 | 0,4219 | 8 |
| Kaynak [53] | 108 | 112 | 109 | 104 | 0,5012 | 0,5012 | 0,5156 | 0,4531 | 8 |
| Kaynak [76] | 106 | 110 | 108,5 | 104 | 0,4971 | 0,5017 | 0,5938 | 0,4062 | 10 |
| Kaynak [42] | 108 | 108 | 108 | 90 | 0,495 | 0,5068 | 0,5781 | 0,4063 | 10 |
| Kaynak [55] | 104 | 110 | 108 | 112 | 0,5006 | 0,5007 | 0,5175 | 0,4258 | 12 |
| Kaynak [69] | 106 | 108 | 107,5 | 104,3 | 0,5001 | 0,4944 | 0,5731 | 0,4219 | 10 |
| Kaynak [57] | 106 | 110 | 107 | 105,5 | 0,501 | 0,5015 | 0,5625 | 0,4063 | 10 |
| Kaynak [35a] | 106 | 108 | 106,7 | 103,5 | 0,4957 | 0,4941 | 0,6094 | 0,3909 | 10 |
| Kaynak [35b] | 106 | 108 | 106,7 | 103,2 | 0,4994 | 0,4063 | 0,4971 | 0,4063 | 10 |
| Kaynak [60] | 106 | 108 | 106,7 | 104 | 0,4951 | 0,5034 | 0,625 | 0,4219 | 10 |
| Kaynak [70] | 104 | 108 | 106,7 | 103,5 | 0,504 | 0,4976 | 0,625 | 0,4062 | 10 |
| Kaynak [61] | 104 | 110 | 106,5 | 105,2 | 0,4984 | 0,512 | 0,6406 | 0,4375 | 10 |
| Kaynak [73] | 106 | 108 | 106,5 | 104,2 | 0,5003 | 0,4978 | 0,5938 | 0,4375 | 10 |
| Kaynak [66] | 104 | 110 | 106,2 | 102,3 | 0,5023 | 0,5039 | 0,5938 | 0,4219 | 10 |
| Kaynak [67] | 102 | 108 | 106 | 105,4 | 0,4968 | 0,5002 | 0,5938 | 0,4219 | 10 |
| Kaynak [71] | 104 | 110 | 106 | 103,5 | 0,4977 | 0,5012 | 0,6406 | 0,4062 | 10 |
| Kaynak [74] | 104 | 110 | 106 | 104,2 | 0,5014 | 0,5197 | 0,625 | 0,4375 | 10 |
| Kaynak [56] | 104 | 108 | 105,7 | 104 | 0,5032 | 0,4976 | 0,5938 | 0,4219 | 10 |
| Kaynak [28] | 100 | 110 | 105,5 | 107 | 0,4983 | 0,5022 | 0,5781 | 0,4063 | 32 |
| Kaynak [30] | 98 | 110 | 105,5 | 105,7 | 0,4994 | 0,4926 | 0,5937 | 0,4062 | 32 |
| Kaynak [63] | 102 | 110 | 105,5 | 104,3 | 0,4988 | 0,501 | 0,6094 | 0,4063 | 12 |
| Kaynak [65] | 102 | 108 | 105,3 | 104 | 0,4971 | 0,5056 | 0,5781 | 0,4375 | 10 |
| Kaynak [51] | 102 | 108 | 105,2 | 104,3 | 0,5013 | 0,5059 | 0,5781 | 0,4063 | 12 |
| Kaynak [68] | 104 | 106 | 105 | 103,4 | 0,4994 | 0,5012 | 0,5938 | 0,4063 | 10 |
| Kaynak [44] | 100 | 107 | 104,8 | 104,7 | 0,489 | 0,499 | 0,585 | 0,429 | 12 |
| Kaynak [58] | 100 | 108 | 104,75 | 103,6 | 0,5009 | 0,4978 | 0,6093 | 0,4218 | 12 |
| **FY\_YDK-değ** | **102** | **108** | **104,75** | **104,14** | **0,4981** | **0,5071** | **0,6094** | **0,4219** | **10** |
| Kaynak [29] | 100 | 108 | 104,7 | 105 | 0,4965 | 0,4037 | 0,5938 | 0,3906 | 32 |
| Kaynak [45] | 102 | 108 | 104,7 | 104,1 | 0,5021 | 0,5056 | 0,5937 | 0,3906 | 12 |
| Kaynak [62] | 100 | 108 | 104,7 | 103,1 | 0,4942 | 0,4982 | 0,5781 | 0,4218 | 10 |
| Kaynak [72] | 102 | 108 | 104,7 | 103,3 | 0,4972 | 0,5034 | 0,5938 | 0,3906 | 10 |
| Kaynak [75] | 102 | 108 | 104,5 | 104,6 | 0,5013 | 0,498 | 0,6406 | 0,4219 | 12 |
| Kaynak [40] | 102 | 106 | 104 | 103,2 | 0,4971 | 0,498 | 0,6093 | 0,375 | 10 |
| Kaynak [48] | 98 | 108 | 104 | 102 | 0,4967 | 0,4954 | 0,6094 | 0,2813 | 12 |
| Kaynak [52] | 100 | 106 | 104 | 102,5 | 0,499 | 0,4946 | 0,625 | 0,375 | 10 |
| Kaynak [54] | 102 | 106 | 104 | 103,5 | 0,5019 | 0,5018 | 0,5175 | 0,4825 | 10 |
| Kaynak [59] | 98 | 108 | 104 | 104 | 0,5078 | 0,5039 | 0,6093 | 0,4218 | 12 |
| Kaynak [38] | 101 | 108 | 103,8 | 102,6 | 0,4958 | 0,5058 | 0,5781 | 0,3906 | 14 |
| Kaynak [47] | 101 | 106 | 103,8 | 103,4 | 0,5037 | 0,5036 | 0,6328 | 0,414 | 10 |
| Kaynak [37] | 99 | 106 | 103,3 | 103,3 | 0,4995 | 0,4987 | 0,6015 | 0,414 | 10 |
| Kaynak [36] | 98 | 108 | 103,2 | 104,2 | 0,5031 | 0,5058 | 0,5975 | 0,3671 | 12 |
| Kaynak [41] | 100 | 106 | 103,2 | 103,7 | 0,5009 | 0,5048 | 0,5937 | 0,4218 | 10 |
| Kaynak [39] | 100 | 106 | 103 | 103,1 | 0,5024 | 0,5 | 0,6093 | 0,4218 | 14 |
| Kaynak [43] | 96 | 106 | 103 | 100,3 | 0,501 | 0,5039 | 0,625 | 0,3906 | 12 |
| Kaynak [46] | 98 | 108 | 103 | 104,1 | 0,4988 | 0,5012 | 0,5937 | 0,4062 | 12 |
| Kaynak [34] | 96 | 106 | 102,5 | 102,5 | 0,4026 | 0,5178 | 0,6719 | 0,3906 | 54 |
| Kaynak [32] | 98 | 108 | 102,3 | 100 | 0,4992 | 0,4836 | 0,6016 | 0,3281 | 14 |
| **FY\_YDK** | **98** | **106** | **101,75** | **103,36** | **0,5034** | **0,4905** | **0,5938** | **0,4062** | **10** |
| Kaynak [31] | 84 | 106 | 100 | 101,9 | 0,4962 | 0,4812 | 0,625 | 0,125 | 16 |
| Kaynak [33] | 84 | 106 | 100 | 101,9 | 0,4962 | 0,4812 | 0,625 | 0,125 | 16 |



31

Yukarıda Tablo 5.5 ve Tablo 5.6’ da; önerilen yapılar ile literatürdeki yapılar, doğrusal olmama ölçütüne göre sıralı bir şekilde (performansı iyiden kötüye doğru) verilmiştir. Fisher-Yates son işlem tekniği uygulanmadan önce ve sonraki YDK yapıları tablolarda (Tablo 5.5 ve Tablo 5.6) koyu renkle gösterilmiştir, bu tablolar incelendiğinde son işlem tekniği ile iyileştirilmeden önce daha kötü sonuç veren YDK yapısının işlem sonrası daha iyi sonuç verdiği gözlemlenmiştir. Ayrıca önerilen yapıların literatürdeki birçok çalışmadan daha iyi sonuçlar verdiği gözlemlenmiştir.

**5.4. Nose–Hoover Kaotik Sistemini Temel** **Alan Yer Değiştirme Kutusu** **için**

**Performans Analizleri**

Rasgele seçilen farklı başlangıç koşulları için 100’e yakın YDK yapısı Nose-Hoover kaotik sistemi kullanılarak üretilmiştir. Bu YDK yapılarından sadece doğrusal olmama ölçütü 105 ve üstü olan yapıların performans analizleri aşağıda Tablo 5.7’ de verilmiştir.



**Tablo 5.7.** Nose–Hoover kaotik sistemini temel alan YDKiçinperformans analizleri

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** | **Doğrusalsızlık** | | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  |  |  |  |  | **I/O XOR** |
|  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |
|  |  |  |  |  |  |  |  |  |  |
| **NH\_YDK\_1** | 98 | 108 | 105 | 103 | 0.4969 | 0.5044 | 0.6094 | 0.4219 | 10 |
| **NH\_YDK\_2** | 102 | 108 | 105.5 | 104.36 | 0.5042 | 0.5007 | 0.5038 | 0.4219 | 10 |
| **NH\_YDK\_3** | 104 | 108 | 105.75 | 103.36 | 0.4989 | 0.5132 | 0.625 | 0.4219 | 10 |
| **NH\_YDK\_4** | 100 | 108 | 105 | 103.86 | 0.5011 | 0.4917 | 0.5781 | 0.375 | 10 |
| **NH\_YDK\_5** | 100 | 110 | 105 | 104 | 0.5028 | 0.5005 | 0.6406 | 0.4219 | 10 |
| **NH\_YDK\_6** | 102 | 108 | 105 | 102.36 | 0.5051 | 0.5037 | 0.5625 | 0.4062 | 10 |
| **NH\_YDK\_7** | 104 | 108 | 105.25 | 103.93 | 0.501 | 0.5049 | 0.5938 | 0.4062 | 10 |
| **NH\_YDK\_8** | 100 | 108 | 105 | 103.14 | 0.4984 | 0.4973 | 0.5781 | 0.4062 | 10 |
| **NH\_YDK\_9** | 100 | 108 | 105 | 103.36 | 0.4996 | 0.5073 | 0.6094 | 0.4062 | 10 |
| **NH\_YDK\_10** | 100 | 108 | 105 | 103.71 | 0.4954 | 0.5061 | 0.5938 | 0.4062 | 10 |
| **NH\_YDK\_11** | 102 | 108 | 105 | 103.36 | 0.4952 | 0.5 | 0.5938 | 0.4062 | 10 |
| **NH\_YDK\_12** | 102 | 108 | 105 | 103.29 | 0.5026 | 0.5027 | 0.5938 | 0.4219 | 10 |
| **NH\_YDK\_13** | 102 | 108 | 105.5 | 104.21 | 0.5004 | 0.5022 | 0.6094 | 0.4062 | 10 |
| **NH\_YDK\_14** | 102 | 108 | 105 | 103.21 | 0.4999 | 0.5049 | 0.6094 | 0.4375 | 10 |
| **NH\_YDK\_15** | 104 | 108 | 105.75 | 102.71 | 0.5035 | 0.5022 | 0.625 | 0.3906 | 10 |
| **NH\_YDK\_16** | 102 | 108 | 105.5 | 103.79 | 0.4974 | 0.4956 | 0.6406 | 0.3906 | 10 |
| **NH\_YDK\_17** | 100 | 108 | 105.25 | 102.64 | 0.4946 | 0.5063 | 0.5938 | 0.3906 | 10 |
| **NH\_YDK\_18** | 102 | 108 | 105.25 | 104.21 | 0.4997 | 0.5039 | 0.5938 | 0.4219 | 10 |
| **NH\_YDK\_19** | 102 | 108 | 105 | 103.57 | 0.498 | 0.499 | 0.6094 | 0.4219 | 10 |
| **NH\_YDK\_20** | 102 | 108 | 105 | 102.29 | 0.4981 | 0.5056 | 05938 | 0.4531 | 10 |
|  |  |  |  |  |  |  |  |  |  |

Literatürdeki mevcut çalışmalar ile Tablo 5.7’ de listelenen YDK yapılarının performans

karşılaştırmaları Tablo 5.8’ de verilmiştir. Göreceli olarak az sayıda YDK yapısı üretilmesine

32

rağmen neredeyse %20’sinin literatürdeki birçok YDK’ dan daha iyi doğrusal olmama ölçütüne sahip olması önemli bir avantajdır. Ayrıca Nose-Hoover sisteminin herhangi bir kontrol parametresine sahip olmaması bu kaotik sistemin başlangıç koşullarının optimize edilerek daha uygun rasgelelik karakteristiklerinin elde edilebileceğine işaret etmektedir.

**Tablo 5.8.** Nose–Hoover kaotik sistemini temel alan YDK için performans karşılaştırmaları (Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** | **Doğrusalsızlık** | | | **Bit Bağımsızlık** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  | **Kriteri** | |  |  |  | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |
|  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |  |
|  |  |  |  |  |  |  |  |  |  |
| Kaynak [49] | 112 | 112 | 112 | 112 | 0,4992 | 0,5049 | 0,5625 | 0,4531 | 4 |
| Kaynak [50] | 112 | 112 | 112 | 112 | 0,4992 | 0,5049 | 0,5625 | 0,4531 | 4 |
| Kaynak [64] | 112 | 112 | 112 | 108 | 0,5027 | 0,5115 | 0,5469 | 0,4219 | 8 |
| Kaynak [53] | 108 | 112 | 109 | 104 | 0,5012 | 0,5012 | 0,5156 | 0,4531 | 8 |
| Kaynak [76] | 106 | 110 | 108,5 | 104 | 0,4971 | 0,5017 | 0,5938 | 0,4062 | 10 |
| Kaynak [42] | 108 | 108 | 108 | 90 | 0,495 | 0,5068 | 0,5781 | 0,4063 | 10 |
| Kaynak [55] | 104 | 110 | 108 | 112 | 0,5006 | 0,5007 | 0,5175 | 0,4258 | 12 |
| Kaynak [69] | 106 | 108 | 107,5 | 104,3 | 0,5001 | 0,4944 | 0,5731 | 0,4219 | 10 |
| Kaynak [57] | 106 | 110 | 107 | 105,5 | 0,501 | 0,5015 | 0,5625 | 0,4063 | 10 |
| Kaynak [35a] | 106 | 108 | 106,7 | 103,5 | 0,4957 | 0,4941 | 0,6094 | 0,3909 | 10 |
| Kaynak [35b] | 106 | 108 | 106,7 | 103,2 | 0,4994 | 0,4063 | 0,4971 | 0,4063 | 10 |
| Kaynak [60] | 106 | 108 | 106,7 | 104 | 0,4951 | 0,5034 | 0,625 | 0,4219 | 10 |
| Kaynak [70] | 104 | 108 | 106,7 | 103,5 | 0,504 | 0,4976 | 0,625 | 0,4062 | 10 |
| Kaynak [61] | 104 | 110 | 106,5 | 105,2 | 0,4984 | 0,512 | 0,6406 | 0,4375 | 10 |
| Kaynak [73] | 106 | 108 | 106,5 | 104,2 | 0,5003 | 0,4978 | 0,5938 | 0,4375 | 10 |
| Kaynak [66] | 104 | 110 | 106,2 | 102,3 | 0,5023 | 0,5039 | 0,5938 | 0,4219 | 10 |
| Kaynak [67] | 102 | 108 | 106 | 105,4 | 0,4968 | 0,5002 | 0,5938 | 0,4219 | 10 |
| Kaynak [71] | 104 | 110 | 106 | 103,5 | 0,4977 | 0,5012 | 0,6406 | 0,4062 | 10 |
| Kaynak [74] | 104 | 110 | 106 | 104,2 | 0,5014 | 0,5197 | 0,625 | 0,4375 | 10 |
| **NH\_YDK\_3** | **104** | **108** | **105.75** | **103.36** | **0.4989** | **0.5132** | **0.625** | **0.4219** | **10** |
| **NH\_YDK\_15** | **104** | **108** | **105.75** | **102.71** | **0.5035** | **0.5022** | **0.625** | **0.3906** | **10** |
| Kaynak [56] | 104 | 108 | 105,7 | 104 | 0,5032 | 0,4976 | 0,5938 | 0,4219 | 10 |
| **NH\_YDK\_13** | **102** | **108** | **105.5** | **104.21** | **0.5004** | **0.5022** | **0.6094** | **0.4062** | **10** |
| **NH\_YDK\_2** | **102** | **108** | **105.5** | **104.36** | **0.5042** | **0.5007** | **0.5038** | **0.4219** | **10** |
| Kaynak [28] | 100 | 110 | 105,5 | 107 | 0,4983 | 0,5022 | 0,5781 | 0,4063 | 32 |
| Kaynak [30] | 98 | 110 | 105,5 | 105,7 | 0,4994 | 0,4926 | 0,5937 | 0,4062 | 32 |
| Kaynak [63] | 102 | 110 | 105,5 | 104,3 | 0,4988 | 0,501 | 0,6094 | 0,4063 | 12 |
| **NH\_YDK\_16** | **102** | **108** | **105.5** | **103.79** | **0.4974** | **0.4956** | **0.6406** | **0.3906** | **10** |
| Kaynak [65] | 102 | 108 | 105,3 | 104 | 0,4971 | 0,5056 | 0,5781 | 0,4375 | 10 |
| **NH\_YDK\_7** | **104** | **108** | **105.25** | **103.93** | **0.501** | **0.5049** | **0.5938** | **0.4062** | **10** |
| **NH\_YDK\_18** | **102** | **108** | **105.25** | **104.21** | **0.4997** | **0.5039** | **0.5938** | **0.4219** | **10** |
| **NH\_YDK\_17** | **100** | **108** | **105.25** | **102.64** | **0.4946** | **0.5063** | **0.5938** | **0.3906** | **10** |
| Kaynak [51] | 102 | 108 | 105,2 | 104,3 | 0,5013 | 0,5059 | 0,5781 | 0,4063 | 12 |
| **NH\_YDK\_14** | **102** | **108** | **105** | **103.21** | **0.4999** | **0.5049** | **0.6094** | **0.4375** | **10** |
| **NH\_YDK\_19** | **102** | **108** | **105** | **103.57** | **0.498** | **0.499** | **0.6094** | **0.4219** | **10** |
| **NH\_YDK\_9** | **100** | **108** | **105** | **103.36** | **0.4996** | **0.5073** | **0.6094** | **0.4062** | **10** |

****

33

**Tablo 5.8.** Nose–Hoover kaotik sistemini temel alan YDK için performans karşılaştırmaları (Devamı)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **YDK** | **Doğrusalsızlık** | | | **Bit Bağımsızlık** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  | **Kriteri** | |  |  |  | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  | **min** | **mak** | **ort** | **Doğ.** | **KÇK** | **ort** | **mak** | **min** |  |
|  |  |  |  |  |  |  |  |  |  |  |
|  | Kaynak [68] | 104 | 106 | 105 | 103,4 | 0,4994 | 0,5012 | 0,5938 | 0,4063 | 10 |
|  | **NH\_YDK\_4** | **100** | **108** | **105** | **103.86** | **0.5011** | **0.4917** | **0.5781** | **0.375** | **10** |
|  | **NH\_YDK\_8** | **100** | **108** | **105** | **103.14** | **0.4984** | **0.4973** | **0.5781** | **0.4062** | **10** |
|  | **NH\_YDK\_20** | **102** | **108** | **105** | **102.29** | **0.4981** | **0.5056** | **05938** | **0.4531** | **10** |
|  | **NH\_YDK\_12** | **102** | **108** | **105** | **103.29** | **0.5026** | **0.5027** | **0.5938** | **0.4219** | **10** |
|  | **NH\_YDK\_5** | **100** | **110** | **105** | **104** | **0.5028** | **0.5005** | **0.6406** | **0.4219** | **10** |
|  | **NH\_YDK\_1** | **98** | **108** | **105** | **103** | **0.4969** | **0.5044** | **0.6094** | **0.4219** | **10** |
|  | **NH\_YDK\_10** | **100** | **108** | **105** | **103.71** | **0.4954** | **0.5061** | **0.5938** | **0.4062** | **10** |
|  | **NH\_YDK\_6** | **102** | **108** | **105** | **102.36** | **0.5051** | **0.5037** | **0.5625** | **0.4062** | **10** |
|  | **NH\_YDK\_11** | **102** | **108** | **105** | **103.36** | **0.4952** | **0.5** | **0.5938** | **0.4062** | **10** |
|  | Kaynak [44] | 100 | 107 | 104,8 | 104,7 | 0,489 | 0,499 | 0,585 | 0,429 | 12 |
|  | Kaynak [58] | 100 | 108 | 104,75 | 103,6 | 0,5009 | 0,4978 | 0,6093 | 0,4218 | 12 |
|  | Kaynak [29] | 100 | 108 | 104,7 | 105 | 0,4965 | 0,4037 | 0,5938 | 0,3906 | 32 |
|  | Kaynak [45] | 102 | 108 | 104,7 | 104,1 | 0,5021 | 0,5056 | 0,5937 | 0,3906 | 12 |
|  | Kaynak [62] | 100 | 108 | 104,7 | 103,1 | 0,4942 | 0,4982 | 0,5781 | 0,4218 | 10 |
|  | Kaynak [72] | 102 | 108 | 104,7 | 103,3 | 0,4972 | 0,5034 | 0,5938 | 0,3906 | 10 |
|  | Kaynak [75] | 102 | 108 | 104,5 | 104,6 | 0,5013 | 0,498 | 0,6406 | 0,4219 | 12 |
|  | Kaynak [40] | 102 | 106 | 104 | 103,2 | 0,4971 | 0,498 | 0,6093 | 0,375 | 10 |
|  | Kaynak [48] | 98 | 108 | 104 | 102 | 0,4967 | 0,4954 | 0,6094 | 0,2813 | 12 |
|  | Kaynak [52] | 100 | 106 | 104 | 102,5 | 0,499 | 0,4946 | 0,625 | 0,375 | 10 |
|  | Kaynak [54] | 102 | 106 | 104 | 103,5 | 0,5019 | 0,5018 | 0,5175 | 0,4825 | 10 |
|  | Kaynak [59] | 98 | 108 | 104 | 104 | 0,5078 | 0,5039 | 0,6093 | 0,4218 | 12 |
|  | Kaynak [38] | 101 | 108 | 103,8 | 102,6 | 0,4958 | 0,5058 | 0,5781 | 0,3906 | 14 |
|  | Kaynak [47] | 101 | 106 | 103,8 | 103,4 | 0,5037 | 0,5036 | 0,6328 | 0,414 | 10 |
|  | Kaynak [37] | 99 | 106 | 103,3 | 103,3 | 0,4995 | 0,4987 | 0,6015 | 0,414 | 10 |
|  | Kaynak [36] | 98 | 108 | 103,2 | 104,2 | 0,5031 | 0,5058 | 0,5975 | 0,3671 | 12 |
|  | Kaynak [41] | 100 | 106 | 103,2 | 103,7 | 0,5009 | 0,5048 | 0,5937 | 0,4218 | 10 |
|  | Kaynak [39] | 100 | 106 | 103 | 103,1 | 0,5024 | 0,5 | 0,6093 | 0,4218 | 14 |
|  | Kaynak [43] | 96 | 106 | 103 | 100,3 | 0,501 | 0,5039 | 0,625 | 0,3906 | 12 |
|  | Kaynak [46] | 98 | 108 | 103 | 104,1 | 0,4988 | 0,5012 | 0,5937 | 0,4062 | 12 |
|  | Kaynak [34] | 96 | 106 | 102,5 | 102,5 | 0,4026 | 0,5178 | 0,6719 | 0,3906 | 54 |
|  | Kaynak [32] | 98 | 108 | 102,3 | 100 | 0,4992 | 0,4836 | 0,6016 | 0,3281 | 14 |
|  | Kaynak [31] | 84 | 106 | 100 | 101,9 | 0,4962 | 0,4812 | 0,625 | 0,125 | 16 |
|  | Kaynak [33] | 84 | 106 | 100 | 101,9 | 0,4962 | 0,4812 | 0,625 | 0,125 | 16 |
|  |  |  |  |  |  |  |  |  |  |  |



Yukarıda Tablo 5.8’ de; önerilen yapılar ile literatürdeki yapılar, doğrusal olmama ölçütüne göre sıralı bir şekilde (performansı iyiden kötüye doğru) verilmiştir. Kaos tabanlı yeni bir YDK tasarım algoritması ile elde edilen YDK’ ları Tablo 5.8’ de koyu renkle gösterilmiştir, bu tablo incelendiğinde önerilen yeni yöntemin literatürdeki birçok çalışmadan daha iyi sonuçlar verdiği gözlemlenmiştir.

34

1. **SONUÇLAR**

Bilgi güvenliği kavramı hayatlarımızın dijitalleşmesi ile birlikte giderek önem kazanmıştır. Bu yüzden bilgi güvenliğini problemini adresleyebilmek için kriptolojik protokoller daima aktif bir araştırma konusu olmuştur. Farklı güvenlik gereksinimlerini karşılamak için farklı kriptolojik protokoller oluşturulmuştur. Bu protokollerden biri de blok şifreleme algoritmalarıdır. Blok şifreleme algoritmalarının tasarımında yer değiştirme kutuları doğrusal olmayan tek birleşen olduğu için kritik bir yapı olarak araştırmacıların ilgi odağı haline gelmiştir.

Yer değiştirme kutularının tasarımı için geliştirilen yöntemler kriptolojik protokollere yapılan saldırılar ile değişiklik gösterilmiştir. DES algoritmasında kullanılan YDK yapısına gerçekleştirilen saldırılar sonucunda AES YDK yapısı matematiksel dönüşümleri temel olarak tasarlanmıştır ve doğrusal diferansiyel saldırılara arşı dirençli olduğu gösterilmiştir. Ancak son zamanlarda gerçekleştirilen uygulama saldırıları AES YDK yapılarının çeşitli zafiyetler içerebileceğini göstermiştir. Bu zafiyetleri engellemek için rasgele seçim tabanlı YDK yapılarının bir alternatif olabileceği gösterilmiştir.



Bu tez çalışmasında modern blok şifreleme algoritmalarında kullanılabilecek alternatif YDK yapıları araştırılmıştır. Bu kapsamda aşağıdaki sonuçlar elde edilmiştir.

* YDK performans iyileştirmesi için yeni bir son işlem tekniği önerilmiştir. Önerilen son işlem tekniğinin özellikle düşük performans metriklerine sahip YDK yapılarının doğrusal olmama metriğini iyileştirebileceği gözlemlenmiştir.
* Önerilen son işlem algoritması sekiz farklı teknik içermektedir. Elde edilen başarılı sonuçlar ileride farklı son işlem teknikleri geliştirilerek performans iyileştirmelerinin yapılabileceğini göstermiştir.
* YDK yapılarının üretiminde kullanılan entropi kaynağının rastgeleliğinin iyileştirilerek YDK performans ölçütlerinin iyileştirilebileceği gösterilmiştir. Bu çalışma rastgelelik kaynağının düzensizliği ile YDK performans ölçütleri arasındaki doğrusal ilişkiyi analiz etmiştir.
* Entropi kaynağının rastgeleliğinin iyileştirilmesi için zig-zag dönüşüm tekniği kullanılmıştır. Bu yaklaşımın bir son işlem tekniği olarak kullanılabilecek olması gerçekleştirilen çalışmanın bir diğer avantajıdır.
* YDK tasarım sürecinde entropi kaynağının rastgeleliğine ek olarak çeşitli karma algoritmalarında başarılı performans metrikleri üzerinde başarılı olabileceği gösterilmiştir.
* Önerilen yöntemde Fisher-Yates algoritması gibi güçlü karma algoritmalarının başarısı denenmiştir. Elde edilen başarılı sonuçlar karma tasarım tekniklerinin yeni YDK yapılarının oluşturulmasında kullanılabileceğini göstermiştir.

* Farklı kaotik sistemlerin zengin dinamiklerinin YDK tasarıları için çeşitli fırsatlar barındırdığı gösterilmiştir.
* Literatürde ilk defa Nose – Hoover kaotik sistemini temel alan bir YDK yapısı geliştirilmiştir.
* Nose – Hoover kaotik sistemini üçüncü dereceden kontrol parametresine sahip olmayan bir kaotik sistemdir. Elde edilen başarılı sonuçlar bu gürbüz kaotik sistemin görüntü şifreleme algoritmalarından rasgele sayı üreteçlerine kadar birçok farklı kriptolojik tasarımlarda bilgi güvenliğini sağlamak için kullanılabileceği gösterilmiştir.



36

**ÖNERİLER**

Analiz çalışmaları sonucunda elde edilen başarılı sonuçlar kapsamında ileriye yönelik aşağıdaki çalışmaların yapılması planlanmaktadır.

* Geliştirilen yeni YDK yapılarını AES blok şifreleme algoritmasında kullanarak yan kanal saldırılarına karşı ne kadar direnç gösterdiği analiz edilecektir.
* Farklı son işlem algoritmaları geliştirilerek performans metriklerinin iyileştirilmesi araştırılacaktır.
* Cebirsel tabanlı YDK yapıları ile rasgele seçim tabanlı YDK yapılarının tasarı teknikeri birleştirilerek hibrit tasarım yaklaşımlarının başarısı araştırılacaktır.
* Geliştirilen kriptolojik bileşenlerin görüntü şifreleme algoritması gibi pratik uygulamaları gerçekleştirilecektir.



**KAYNAKLAR**

1. Özkaynak, F. (2018). Brief review on application of nonlinear dynamics in image encryption.

Nonlinear Dynamics, 92(2), 305-313

1. Açikkapi, M. Ş., Özkaynak, F., Özer, A. B. (2019). Side-channel analysis of chaos-based substitution box structures. IEEE Access, 7, 79030-79043
2. Kocarev, L., Lian, S. (Eds.). (2011). Chaos-based cryptography: Theory, algorithms and applications (Vol. 354). Springer Science & Business Media
3. Sprott, J. C. (2010). Elegant chaos: algebraically simple chaotic flows. World Scientific
4. Garipcan, A. M., Erdem, E. (2020). A TRNG using chaotic entropy pool as a post-processing technique: analysis, design and FPGA implementation. Analog Integrated Circuits and Signal Processing, 1-20
5. Ozkaynak, F. (2020). A Novel Random Number Generator Based on Fractional Order Chaotic Chua System. Elektronika ir Elektrotechnika, 26(1), 52-57
6. Garipcan, A. M., Erdem, E. (2019). Implementation and performance analysis of true random number generator on FPGA environment by using non-periodic chaotic signals obtained from chaotic maps. Arabian Journal for Science and Engineering, 44(11), 9427-9441
7. Tanyıldızı, E., Özkaynak, F., (2019). A new chaotic S-box generation method using parameter optimization of one dimensional chaotic maps
8. Özkaynak, F. (2014). Cryptographically secure random number generator with chaotic additional input. Nonlinear Dynamics, 78(3), 2015-2020
9. Nyberg, K. (1993, May). Differentially uniform mappings for cryptography. In Workshop on the Theory and Application of of Cryptographic Techniques (pp. 55-64). Springer, Berlin, Heidelberg
10. Biham, E., Shamir, A. (1991). Differential cryptanalysis of DES-like cryptosystems. Journal of CRYPTOLOGY, 4(1), 3-72
11. Webster, A. F., Tavares, S. (1986). Advances in Cryptology: Proceedings of CRYPTO\_85. Lecture Notes in Computer Science, 523-534
12. Detombe, J., Tavares, S. (1992). Chapter-7. Advances in Cryptology: Proceedings of CRYPTO\_92. Lecture Notes in Computer Science
13. Dawson, M., Tavares, S. (1991). Advances in Cryptology: Proceedings of EUROCRYPT\_91. Lecture Notes in Computer Science, 352-367
14. Pieprzyk, J., Finkelstein, G. (1988). Towards effective nonlinear cryptosystem design. IEE Proceedings E-Computers and Digital Techniques, 135(6), 325-335
15. Lambić, D., Nikolić, M. (2017). Pseudo-random number generator based on discrete-space chaotic map. Nonlinear Dynamics, 90(1), 223-232
16. Dastgheib, M. A., Farhang, M. (2017). A digital pseudo-random number generator based on sawtooth chaotic map with a guaranteed enhanced period. Nonlinear Dynamics, 89(4), 2957-2966
17. Lv, X., Liao, X., Yang, B. (2018). A novel pseudo-random number generator from coupled map lattice with time-varying delay. Nonlinear Dynamics, 94(1), 325-341



1. Sahari, M. L., Boukemara, I. (2018). A pseudo-random numbers generator based on a novel 3D chaotic map with an application to color image encryption. Nonlinear Dynamics, 94(1), 723-744
2. Bakiri, M., Guyeux, C., Couchot, J. F., Oudjida, A. K. (2018). Survey on hardware implementation of random number generators on FPGA: Theory and experimental analyses. Computer Science Review, 27, 135-153
3. Daemen, J., Rijmen, V. (1999). AES proposal: Rijndael.
4. Elmanfaloty, R. A., Abou-Bakr, E. (2019). Random property enhancement of a 1D chaotic PRNG with finite precision implementation. Chaos, Solitons & Fractals, 118, 134-144
5. Asgari-Chenaghlu, M., Balafar, M. A., Feizi-Derakhshi, M. R. (2019). A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation. Signal Processing, 157, 1-13
6. Hemdan, A. M., Faragallah, O. S., Elshakankiry, O., Elmhalaway, A. (2019). A fast hybrid image cryptosystem based on random generator and modified logistic map. Multimedia Tools and Applications, 78(12), 16177-16193
7. Li, B., Liao, X., Jiang, Y. (2019). A novel image encryption scheme based on improved random number generator and its implementation. Nonlinear Dynamics, 95(3), 1781-1805
8. Cusick, T. W., Stanica, P. (2017). Cryptographic Boolean functions and applications. Academic Press
9. Wu, C. K., Feng, D. (2016). Boolean functions and their applications in cryptography. Springer Berlin Heidelberg
10. Hussain, I., Shah, T., Mahmood, H., Gondal, M. A. (2013). A projective general linear group based algorithm for the construction of substitution box for block ciphers. Neural Computing and Applications, 22(6), 1085-1093
11. Hussain, I., Shah, T., Gondal, M. A., Khan, W. A., Mahmood, H. (2013). A group theoretic approach to construct cryptographically strong substitution boxes. Neural Computing and Applications, 23(1), 97-104
12. Khan, M., Shah, T. (2014). A novel image encryption technique based on Hénon chaotic map and S

8 symmetric group. Neural Computing and Applications, 25(7-8), 1717-1722

1. Khan, M. (2015). A novel image encryption scheme based on multiple chaotic S-boxes. Nonlinear Dynamics, 82(1-2), 527-533
2. Jamal, S. S., Khan, M. U., Shah, T. (2016). A watermarking technique with chaotic fractional S-box transformation. Wireless Personal Communications, 90(4), 2033-2049
3. Khan, M., Shah, T., Batool, S. I. (2016). Construction of S-box based on chaotic Boolean functions and its application in image encryption. Neural Computing and Applications, 27(3), 677-685
4. Khan, M., Asghar, Z. (2018). A novel construction of substitution box for image encryption applications with Gingerbreadman chaotic map and S 8 permutation. Neural Computing and Applications, 29(4), 993-999
5. Özkaynak, F. (2019). Construction of robust substitution boxes based on chaotic systems. Neural

Computing and Applications, 31(8), 3317-3326



39

1. Jakimoski, G., Kocarev, L. (2001). Chaos and cryptography: block encryption ciphers based on

chaotic maps. Ieee transactions on circuits and systems i: fundamental theory and applications, 48(2), 163-169

1. Tang, G., Liao, X., Chen, Y. (2005). A novel method for designing S-boxes based on chaotic maps. Chaos, Solitons & Fractals, 23(2), 413-419
2. Tang, G., Liao, X. (2005). A method for designing dynamical S-boxes based on discretized chaotic map. Chaos, solitons & fractals, 23(5), 1901-1909
3. Chen, G., Chen, Y., Liao, X. (2007). An extended method for obtaining S-boxes based on three-dimensional chaotic Baker maps. Chaos, solitons & fractals, 31(3), 571-579
4. Chen, G. (2008). A novel heuristic method for obtaining S-boxes. Chaos, Solitons & Fractals, 36(4), 1028-1036
5. Özkaynak, F., Özer, A. B. (2010). A method for designing strong S-Boxes based on chaotic Lorenz system. Physics Letters A, 374(36), 3733-3738
6. Wang, Y., Wong, K. W., Li, C., Li, Y. (2012). A novel method to design S-box based on chaotic map and genetic algorithm. Physics Letters A, 376(6-7), 827-833
7. Khan, M., Shah, T., Mahmood, H., Gondal, M. A., Hussain, I. (2012). A novel technique for the construction of strong S-boxes based on chaotic Lorenz systems. Nonlinear Dynamics, 70(3), 2303-2311
8. Hussain, I., Shah, T., Mahmood, H., Gondal, M. A. (2012). Construction of S8 Liu J S-boxes and their applications. Computers & Mathematics with Applications, 64(8), 2450-2458
9. Hussain, I., Shah, T., Gondal, M. A. (2012). A novel approach for designing substitution-boxes based on nonlinear chaotic algorithm. Nonlinear Dynamics, 70(3), 1791-1794
10. Khan, M., Shah, T., Mahmood, H., Gondal, M. A. (2013). An efficient method for the construction of block cipher with multi-chaotic systems. Nonlinear Dynamics, 71(3), 489-492
11. Özkaynak, F., Yavuz, S. (2013). Designing chaotic S-boxes based on time-delay chaotic system. Nonlinear Dynamics, 74(3), 551-557
12. Khan, M., Shah, T., Gondal, M. A. (2013). An efficient technique for the construction of substitution box with chaotic partial differential equation. Nonlinear Dynamics, 73(3), 1795-1801
13. Hussain, I., Shah, T., Gondal, M. A., Mahmood, H. (2013). An efficient approach for the construction of LFT S-boxes using chaotic logistic map. Nonlinear Dynamics, 71(1-2), 133-140
14. Hussain, I., Shah, T., Gondal, M. A., Mahmood, H. (2013). Efficient method for designing chaotic S-boxes based on generalized Baker’s map and TDERC chaotic sequence. Nonlinear Dynamics,

74(1-2), 271-275

1. Hussain, I., Shah, T., Gondal, M. A., Mahmood, H. (2013). A novel method for designing nonlinear component for block cipher based on TD-ERCS chaotic sequence. Nonlinear Dynamics, 73(1-2), 633-637
2. Khan, M., Shah, T. (2014). A construction of novel chaos base nonlinear component of block cipher. Nonlinear Dynamics, 76(1), 377-382



40

1. Lambić, D. (2014). A novel method of S-box design based on chaotic map and composition method. Chaos, Solitons & Fractals, 58, 16-21
2. Liu, H., Kadir, A., Niu, Y. (2014). Chaos-based color image block encryption scheme using S-box. AEU-international Journal of Electronics and Communications, 68(7), 676-686
3. Zhang, X., Zhao, Z., Wang, J. (2014). Chaotic image encryption based on circular substitution box and key stream buffer. Signal Processing: Image Communication, 29(8), 902-913
4. Liu, G., Yang, W., Liu, W., Dai, Y. (2015). Designing S-boxes based on 3-D four-wing autonomous chaotic system. Nonlinear Dynamics, 82(4), 1867-1877
5. Ahmad, M., Bhatia, D., Hassan, Y. (2015). A novel ant colony optimization based scheme for substitution box design. Procedia Computer Science, 57(2015), 572-580
6. Khan, M., Shah, T. (2015). An efficient construction of substitution box with fractional chaotic system. Signal, Image and Video Processing, 9(6), 1335-1338
7. Khan, M., Shah, T., Batool, S. I. (2016). A new implementation of chaotic S-boxes in CAPTCHA. Signal, Image and Video Processing, 10(2), 293-300
8. Lambić, D. (2017). A novel method of S-box design based on discrete chaotic map. Nonlinear Dynamics, 87(4), 2407-2413
9. Farah, T., Rhouma, R., Belghith, S. (2017). A novel method for designing S-box based on chaotic map and Teaching–Learning-Based Optimization. Nonlinear Dynamics, 88(2), 1059-1074
10. Özkaynak, F., Çelik, V., Özer, A. B. (2017). A new S-box construction method based on the fractional-order chaotic Chen system. Signal, Image and Video Processing, 11(4), 659-664
11. Belazi, A., Abd El-Latif, A. A. (2017). A simple yet efficient S-box method based on chaotic sine map. Optik, 130, 1438-1444
12. Belazi, A., Abd El-Latif, A. A., Diaconu, A. V., Rhouma, R., Belghith, S. (2017). Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. Optics and Lasers in Engineering, 88, 37-50
13. Belazi, A., Khan, M., Abd El-Latif, A. A., Belghith, S. (2017). Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption. Nonlinear Dynamics, 87(1), 337-361
14. Çavuşoğlu, Ü., Zengin, A., Pehlivan, I., Kaçar, S. (2017). A novel approach for strong S-Box generation algorithm design based on chaotic scaled Zhongtang system. Nonlinear Dynamics, 87(2), 1081-1094
15. ul Islam, F., Liu, G. (2017). Designing S-box based on 4D-4wing hyperchaotic system. 3D Research, 8(1), 9
16. Özkaynak, F. (2017, September). From biometric data to cryptographic primitives: A new method for generation of substitution boxes. In Proceedings of the 2017 International Conference on Biomedical Engineering and Bioinformatics (pp. 27-33)
17. Ahmed, H. A., Zolkipli, M. F., Ahmad, M. (2019). A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. Neural Computing and Applications, 31(11), 7201-7210.



41

1. Ye, T., Zhimao, L. (2018). Chaotic S-box: Six-dimensional fractional Lorenz–Duffing chaotic system and O-shaped path scrambling. Nonlinear Dynamics, 94(3), 2115-2126
2. Çavuşoğlu, Ü., Kaçar, S., Zengin, A., Pehlivan, I. (2018). A novel hybrid encryption algorithm based on chaos and S-AES algorithm. Nonlinear Dynamics, 92(4), 1745-1759
3. Özkaynak, F. (2020). An analysis and generation toolbox for chaotic substitution boxes: A case study based on chaotic labyrinth rene thomas system. Iranian Journal of Science and Technology, Transactions of Electrical Engineering, 44(1), 89-98
4. Lambić, D. (2018). S-box design method based on improved one-dimensional discrete chaotic map. Journal of Information and Telecommunication, 2(2), 181-191
5. Wang, X., Akgul, A., Cavusoglu, U., Pham, V. T., Vo Hoang, D., Nguyen, X. Q. (2018). A chaotic system with infinite equilibria and its S-box constructing application. Applied Sciences, 8(11), 2132
6. Liu, L., Zhang, Y., Wang, X. (2018). A novel method for constructing the S-box based on spatiotemporal chaotic dynamics. Applied Sciences, 8(12), 2650
7. Al Solami, E., Ahmad, M., Volos, C., Doja, M. N., Beg, M. M. S. (2018). A new hyperchaotic system-based design for efficient bijective substitution-boxes. Entropy, 20(7), 525
8. Lambić, D., Živković, M. (2013). Comparison of random S-box generation methods. Publications de l'institut mathematique, 93(107), 109-115
9. Ahmad, M., Ahmad, Z. (2018). Random search based efficient chaotic substitution box design for image encryption. International Journal of Rough Sets and Data Analysis (IJRSDA), 5(2), 131-147
10. Ahmed, H. A., Zolkipli, M. F., Ahmad, M. (2019). A novel efficient substitution-box design based on firefly algorithm and discrete chaotic map. Neural Computing and Applications, 31(11), 7201-7210
11. Ali, K. M., Khan, M. (2019). Application based construction and optimization of substitution boxes over 2D mixed chaotic maps. International Journal of Theoretical Physics, 58(9), 3091-3117
12. Yi, L., Tong, X., Wang, Z., Zhang, M., Zhu, H., Liu, J. (2019). A novel block encryption algorithm based on chaotic S-box for wireless sensor network. IEEE Access, 7, 53079-53090
13. Zahid, A. H., Arshad, M. J. (2019). An innovative design of substitution-boxes using cubic polynomial mapping. Symmetry, 11(3), 437
14. Khan, M. F., Ahmed, A., Saleem, K., Shah, T. (2019). A novel design of cryptographic SP-network based on gold sequences and chaotic logistic tent system. IEEE Access, 7, 84980-84991
15. Naseer, Y., Shah, T., Shah, D., Hussain, S. (2019). A novel algorithm of constructing highly nonlinear sp-boxes. Cryptography, 3(1), 6
16. Khan, M. F., Ahmed, A., Saleem, K. (2019). A novel cryptographic substitution box design using Gaussian distribution. IEEE Access, 7, 15999-16007
17. Bahceci, Y. S., Özkaynak, F.(2019). Rasgele Seçim Tabanlı Yer Değiştirme Kutularının Performans İyileştirmesi için Son İşlem Algoritmaları. Bilgisayar Bilimleri ve Teknolojileri Dergisi, 1(1), 16-21.



42

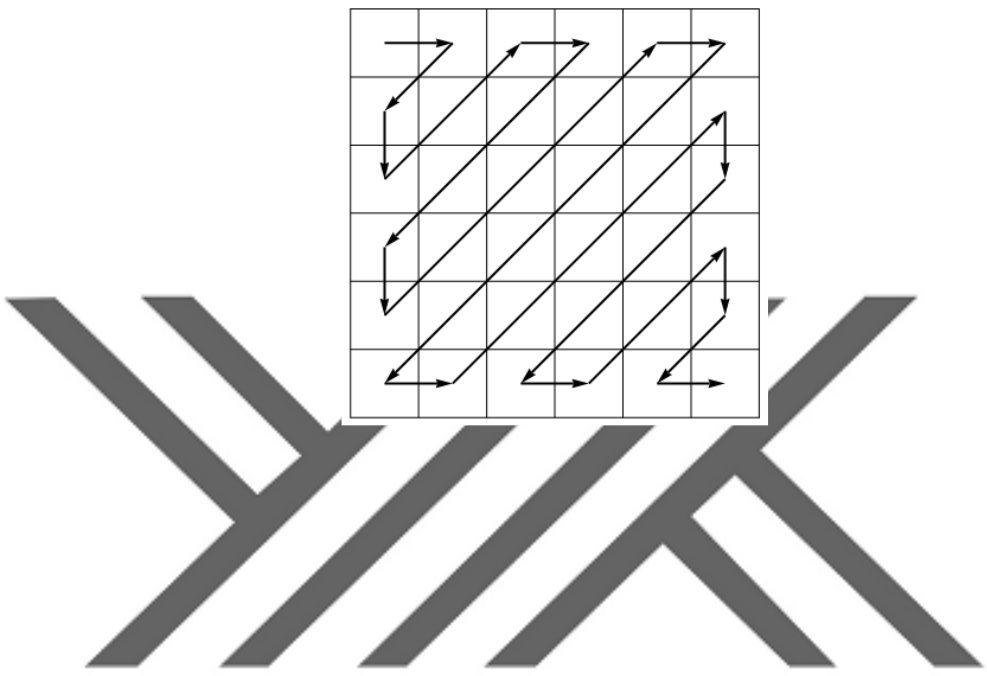
1. Bahceci Y. S., Özkaynak F., (2019), A new method for performance improvement of chaotic s-box structures International Conference on Engineering Technologies, 25-27 October 2019 Konya, Turkey
2. Bahceci Y. S., Özkaynak F., (2020), A New Substitution Box Structure Based on Nose– Hoover Chaotic System , 13th CHAOS2020 Tuesday 9 - Friday 12 June 2020, Florence, Italy
3. Artuğer, F., Özkaynak, F. (2020). A novel method for performance improvement of chaos-based substitution Boxes. Symmetry, 12(4), 571.



43

**EKLER**

**EK- 1:** **ZİG-ZAG ALGORİTMASININ TEMSİLİ GÖSTERİMİ VE KODU**

****

**Şekil E1.1**.Zigzag algortimasının gösterimi

**Tablo E1.1** Zig-zag dönüşüm öncesi temsili matris

|  |  |  |  |
| --- | --- | --- | --- |
| 1 | 2 | 3 | 4 |
|  |  |  |  |
| 5 | 6 | 7 | 8 |
|  |  |  |  |
| 9 | 1 | 2 | 3 |
|  |  |  |  |

**Tablo E1.2** Zig-zag dönüşüm sonrasımatris

1

2

5

9

6

3

4 7 1 2

8

3

**Tablo E1.3** Algoritmanın MatLab kodu

function V=z(M)

[m,n]=size(M);

a=(1:m)'\*ones(1,n);

b=ones(m,1)\*(1:n);

A=a+b-1;

B=a-b;

C=(A.^2+(-1).^A.\*B+1);

[~,I]=sort(C(:));

V=M(:);

V=V(I)';

44

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **EK- 2:** | **ORİJİNAL YDK TABLOSU** | | | |  |  |  |  |  |
|  |  |  | **Tablo E2.1.** Orijinal YDK(Devamı) | | | |  |  |  |
|  |  |  | |  | |  | | |  |
| **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |
| **YDK1** | 98 | 106 | 101,75 | 0.4989 | 102,79 | 0,4062 | 0,5781 | 0,5054 | 10 |
| **YDK2** | 100 | 108 | 104 | 0,4938 | 102,29 | 0,3438 | 0,5781 | 0,5049 | 12 |
| **YDK3** | 98 | 108 | 102,5 | 0.4989 | 103,93 | 0,3281 | 0,6406 | 0,5063 | 12 |
| **YDK4** | 100 | 106 | 103,5 | 0,5067 | 104,36 | 0,3594 | 0,6406 | 0,4983 | 12 |
| **YDK5** | 96 | 106 | 103,25 | 0,4958 | 103,21 | 0,3906 | 0,6406 | 0,4976 | 12 |
| **YDK6** | 102 | 106 | 104 | 0,4981 | 104 | 0,4219 | 0,5938 | 0,5012 | 12 |
| **YDK7** | 96 | 104 | 102 | 0,4994 | 102,64 | 0,375 | 0,6094 | 0,4956 | 10 |
| **YDK8** | 100 | 106 | 103,5 | 0,5031 | 104,21 | 0,4062 | 0,5938 | 0,5032 | 12 |
| **YDK9** | 102 | 108 | 105 | 0,499 | 103,07 | 0,4062 | 0,6094 | 0,4966 | 12 |
| **YDK10** | 98 | 106 | 101,75 | 0,4992 | 103,79 | 0,4219 | 0,6094 | 0,4998 | 10 |
| **YDK11** | 98 | 108 | 102,75 | 0,4967 | 103,07 | 0,375 | 0,6719 | 0,5005 | 10 |
| **YDK12** | 100 | 106 | 104,5 | 0,4979 | 103,64 | 0,4062 | 0,5938 | 0,499 | 10 |
| **YDK13** | 98 | 108 | 104,25 | 0,502 | 103,93 | 0,3906 | 0,5781 | 0,5044 | 10 |
| **YDK14** | 98 | 108 | 102 | 0,4953 | 104,5 | 0,375 | 0,5938 | 0,5005 | 12 |
| **YDK15** | 96 | 106 | 102,5 | 0,5016 | 103,21 | 0,3906 | 0,6094 | 0,5059 | 12 |
| **YDK16** | 98 | 108 | 104 | 0,5017 | 102,64 | 0,4062 | 0,625 | 0,5078 | 10 |
| **YDK17** | 96 | 106 | 103 | 0,4992 | 103,71 | 0,3906 | 0,5938 | 0,5061 | 12 |
| **YDK18** | 100 | 106 | 102,75 | 0,4999 | 102,86 | 0,3906 | 0,625 | 0,498 | 14 |
| **YDK19** | 96 | 108 | 103 | 0,4979 | 103,07 | 0,3906 | 0,625 | 0,5156 | 12 |
| **YDK20** | 100 | 108 | 104,75 | 0,4998 | 103,21 | 0,4062 | 0,625 | 0,5083 | 12 |
| **YDK21** | 100 | 108 | 104,25 | 0,506 | 103,71 | 0,4219 | 0,6094 | 0,5061 | 12 |
| **YDK22** | 102 | 106 | 104,5 | 0,4999 | 102,93 | 0,4062 | 0,5938 | 0,5037 | 14 |
| **YDK23** | 98 | 106 | 103,5 | 0,5048 | 104,21 | 0,4062 | 0,5625 | 0,4949 | 12 |
| **YDK24** | 100 | 106 | 103 | 0,4996 | 102,93 | 0,4062 | 0,625 | 0,4932 | 12 |
| **YDK25** | 98 | 106 | 103 | 0,4987 | 103,79 | 0,4062 | 0,6094 | 0,5049 | 10 |
| **YDK26** | 98 | 104 | 102,5 | 0,4973 | 103,43 | 0,3438 | 0,5938 | 0,5022 | 12 |
| **YDK27** | 96 | 108 | 103,75 | 0,4932 | 103,57 | 0,3906 | 0,5938 | 0,5005 | 12 |
| **YDK28** | 98 | 108 | 103,5 | 0,4985 | 104 | 0,4062 | 0,625 | 0,5027 | 16 |
| **YDK29** | 100 | 108 | 104,5 | 0,5014 | 103,36 | 0,375 | 0,6406 | 0,4961 | 10 |
| **YDK30** | 98 | 108 | 104,25 | 0,4993 | 103,79 | 0,375 | 0,6094 | 0,5066 | 10 |
| **YDK31** | 100 | 106 | 103,75 | 0,5003 | 104,07 | 0,3906 | 0,5781 | 0,4915 | 12 |
| **YDK32** | 100 | 104 | 103 | 0,5024 | 104,14 | 0,4062 | 0,5938 | 0,5 | 14 |
| **YDK33** | 98 | 108 | 103,5 | 0,4996 | 104,36 | 0,3906 | 0,6094 | 0,4995 | 12 |
| **YDK34** | 96 | 108 | 102 | 0,5016 | 103,21 | 0,3906 | 0,5781 | 0,4946 | 10 |
| **YDK35** | 102 | 108 | 104,75 | 0,5034 | 104,43 | 0,375 | 0,6406 | 0,5034 | 10 |
| **YDK36** | 98 | 108 | 102,5 | 0,5006 | 103,21 | 0,4062 | 0,625 | 0,5056 | 10 |
| **YDK37** | 96 | 108 | 102 | 0,5001 | 102,79 | 0,4219 | 0,6094 | 0,5056 | 10 |
|  |  |  |  |  | 45 |  |  |  |  |



**Tablo E2.1.** Orijinal YDK(Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |
| **YDK38** | 98 | 108 | 104,75 | 0,4952 | 103,43 | 0,375 | 0,5938 | 0,4954 | 10 |
| **YDK39** | 100 | 106 | 102,75 | 0,5005 | 104,14 | 0,4062 | 0,625 | 0,4915 | 10 |
| **YDK40** | 94 | 106 | 102,75 | 0,5054 | 103,86 | 0,3906 | 0,6094 | 0,5061 | 12 |
| **YDK41** | 98 | 106 | 103,25 | 0,5054 | 103 | 0,375 | 0,5938 | 0,4993 | 10 |
| **YDK42** | 102 | 108 | 105 | 0,4995 | 103,93 | 0,375 | 0,5781 | 0,5034 | 12 |
| **YDK43** | 96 | 106 | 102 | 0,5024 | 103 | 0,4062 | 0,625 | 0,5068 | 12 |
| **YDK44** | 98 | 106 | 103,75 | 0,5014 | 103,43 | 0,3906 | 0,5938 | 0,4917 | 12 |
| **YDK45** | 96 | 106 | 104 | 0,4991 | 104,07 | 0,3906 | 0,5781 | 0,4871 | 10 |
| **YDK46** | 100 | 106 | 104,25 | 0,5009 | 103,57 | 0,4062 | 0,6406 | 0,5015 | 12 |
| **YDK47** | 96 | 106 | 103,25 | 0,5012 | 102,93 | 0,4062 | 0,6406 | 0,5024 | 12 |
| **YDK48** | 100 | 106 | 103,75 | 0,5027 | 103,93 | 0,3906 | 0,6094 | 0,5 | 12 |
| **YDK49** | 100 | 108 | 104,25 | 0,498 | 103,57 | 0,4219 | 0,5781 | 0,5037 | 10 |
| **YDK50** | 102 | 108 | 104,75 | 0,501 | 103,5 | 0,4062 | 0,5938 | 0,4976 | 12 |
| **YDK51** | 102 | 108 | 104,25 | 0,5031 | 103,21 | 0,4219 | 0,625 | 0,5017 | 12 |
| **YDK52** | 102 | 106 | 104 | 0,4937 | 103,21 | 0,4219 | 0,6094 | 0,5012 | 12 |
| **YDK53** | 96 | 108 | 103,5 | 0,4972 | 104,07 | 0,3906 | 0,5781 | 0,4963 | 10 |
| **YDK54** | 98 | 108 | 104 | 0,4991 | 103,79 | 0,4062 | 0,5781 | 0,4995 | 10 |
| **YDK55** | 102 | 108 | 105,5 | 0,5002 | 103,29 | 0,3906 | 0,625 | 0,5024 | 12 |
| **YDK56** | 100 | 108 | 105 | 0,5002 | 103,29 | 0,4219 | 0,625 | 0,5071 | 10 |
| **YDK57** | 102 | 108 | 104,5 | 0,5043 | 102,93 | 0,4219 | 0,5938 | 0,5024 | 10 |
| **YDK58** | 100 | 108 | 104,5 | 0,501 | 103,29 | 0,375 | 0,625 | 0,5098 | 12 |
| **YDK59** | 98 | 104 | 101,75 | 0,5015 | 104,64 | 0,3906 | 0,6094 | 0,502 | 12 |
| **YDK60** | 100 | 108 | 103 | 0,4976 | 103,86 | 0,4062 | 0,6406 | 0,5022 | 10 |
| **YDK61** | 98 | 108 | 103,25 | 0,4988 | 102,86 | 0,4062 | 0,5938 | 0,5059 | 14 |
| **YDK62** | 100 | 108 | 104,25 | 0,4978 | 102,93 | 0,3906 | 0,6094 | 0,5037 | 12 |
| **YDK63** | 100 | 108 | 104,5 | 0,4913 | 103,64 | 0,4375 | 0,5781 | 0,5007 | 12 |
| **YDK64** | 100 | 108 | 105,5 | 0,502 | 103,71 | 0,3906 | 0,5938 | 0,4973 | 12 |
| **YDK65** | 98 | 108 | 104,75 | 0,5003 | 103,64 | 0,375 | 0,6094 | 0,5054 | 10 |
| **YDK66** | 100 | 110 | 104,75 | 0,4959 | 104 | 0,3906 | 0,5938 | 0,5015 | 12 |
| **YDK67** | 98 | 106 | 103,25 | 0,5029 | 103,57 | 0,4062 | 0,5938 | 0,5 | 12 |
| **YDK68** | 100 | 106 | 104,25 | 0,4996 | 104 | 0,4062 | 0,5938 | 0,4985 | 10 |
| **YDK69** | 102 | 106 | 104,25 | 0,4983 | 104 | 0,4062 | 0,625 | 0,5007 | 12 |
| **YDK70** | 102 | 108 | 104,75 | 0,5008 | 103,71 | 0,4062 | 0,5938 | 0,4983 | 12 |
| **YDK71** | 100 | 108 | 103 | 0,503 | 102,79 | 0,4062 | 0,5781 | 0,501 | 12 |
| **YDK72** | 100 | 106 | 104,25 | 0,4973 | 102,86 | 0,3594 | 0,6406 | 0,4934 | 10 |
| **YDK73** | 100 | 106 | 102,5 | 0,4972 | 103,71 | 0,4062 | 0,6094 | 0,5017 | 12 |
| **YDK74** | 102 | 110 | 105,25 | 0,5003 | 103,5 | 0,4219 | 0,5781 | 0,4937 | 12 |
| **YDK75** | 92 | 108 | 103,25 | 0,498 | 104 | 0,375 | 0,625 | 0,5085 | 14 |
| **YDK76** | 98 | 108 | 104 | 0,5035 | 103,57 | 0,4062 | 0,6094 | 0,5039 | 12 |
| **YDK77** | 104 | 106 | 104,25 | 0,5015 | 102,93 | 0,4219 | 0,6094 | 0,5066 | 12 |



46

**Tablo E2.1.** Orijinal YDK(Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |
| **YDK78** | 94 | 108 | 101 | 0,4978 | 102,93 | 0,3906 | 0,5781 | 0,5032 | 12 |
| **YDK79** | 100 | 106 | 103,25 | 0,4962 | 104 | 0,4062 | 0,5938 | 0,5081 | 12 |
| **YDK80** | 100 | 106 | 103,25 | 0,5006 | 104,14 | 0,3906 | 0,6094 | 0,5061 | 14 |
| **YDK81** | 100 | 108 | 104,5 | 0,4988 | 103,07 | 0,375 | 0,5938 | 0,5 | 12 |
| **YDK82** | 98 | 106 | 102,75 | 0,4999 | 103,64 | 0,4219 | 0,5781 | 0,4932 | 12 |
| **YDK83** | 102 | 108 | 103,75 | 0,4989 | 103,71 | 0,3438 | 0,625 | 0,4912 | 10 |
| **YDK84** | 100 | 106 | 103,5 | 0,4995 | 103,71 | 0,4062 | 0,6406 | 0,501 | 10 |
| **YDK85** | 96 | 106 | 103 | 0,4983 | 103,79 | 0,3906 | 0,6094 | 0,4998 | 12 |
| **YDK86** | 100 | 106 | 103,25 | 0,4971 | 103,86 | 0,4219 | 0,6562 | 0,5037 | 10 |
| **YDK87** | 100 | 108 | 104,75 | 0,5025 | 103,14 | 0,3906 | 0,6094 | 0,5012 | 12 |
| **YDK88** | 98 | 106 | 103,5 | 0,5011 | 104,14 | 0,4062 | 0,5938 | 0,51 | 14 |
| **YDK89** | 100 | 108 | 103,75 | 0,499 | 103,93 | 0,4219 | 0,5781 | 0,4988 | 10 |
| **YDK90** | 94 | 106 | 102,5 | 0,501 | 103,14 | 0,3906 | 0,5938 | 0,5027 | 10 |
| **YDK91** | 100 | 104 | 102,5 | 0,4969 | 103,21 | 0,4062 | 0,6094 | 0,5027 | 12 |
| **YDK92** | 102 | 106 | 104 | 0,4994 | 103,07 | 0,4219 | 0,6094 | 0,5022 | 10 |
| **YDK93** | 100 | 106 | 103,5 | 0,4981 | 103,43 | 0,3906 | 0,625 | 0,5007 | 12 |
| **YDK94** | 94 | 108 | 103 | 0,4956 | 103,36 | 0,4062 | 0,5781 | 0,5022 | 10 |
| **YDK95** | 100 | 106 | 102,75 | 0,5023 | 103,5 | 0,4062 | 0,5625 | 0,4937 | 10 |
| **YDK96** | 100 | 108 | 103,25 | 0,497 | 102,93 | 0,4062 | 0,5781 | 0,4905 | 12 |
| **YDK97** | 96 | 106 | 101,75 | 0,5015 | 102,71 | 0,375 | 0,5625 | 0,4929 | 12 |
| **YDK98** | 102 | 108 | 105,75 | 0,5023 | 103,93 | 0,3906 | 0,625 | 0,5 | 12 |
| **YDK99** | 100 | 106 | 103 | 0,5001 | 103,36 | 0,3906 | 0,5938 | 0,4949 | 12 |
| **YDK100** | 100 | 106 | 104 | 0,5012 | 103,71 | 0,4062 | 0,625 | 0,5063 | 12 |
| **YDK101** | 102 | 108 | 104,75 | 0,4987 | 102,93 | 0,4062 | 0,5781 | 0,4971 | 10 |
| **YDK102** | 98 | 106 | 104,25 | 0,5008 | 102,79 | 0,4219 | 0,6094 | 0,5046 | 10 |
| **YDK103** | 98 | 106 | 102,75 | 0,5024 | 104,36 | 0,4062 | 0,5938 | 0,4958 | 10 |
| **YDK104** | 104 | 106 | 104,75 | 0,5017 | 103,21 | 0,375 | 0,5781 | 0,491 | 10 |
| **YDK105** | 98 | 106 | 103 | 0,4939 | 104,07 | 0,4219 | 0,6094 | 0,4976 | 10 |
| **YDK106** | 96 | 104 | 101,25 | 0,5008 | 103,21 | 0,4219 | 0,5781 | 0,4993 | 12 |
| **YDK107** | 98 | 108 | 105 | 0,4969 | 103,86 | 0,3906 | 0,6094 | 0,4973 | 12 |
| **YDK108** | 100 | 108 | 104,75 | 0,4988 | 103,21 | 0,4219 | 0,6406 | 0,5068 | 12 |
| **YDK109** | 98 | 106 | 103,75 | 0,4996 | 104,57 | 0,4062 | 0,5938 | 0,5005 | 12 |
| **YDK110** | 96 | 108 | 101,75 | 0,4934 | 103,29 | 0,3594 | 0,625 | 0,4905 | 12 |
| **YDK111** | 100 | 110 | 104,75 | 0,505 | 103,29 | 0,4219 | 0,6094 | 0,5015 | 10 |
| **YDK112** | 102 | 106 | 104 | 0,4998 | 103,5 | 0,4219 | 0,5938 | 0,5044 | 10 |
| **YDK113** | 100 | 106 | 103,5 | 0,4995 | 104,5 | 0,4062 | 0,5781 | 0,4976 | 12 |
| **YDK114** | 100 | 108 | 103,5 | 0,5031 | 103,43 | 0,4062 | 0,5938 | 0,5005 | 12 |
| **YDK115** | 104 | 106 | 104,75 | 0,4973 | 103,71 | 0,4062 | 0,5938 | 0,4998 | 12 |
| **YDK116** | 102 | 108 | 105 | 0,4982 | 103,93 | 0,4062 | 0,625 | 0,498 | 12 |
| **YDK117** | 102 | 106 | 104,5 | 0,4989 | 104,36 | 0,375 | 0,6094 | 0,4951 | 14 |



47

**Tablo E2.1.** Orijinal YDK(Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |
| **YDK118** | 102 | 108 | 105,25 | 0,502 | 102,64 | 0,3594 | 0,5781 | 0,4958 | 12 |
| **YDK119** | 98 | 106 | 102,5 | 0,5048 | 103,36 | 0,3906 | 0,5938 | 0,4912 | 12 |
| **YDK120** | 100 | 106 | 103,75 | 0,5 | 103,5 | 0,4062 | 0,5938 | 0,5127 | 10 |
| **YDK121** | 100 | 106 | 103,5 | 0,501 | 104,14 | 0,4062 | 0,6094 | 0,5122 | 10 |
| **YDK122** | 102 | 108 | 105 | 0,4962 | 104,29 | 0,4062 | 0,5938 | 0,5037 | 10 |
| **YDK123** | 98 | 106 | 102,75 | 0,4932 | 103,29 | 0,375 | 0,6719 | 0,5042 | 14 |
| **YDK124** | 98 | 106 | 103 | 0,5018 | 104,21 | 0,4375 | 0,625 | 0,5071 | 12 |
| **YDK125** | 98 | 106 | 103,75 | 0,4947 | 103,79 | 0,4062 | 0,6094 | 0,4946 | 12 |
| **YDK126** | 102 | 106 | 104 | 0,5033 | 103,57 | 0,4219 | 0,625 | 0,5059 | 12 |
| **YDK127** | 100 | 106 | 103,25 | 0,5037 | 103,86 | 0,4062 | 0,5781 | 0,5059 | 12 |
| **YDK128** | 98 | 108 | 104,5 | 0,4988 | 103,57 | 0,3906 | 0,6094 | 0,502 | 12 |
| **YDK129** | 98 | 108 | 104,25 | 0,5008 | 104,14 | 0,4062 | 0,6094 | 0,4998 | 10 |
| **YDK130** | 100 | 106 | 102,5 | 0,4999 | 103,43 | 0,4219 | 0,6406 | 0,5186 | 12 |
| **YDK131** | 98 | 108 | 103 | 0,4995 | 104,07 | 0,4062 | 0,6094 | 0,5149 | 12 |
| **YDK132** | 102 | 108 | 104 | 0,4992 | 103,64 | 0,4062 | 0,6094 | 0,5066 | 10 |
| **YDK133** | 102 | 108 | 104,75 | 0,4998 | 103,71 | 0,3906 | 0,625 | 0,5063 | 12 |
| **YDK134** | 100 | 108 | 104 | 0,4956 | 104,07 | 0,4062 | 0,6094 | 0,4985 | 10 |
| **YDK135** | 98 | 108 | 103,25 | 0,504 | 102 | 0,375 | 0,5781 | 0,4983 | 12 |
| **YDK136** | 98 | 108 | 102,75 | 0,5022 | 103,64 | 0,4062 | 0,5781 | 0,5068 | 10 |
| **YDK137** | 96 | 106 | 102,5 | 0,5038 | 103,86 | 0,3906 | 0,6094 | 0,5073 | 12 |
| **YDK138** | 100 | 108 | 103 | 0,504 | 104,29 | 0,3906 | 0,6094 | 0,501 | 12 |
| **YDK139** | 100 | 108 | 104,25 | 0,4957 | 104 | 0,4062 | 0,6406 | 0,5024 | 10 |
| **YDK140** | 100 | 108 | 104,25 | 0,499 | 103,29 | 0,3906 | 0,5938 | 0,499 | 10 |
| **YDK141** | 98 | 108 | 102,5 | 0,5049 | 104,64 | 0,375 | 0,6094 | 0,4951 | 12 |
| **YDK142** | 98 | 106 | 103,5 | 0,5007 | 104,07 | 0,3594 | 0,5938 | 0,4995 | 12 |
| **YDK143** | 98 | 106 | 103,25 | 0,5056 | 104 | 0,3594 | 0,5938 | 0,4893 | 10 |
| **YDK144** | 100 | 106 | 103,25 | 0,5046 | 103,5 | 0,4219 | 0,5938 | 0,4973 | 10 |
| **YDK145** | 100 | 106 | 103 | 0,4966 | 103,93 | 0,4062 | 0,6094 | 0,4956 | 12 |
| **YDK146** | 100 | 108 | 103,5 | 0,4983 | 103 | 0,4219 | 0,6406 | 0,5042 | 12 |
| **YDK147** | 96 | 104 | 102,5 | 0,4954 | 103,86 | 0,4062 | 0,6094 | 0,4956 | 14 |
| **YDK148** | 102 | 106 | 104,75 | 0,5014 | 103,71 | 0,3906 | 0,5938 | 0,4968 | 12 |
| **YDK149** | 94 | 106 | 102,5 | 0,5033 | 103,57 | 0,3906 | 0,5781 | 0,5024 | 12 |
| **YDK150** | 98 | 108 | 103 | 0,5006 | 104,36 | 0,3906 | 0,625 | 0,5044 | 10 |
| **YDK151** | 98 | 108 | 104.25 | 0,5033 | 103,57 | 0,4219 | 0,5938 | 0.4946 | 12 |
| **YDK152** | 96 | 108 | 103 | 0,5044 | 103 | 0,375 | 0,5781 | 0,4929 | 12 |
| **YDK153** | 102 | 108 | 104,25 | 0,4983 | 102,64 | 0,3906 | 0,5938 | 0,4963 | 12 |
| **YDK154** | 100 | 106 | 103,25 | 0,4987 | 104,29 | 0,375 | 0,6094 | 0,4961 | 12 |
| **YDK155** | 98 | 108 | 104,25 | 0,5004 | 103,86 | 0,3906 | 0,5781 | 0,4944 | 10 |
| **YDK156** | 100 | 106 | 104 | 0,4988 | 103,71 | 0,4062 | 0,6094 | 0,5049 | 10 |
| **YDK157** | 104 | 106 | 104,5 | 0,5002 | 102,79 | 0,3906 | 0,625 | 0,5095 | 10 |



48

**Tablo E2.1.** Orijinal YDK(Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |
| **YDK158** | 100 | 108 | 104,25 | 0,4988 | 103,14 | 0,3906 | 0,6406 | 0,5088 | 12 |
| **YDK159** | 100 | 108 | 104,25 | 0,4939 | 103,93 | 0,4062 | 0,5938 | 0,5024 | 14 |
| **YDK160** | 98 | 108 | 103,25 | 0,4979 | 103,93 | 0,4062 | 0,5938 | 0,5012 | 12 |
| **YDK161** | 100 | 106 | 104 | 0,4987 | 103,93 | 0,3906 | 0,5938 | 0,4939 | 14 |
| **YDK162** | 100 | 106 | 103,5 | 0,5003 | 104 | 0,4219 | 0,6094 | 0,5015 | 10 |
| **YDK163** | 94 | 106 | 100,75 | 0,5003 | 103,71 | 0,4219 | 0,6094 | 0,5034 | 12 |
| **YDK164** | 98 | 108 | 103,5 | 0,4973 | 103,43 | 0,4219 | 0,6094 | 0,5059 | 12 |
| **YDK165** | 98 | 106 | 103 | 0,5041 | 103,86 | 0,4062 | 0,6094 | 0,498 | 12 |
| **YDK166** | 96 | 106 | 102,5 | 0,4963 | 104,43 | 0,3906 | 0,5938 | 0,4927 | 10 |
| **YDK167** | 94 | 104 | 100,5 | 0,5005 | 102,93 | 0,4062 | 0,6406 | 0,501 | 12 |
| **YDK168** | 102 | 108 | 105 | 0,4978 | 103,57 | 0,3906 | 0,6094 | 0,5002 | 10 |
| **YDK169** | 100 | 106 | 103,5 | 0,4931 | 103,79 | 0,3594 | 0,5938 | 0,4893 | 12 |
| **YDK170** | 100 | 110 | 104,25 | 0,4937 | 103,43 | 0,4062 | 0,6094 | 0,4966 | 10 |
| **YDK171** | 98 | 106 | 103,75 | 0,5014 | 103,93 | 0,4062 | 0,625 | 0,4995 | 12 |
| **YDK172** | 100 | 108 | 104,25 | 0,4982 | 104,36 | 0,3906 | 0,6406 | 0,5066 | 12 |
| **YDK173** | 98 | 108 | 104,25 | 0,4994 | 103,57 | 0,4062 | 0,5781 | 0,5059 | 12 |
| **YDK174** | 96 | 106 | 102,5 | 0,5015 | 102,21 | 0,4062 | 0,5938 | 0,4983 | 12 |
| **YDK175** | 102 | 108 | 104,25 | 0,4969 | 103,21 | 0,3906 | 0,6406 | 0,5085 | 12 |
| **YDK176** | 100 | 108 | 104,75 | 0,4969 | 103.21 | 0,4219 | 0,6094 | 0,4951 | 10 |
| **YDK177** | 98 | 108 | 105 | 0,4983 | 101,93 | 0,3906 | 0,6094 | 0,4949 | 10 |
| **YDK178** | 102 | 108 | 105 | 0,4999 | 104,21 | 0,4219 | 0,5781 | 0,5054 | 10 |
| **YDK179** | 100 | 108 | 103 | 0,5036 | 104,29 | 0,4219 | 0,5938 | 0,5037 | 10 |
| **YDK180** | 100 | 106 | 103 | 0,501 | 104,79 | 0,4062 | 0,5781 | 0,4985 | 10 |
| **YDK181** | 100 | 108 | 104 | 0,4995 | 103,29 | 0,4219 | 0,5938 | 0,5039 | 10 |
| **YDK182** | 102 | 108 | 104,75 | 0,499 | 103,29 | 0,3906 | 0,6094 | 0,5 | 12 |
| **YDK183** | 96 | 108 | 102 | 0,5022 | 103,79 | 0,3906 | 0,6562 | 0,5068 | 12 |
| **YDK184** | 100 | 108 | 104,5 | 0,4953 | 102,5 | 0,4062 | 0,6094 | 0,5024 | 12 |
| **YDK185** | 102 | 106 | 104 | 0,4985 | 103,93 | 0,375 | 0,6094 | 0,5 | 12 |
| **YDK186** | 102 | 106 | 103,75 | 0,4992 | 103,21 | 0,375 | 0,5938 | 0,5027 | 10 |
| **YDK187** | 102 | 106 | 104,25 | 0,501 | 104,14 | 0,4062 | 0,6094 | 0,5063 | 12 |
| **YDK188** | 102 | 106 | 104,75 | 0,4995 | 103,71 | 0,4062 | 0,6094 | 0,5066 | 12 |
| **YDK189** | 96 | 106 | 101,5 | 0,5011 | 103,57 | 0,3906 | 0,6094 | 0,4973 | 10 |
| **YDK190** | 98 | 108 | 103,75 | 0,5008 | 103,5 | 0,375 | 0,625 | 0,4937 | 12 |
| **YDK191** | 100 | 108 | 103,25 | 0,4961 | 103,57 | 0,4062 | 0,6094 | 0,5051 | 10 |
| **YDK192** | 98 | 108 | 103,75 | 0,4964 | 103,64 | 0,4375 | 0,6406 | 0,5042 | 10 |
| **YDK193** | 96 | 110 | 103 | 0,4983 | 102,57 | 0,4219 | 0,5938 | 0,5002 | 12 |
| **YDK194** | 98 | 108 | 103,75 | 0,4985 | 104,21 | 0,4062 | 0,6094 | 0,502 | 14 |
| **YDK195** | 98 | 108 | 104,25 | 0,4953 | 103 | 0,4062 | 0,625 | 0,5071 | 10 |
| **YDK196** | 100 | 108 | 105 | 0,5 | 103,64 | 0,4531 | 0,5938 | 0,5059 | 12 |
| **YDK197** | 98 | 108 | 103,25 | 0,5055 | 103,57 | 0,375 | 0,5781 | 0,5046 | 10 |



49

**Tablo E2.1.** Orijinal YDK(Devamı)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** | **I/O XOR** |
|  |  |  |  |  |  |  |  |  |  |  |
|  | **YDK198** | 102 | 106 | 103,25 | 0,5033 | 104,14 | 0,3906 | 0,625 | 0,5063 | 12 |
|  | **YDK199** | 98 | 106 | 102,75 | 0,4989 | 102,93 | 0,4062 | 0,5781 | 0,4985 | 10 |
|  | **YDK200** | 100 | 108 | 105,25 | 0,4999 | 103,36 | 0,4062 | 0,6094 | 0,5002 | 10 |
|  | **YDK201** | 102 | 106 | 104 | 0,4953 | 102,93 | 0,4219 | 0,5938 | 0,502 | 10 |
|  | **YDK202** | 98 | 108 | 104,75 | 0,5031 | 103,93 | 0,375 | 0,5781 | 0,498 | 12 |
|  | **YDK203** | 98 | 106 | 102,75 | 0,4985 | 103,57 | 0,3906 | 0,6406 | 0,4993 | 10 |
|  | **YDK204** | 96 | 106 | 102,75 | 0,5013 | 103,93 | 0,3906 | 0,6094 | 0,5032 | 10 |
|  | **YDK205** | 100 | 108 | 103,75 | 0,5029 | 103,36 | 0,4062 | 0,6094 | 0,511 | 10 |
|  | **YDK206** | 102 | 106 | 104,25 | 0,4997 | 103,29 | 0,3906 | 0,5938 | 0,4978 | 12 |
|  | **YDK207** | 96 | 106 | 101 | 0,4959 | 103,14 | 0,375 | 0,5938 | 0,5063 | 12 |
|  | **YDK208** | 98 | 106 | 102,25 | 0,5033 | 102,71 | 0,4062 | 0,6094 | 0,5027 | 10 |
|  | **YDK209** | 94 | 106 | 101,75 | 0,5008 | 103,93 | 0,4219 | 0,625 | 0,5005 | 10 |
|  | **YDK210** | 102 | 108 | 105 | 0,4962 | 103,5 | 0,375 | 0,5781 | 0,4998 | 10 |
|  | **YDK211** | 98 | 106 | 103,5 | 0,5025 | 103,86 | 0,375 | 0,5781 | 0,4993 | 12 |
|  | **YDK212** | 92 | 106 | 101 | 0,5007 | 103,5 | 0,3906 | 0,6094 | 0,5034 | 12 |
|  | **YDK213** | 100 | 108 | 103,5 | 0,5031 | 103,93 | 0,3906 | 0,5938 | 0,5007 | 14 |
|  | **YDK214** | 100 | 106 | 103,5 | 0,4983 | 103,93 | 0,4062 | 0,5938 | 0,4968 | 10 |
|  | **YDK215** | 100 | 108 | 103,5 | 0,5007 | 104,07 | 0,4219 | 0,5938 | 0,5066 | 12 |
|  | **YDK216** | 96 | 108 | 102,5 | 0,5004 | 103,64 | 0,4062 | 0,6094 | 0,4976 | 10 |
|  | **YDK217** | 96 | 106 | 101,25 | 0,5012 | 104,57 | 0,3438 | 0,6562 | 0,511 | 12 |
|  | **YDK218** | 100 | 106 | 103 | 0,4986 | 103,64 | 0,4062 | 0,6094 | 0,5066 | 12 |
|  | **YDK219** | 96 | 106 | 102,25 | 0,5006 | 103,36 | 0,4219 | 0,5938 | 0,5 | 10 |
|  |  |  |  |  |  |  |  |  |  |  |



50

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **EK- 3:** | **DEĞİŞEN YDK TABLOSU** | | | | |  |  |  |  |  |
|  |  |  |  | **Tablo E3.1.** Değişen YDK (Devamı) | | | |  |  |  |
|  |  |  |  | |  | |  | | |  |
| **YDK** |  |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  |  |  |  |  |  | **I/O XOR** |
|  |  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** |
|  |  | |  |  |  |  |  |  |  |  |
| **YDK\_1** | 98 | | 108 | 103 | 0,5015 | 102,93 | 0,3906 | 0,6562 | 0,5005 | 12 |
| **YDK\_2** | 98 | | 106 | 103,25 | 0,5049 | 102,64 | 0,3906 | 0,5938 | 0,5024 | 10 |
| **YDK\_3** | 100 | | 106 | 102,75 | 0,4994 | 103 | 0,3906 | 0,6094 | 0,502 | 12 |
| **YDK\_4** | 100 | | 106 | 102,75 | 0,4983 | 103,5 | 0,4062 | 0,625 | 0,491 | 14 |
| **YDK\_5** | 98 | | 108 | 103,5 | 0,4998 | 104,36 | 0,4219 | 0,6094 | 0,5046 | 10 |
| **YDK\_6** | 100 | | 108 | 104 | 0,5006 | 102,5 | 0,4062 | 0,5938 | 0,4993 | 12 |
| **YDK\_7** | 100 | | 108 | 104,75 | 0,5022 | 102,71 | 0,3594 | 0,6406 | 0,5042 | 12 |
| **YDK\_8** | 100 | | 106 | 103 | 0,5008 | 103,86 | 0,4062 | 0,6094 | 0,499 | 12 |
| **YDK\_9** | 98 | | 108 | 103,25 | 0,493 | 103,93 | 0,4062 | 0,6562 | 0,5002 | 12 |
| **YDK\_10** | 96 | | 108 | 103,5 | 0,5026 | 104,14 | 0,3906 | 0,6094 | 0,4851 | 12 |
| **YDK\_11** | 98 | | 106 | 102,25 | 0,5001 | 103,64 | 0,3906 | 0,625 | 0,501 | 12 |
| **YDK\_12** | 96 | | 108 | 102 | 0,4982 | 103,21 | 0,3906 | 0,6094 | 0,4978 | 14 |
| **YDK\_13** | 100 | | 108 | 104,25 | 0,5011 | 102,93 | 0,3906 | 0,6094 | 0,501 | 10 |
| **YDK\_14** | 100 | | 106 | 104 | 0,4978 | 103,71 | 0,3906 | 0,6094 | 0,4995 | 10 |
| **YDK\_15** | 102 | | 106 | 103,25 | 0,495 | 103,14 | 0,375 | 0,6094 | 0,5002 | 12 |
| **YDK\_16** | 100 | | 106 | 103 | 0,4992 | 102 | 0,375 | 0,5781 | 0,4976 | 12 |
| **YDK\_17** | 98 | | 104 | 102,75 | 0,4996 | 103,14 | 0,4062 | 0,625 | 0,5125 | 10 |
| **YDK\_18** | 96 | | 108 | 102,75 | 0,5008 | 103,93 | 0,4375 | 0,625 | 0,5046 | 10 |
| **YDK\_19** | 100 | | 108 | 104,25 | 0,4976 | 104 | 0,3594 | 0,6406 | 0,5032 | 10 |
| **YDK\_20** | 100 | | 106 | 103,25 | 0,4975 | 103,71 | 0,4062 | 0,5938 | 0,488 | 10 |
| **YDK\_21** | 98 | | 108 | 103,75 | 0,4966 | 103,5 | 0,4062 | 0,5938 | 0,5051 | 10 |
| **YDK\_22** | 98 | | 108 | 104,25 | 0,4974 | 103,36 | 0,4219 | 0,5938 | 0,4985 | 12 |
| **YDK\_23** | 102 | | 110 | 105,75 | 0,4972 | 103,93 | 0,3906 | 0,5781 | 0,5073 | 10 |
| **YDK\_24** | 96 | | 108 | 103 | 0,5001 | 104,86 | 0,4062 | 0,5938 | 0,5098 | 16 |
| **YDK\_25** | 100 | | 108 | 103,75 | 0,4979 | 103,93 | 0,375 | 0,5938 | 0,4988 | 10 |
| **YDK\_26** | 96 | | 108 | 102,5 | 0,5033 | 104,07 | 0,4219 | 0,6406 | 0,5044 | 10 |
| **YDK\_27** | 98 | | 108 | 102,5 | 0,5046 | 102,93 | 0,4219 | 0,6094 | 0,51 | 14 |
| **YDK\_28** | 102 | | 108 | 104,5 | 0,5062 | 103,64 | 0,4219 | 0,5938 | 0,499 | 10 |
| **YDK\_29** | 98 | | 106 | 103 | 0,4967 | 104,14 | 0,3594 | 0,5938 | 0,4976 | 10 |
| **YDK\_30** | 100 | | 108 | 105 | 0,4974 | 104,79 | 0,3906 | 0,625 | 0,5042 | 12 |
| **YDK\_31** | 102 | | 108 | 105 | 0,5 | 102,64 | 0,4219 | 0,5938 | 0,4941 | 12 |
| **YDK\_32** | 92 | | 108 | 103,75 | 0,5022 | 104,36 | 0,3906 | 0,5938 | 0,4985 | 10 |
| **YDK\_33** | 96 | | 104 | 101,5 | 0,5005 | 103,5 | 0,375 | 0,6094 | 0,5015 | 10 |
| **YDK\_34** | 100 | | 110 | 105,25 | 0,5027 | 102,43 | 0,4062 | 0,5781 | 0,4995 | 14 |
| **YDK\_35** | 98 | | 108 | 103,25 | 0,5025 | 101,79 | 0,3906 | 0,6094 | 0,5081 | 10 |
| **YDK\_36** | 96 | | 106 | 103 | 0,4967 | 103,43 | 0,4062 | 0,5781 | 0,5012 | 10 |
| **YDK\_37** | 96 | | 106 | 103,25 | 0,5008 | 102 | 04219 | 0,5781 | 0,5012 | 12 |



51

**Tablo E3.1.** Değişen YDK (Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  |  |  |  |  | **I/O XOR** |
|  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** |
|  |  |  |  |  |  |  |  |  |  |
| **YDK\_38** | 96 | 106 | 102,75 | 0,4936 | 102,79 | 0,3906 | 0,5938 | 0,4939 | 10 |
| **YDK\_39** | 98 | 108 | 102,75 | 0,4978 | 103,36 | 0,375 | 0,625 | 0,5007 | 10 |
| **YDK\_40** | 98 | 104 | 102,5 | 0,5 | 103,43 | 0,3906 | 0,5938 | 0,5085 | 12 |
| **YDK\_41** | 98 | 110 | 103,25 | 0,4974 | 103,07 | 0,4219 | 0,5938 | 0,5115 | 10 |
| **YDK\_42** | 98 | 108 | 103,5 | 0,4994 | 103,86 | 0,4062 | 0,6094 | 0,5024 | 12 |
| **YDK\_43** | 98 | 108 | 103,75 | 0,4954 | 104,36 | 0,4219 | 0,5938 | 0,5073 | 10 |
| **YDK\_44** | 104 | 106 | 104,5 | 0,4977 | 103,57 | 0,4062 | 0,5938 | 0,5 | 12 |
| **YDK\_45** | 100 | 106 | 103,5 | 0,4994 | 104,07 | 0,375 | 0,5938 | 0,4973 | 12 |
| **YDK\_46** | 100 | 106 | 103,5 | 0,4964 | 103,36 | 0,4219 | 0,6094 | 0,5051 | 12 |
| **YDK\_47** | 98 | 108 | 104 | 0,4983 | 103,57 | 0,4219 | 0,6094 | 0,5083 | 14 |
| **YDK\_48** | 98 | 104 | 102,75 | 0,4993 | 103,86 | 0,3594 | 0,625 | 0,5024 | 12 |
| **YDK\_49** | 100 | 106 | 103,25 | 0,5043 | 103,93 | 0,375 | 0,6406 | 0,5066 | 12 |
| **YDK\_50** | 98 | 106 | 103,25 | 0,5012 | 103,5 | 0,4062 | 0,5938 | 0,5012 | 12 |
| **YDK\_51** | 100 | 106 | 103,75 | 0,4982 | 103,43 | 0,4062 | 0,6094 | 0,5012 | 10 |
| **YDK\_52** | 100 | 108 | 103,5 | 0,4965 | 103,71 | 0,4062 | 0,5938 | 0,51 | 12 |
| **YDK\_53** | 102 | 108 | 105 | 0,503 | 104 | 0,3594 | 0,5938 | 0,5078 | 12 |
| **YDK\_54** | 104 | 108 | 105,5 | 0,5026 | 102,93 | 0,3906 | 0,5938 | 0,5054 | 10 |
| **YDK\_55** | 98 | 108 | 103,75 | 0,4981 | 103,64 | 0,3906 | 0,6562 | 0,4983 | 12 |
| **YDK\_56** | 98 | 106 | 104,25 | 0,4975 | 103,93 | 0,4219 | 0,6094 | 0,499 | 12 |
| **YDK\_57** | 100 | 106 | 103,5 | 0,5031 | 104,29 | 0,4219 | 0,5781 | 0,4927 | 12 |
| **YDK\_58** | 102 | 108 | 105,25 | 0,4971 | 103,21 | 0,4219 | 0,6094 | 0,5 | 10 |
| **YDK\_59** | 100 | 106 | 103,5 | 0,5015 | 103,36 | 0,4062 | 0,5938 | 0,4966 | 10 |
| **YDK\_60** | 100 | 108 | 105 | 0,4994 | 103,43 | 0,4219 | 0,5938 | 0,5005 | 12 |
| **YDK\_61** | 100 | 106 | 103 | 0,4974 | 104,21 | 0,4062 | 0,5938 | 0,4971 | 12 |
| **YDK\_62** | 96 | 108 | 104,75 | 0,5023 | 103,5 | 0,4062 | 0,5781 | 0,4985 | 12 |
| **YDK\_63** | 94 | 106 | 101,5 | 0,5001 | 103,64 | 0,4062 | 0,6094 | 0,5 | 10 |
| **YDK\_64** | 88 | 106 | 100,25 | 0,4968 | 103,36 | 0,3906 | 0,6094 | 0,4995 | 10 |
| **YDK\_65** | 100 | 108 | 104,75 | 0,4978 | 103,36 | 0,3906 | 0,6094 | 0,4958 | 10 |
| **YDK\_66** | 100 | 106 | 102,75 | 0,4998 | 103,07 | 0,4062 | 0,625 | 0,4976 | 10 |
| **YDK\_67** | 102 | 106 | 104 | 0,4923 | 102,86 | 0,4062 | 0,6094 | 0,4993 | 10 |
| **YDK\_68** | 104 | 108 | 105,25 | 0,5007 | 103,21 | 0,4219 | 0,5938 | 0,51 | 12 |
| **YDK\_69** | 100 | 108 | 104 | 0,4982 | 104,21 | 0,4062 | 0,6094 | 0,5024 | 10 |
| **YDK\_70** | 100 | 106 | 103 | 0,4955 | 104,14 | 0,3906 | 0,5938 | 0,4988 | 12 |
| **YDK\_71** | 100 | 108 | 105,75 | 0,4995 | 104,79 | 0,4062 | 0,6094 | 0,488 | 10 |
| **YDK\_72** | 94 | 106 | 102,5 | 0,5052 | 103,71 | 0,3906 | 0,6094 | 0,4915 | 10 |
| **YDK\_73** | 100 | 106 | 103 | 0,5015 | 103,64 | 0,3906 | 0,5938 | 0,4912 | 12 |
| **YDK\_74** | 100 | 106 | 103 | 0,4964 | 103,21 | 0,3906 | 0,625 | 0,4937 | 10 |
| **YDK\_75** | 98 | 106 | 101,5 | 0,5017 | 103,14 | 0,375 | 0,6094 | 0,5007 | 12 |
| **YDK\_76** | 98 | 106 | 103 | 0,4987 | 103,14 | 0,3906 | 0,625 | 0,499 | 12 |
| **YDK\_77** | 102 | 106 | 104 | 0,4973 | 103 | 0,375 | 0,5938 | 0,5002 | 12 |



52

**Tablo E3.1.** Değişen YDK (Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  |  |  |  |  | **I/O XOR** |
|  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** |
|  |  |  |  |  |  |  |  |  |  |
| **YDK\_78** | 98 | 104 | 102 | 0,5008 | 102,5 | 0,3906 | 0,625 | 0,5137 | 10 |
| **YDK\_79** | 98 | 106 | 102,5 | 0,496 | 103,79 | 0,375 | 0,6094 | 0,5044 | 14 |
| **YDK\_80** | 98 | 108 | 103 | 0,4969 | 103,57 | 0,4062 | 0,6562 | 0,5005 | 12 |
| **YDK\_81** | 100 | 108 | 103,25 | 0,4999 | 103,86 | 0,3906 | 0,6094 | 0,5034 | 12 |
| **YDK\_82** | 92 | 106 | 102,5 | 0,4967 | 103,64 | 0,3281 | 0,5938 | 0,4922 | 12 |
| **YDK\_83** | 100 | 108 | 103 | 0,4992 | 104,64 | 0,375 | 0,5938 | 0,502 | 10 |
| **YDK\_84** | 98 | 106 | 102,75 | 0,4979 | 103,21 | 0,4219 | 0,5781 | 0,5046 | 10 |
| **YDK\_85** | 100 | 106 | 104,25 | 0,4969 | 104,36 | 0,4062 | 0,5938 | 0,5063 | 10 |
| **YDK\_86** | 98 | 106 | 102,75 | 0,4955 | 103,86 | 0,3594 | 0,625 | 0,5037 | 12 |
| **YDK\_87** | 100 | 104 | 103 | 0,499 | 103,36 | 0,4062 | 0,5938 | 0,5085 | 12 |
| **YDK\_88** | 98 | 106 | 101,25 | 0,4934 | 102,76 | 0,375 | 0,625 | 0,5054 | 10 |
| **YDK\_89** | 96 | 108 | 103,5 | 0,5005 | 103,71 | 0,4062 | 0,625 | 0,5093 | 12 |
| **YDK\_90** | 98 | 108 | 102,5 | 0,4989 | 102,36 | 0,375 | 0,5938 | 0,4971 | 10 |
| **YDK\_91** | 104 | 106 | 104,75 | 0,4953 | 102,86 | 0,375 | 0,625 | 0,4902 | 12 |
| **YDK\_92** | 96 | 106 | 102,75 | 0,4959 | 103,07 | 0,3594 | 0,5938 | 0,501 | 12 |
| **YDK\_93** | 102 | 108 | 104,75 | 0,5004 | 103,5 | 0,4062 | 0,5781 | 0,5007 | 10 |
| **YDK\_94** | 98 | 108 | 104 | 0,4987 | 103,79 | 0,4062 | 0,625 | 0,5024 | 10 |
| **YDK\_95** | 102 | 106 | 104,5 | 0,5061 | 103 | 0,3594 | 0,6562 | 0,502 | 10 |
| **YDK\_96** | 100 | 104 | 101,75 | 0,4958 | 103,64 | 0,4062 | 0,6562 | 0,5032 | 12 |
| **YDK\_97** | 98 | 108 | 104 | 0,497 | 102,93 | 0,4062 | 0,5938 | 0,498 | 14 |
| **YDK\_98** | 98 | 108 | 104,5 | 0,499 | 102,71 | 0,3906 | 0,6094 | 0,4905 | 12 |
| **YDK\_99** | 100 | 108 | 104,25 | 0,4988 | 102,79 | 0,4062 | 0,5781 | 0,4946 | 12 |
| **YDK\_100** | 100 | 106 | 103,25 | 0,496 | 103,79 | 0,4062 | 0,5781 | 0,5017 | 12 |
| **YDK\_101** | 100 | 106 | 103,25 | 0,4981 | 103,64 | 0,4219 | 0,5938 | 0,4927 | 12 |
| **YDK\_102** | 98 | 104 | 101 | 0,4956 | 103,93 | 0,375 | 0,5938 | 0,5037 | 14 |
| **YDK\_103** | 100 | 106 | 102,75 | 0,4971 | 104,14 | 0,375 | 0,625 | 0,502 | 10 |
| **YDK\_104** | 98 | 108 | 103,5 | 0,5011 | 103,64 | 0,4219 | 0,5938 | 0,4985 | 10 |
| **YDK\_105** | 98 | 106 | 102,25 | 0,5059 | 103,79 | 0,3906 | 0,5938 | 0,5002 | 10 |
| **YDK\_106** | 100 | 108 | 104 | 0,5054 | 103,5 | 0,4062 | 0,6094 | 0,4985 | 12 |
| **YDK\_107** | 96 | 106 | 101,75 | 0,4955 | 103,93 | 0,4219 | 0,6094 | 0,5054 | 12 |
| **YDK\_108** | 98 | 106 | 103 | 0,5 | 104 | 0,3906 | 0,5781 | 0,4978 | 10 |
| **YDK\_109** | 98 | 106 | 102,75 | 0,5006 | 103,43 | 0,4062 | 0,6406 | 0,5063 | 10 |
| **YDK\_110** | 102 | 108 | 105 | 0,5038 | 103,36 | 0,4062 | 0,5938 | 0,4922 | 14 |
| **YDK\_111** | 100 | 104 | 103 | 0,5025 | 103,71 | 0,4062 | 0,6562 | 0,4956 | 12 |
| **YDK\_112** | 90 | 108 | 102,25 | 0,4974 | 103,79 | 0,375 | 0,5938 | 0,5005 | 12 |
| **YDK\_113** | 100 | 108 | 102,75 | 0,4978 | 103,86 | 0,4062 | 0,5938 | 0,5015 | 12 |
| **YDK\_114** | 100 | 108 | 104 | 0,504 | 102,93 | 0,4062 | 0,625 | 0,5027 | 12 |
| **YDK\_115** | 100 | 106 | 103,25 | 0,5048 | 102,71 | 0,375 | 0,5781 | 0,498 | 10 |
| **YDK\_116** | 102 | 108 | 104,5 | 0,498 | 104,36 | 0,4375 | 0,5938 | 0,5017 | 12 |
| **YDK\_117** | 100 | 108 | 104,5 | 0,505 | 103,14 | 0,4219 | 0,5938 | 0,4985 | 12 |



53

**Tablo E3.1.** Değişen YDK (Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  |  |  |  |  | **I/O XOR** |
|  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** |
|  |  |  |  |  |  |  |  |  |  |
| **YDK\_118** | 98 | 106 | 102,75 | 0,499 | 103,64 | 0,4062 | 0,5781 | 0,5037 | 10 |
| **YDK\_119** | 94 | 106 | 102,75 | 0,4928 | 103,43 | 0,375 | 0,5938 | 0,5027 | 12 |
| **YDK\_120** | 100 | 108 | 105,5 | 0,5064 | 103,14 | 0,4375 | 0,625 | 0,5083 | 14 |
| **YDK\_121** | 102 | 106 | 104,75 | 0,4974 | 104,14 | 0,3906 | 0,5781 | 0,5034 | 10 |
| **YDK\_122** | 98 | 108 | 105 | 0,4964 | 103,21 | 0,4219 | 0,5781 | 0,5042 | 12 |
| **YDK\_123** | 100 | 108 | 104,75 | 0,4903 | 103,07 | 0,3906 | 0,5781 | 0,4995 | 12 |
| **YDK\_124** | 98 | 106 | 103 | 0,4934 | 103,43 | 0,4062 | 0,5781 | 0,5071 | 12 |
| **YDK\_125** | 100 | 106 | 104,25 | 0,4983 | 103,79 | 0,4062 | 0,625 | 0,5039 | 14 |
| **YDK\_126** | 98 | 108 | 102,5 | 0,4959 | 103,64 | 0,4062 | 0,625 | 0,5112 | 12 |
| **YDK\_127** | 98 | 106 | 103 | 0,4905 | 103 | 0,4062 | 0,6094 | 0,5088 | 12 |
| **YDK\_128** | 100 | 106 | 103,75 | 0,505 | 102,14 | 0,4219 | 0,6094 | 0,5154 | 12 |
| **YDK\_129** | 100 | 106 | 102,75 | 0,5045 | 102,5 | 0,4062 | 0,625 | 0,5112 | 12 |
| **YDK\_130** | 102 | 106 | 104,75 | 0,4975 | 103 | 0,4375 | 0,5781 | 0,5115 | 10 |
| **YDK\_131** | 98 | 108 | 104,25 | 0,5022 | 103,36 | 0,375 | 0,5938 | 0,5027 | 12 |
| **YDK\_132** | 100 | 108 | 104,25 | 0,4991 | 103,21 | 0,3906 | 0,5938 | 0,5049 | 10 |
| **YDK\_133** | 100 | 108 | 104,5 | 0,4998 | 103,21 | 0,4062 | 0,5781 | 0,4973 | 12 |
| **YDK\_134** | 100 | 108 | 104,25 | 0,4992 | 103,43 | 0,4219 | 0,625 | 0,4949 | 12 |
| **YDK\_135** | 98 | 106 | 103,25 | 0,5029 | 102,93 | 0,3438 | 0,5938 | 0,4993 | 12 |
| **YDK\_136** | 100 | 108 | 104,25 | 0,4978 | 103,57 | 0,3906 | 0,6094 | 0,5068 | 12 |
| **YDK\_137** | 94 | 106 | 103 | 0,4943 | 103,86 | 0,3906 | 0,5781 | 0,4983 | 12 |
| **YDK\_138** | 102 | 104 | 103 | 0,5018 | 103,43 | 0,3906 | 0,625 | 0,5142 | 12 |
| **YDK\_139** | 100 | 106 | 102,75 | 0,5017 | 103,29 | 0,3906 | 0,6406 | 0,5095 | 12 |
| **YDK\_140** | 96 | 106 | 102 | 0,5034 | 104 | 0,3594 | 0,6094 | 0,5032 | 12 |
| **YDK\_141** | 100 | 106 | 102,5 | 0,5017 | 102,71 | 0,4062 | 0,625 | 0,5076 | 12 |
| **YDK\_142** | 100 | 106 | 104,5 | 0,5003 | 103,57 | 0,375 | 0,625 | 0,4976 | 10 |
| **YDK\_143** | 102 | 108 | 104,75 | 0,4971 | 102,71 | 0,375 | 0,6094 | 0,4978 | 12 |
| **YDK\_144** | 96 | 106 | 101,75 | 0,4955 | 103,64 | 0,375 | 0,5938 | 0,5049 | 12 |
| **YDK\_145** | 102 | 106 | 103,5 | 0,5002 | 103,36 | 0,3906 | 0,625 | 0,4934 | 12 |
| **YDK\_146** | 104 | 108 | 106,25 | 0,5047 | 103,29 | 0,4062 | 0,6094 | 0,4985 | 12 |
| **YDK\_147** | 100 | 106 | 103,25 | 0,5047 | 103,86 | 0,4062 | 0,5938 | 0,499 | 10 |
| **YDK\_148** | 100 | 106 | 104 | 0,4998 | 104 | 0,375 | 0,6094 | 0,488 | 12 |
| **YDK\_149** | 100 | 108 | 103,75 | 0,5052 | 103,71 | 0,3906 | 0,5781 | 0,4998 | 12 |
| **YDK\_150** | 96 | 106 | 102,75 | 0,4964 | 103,29 | 0,3594 | 0,5781 | 0,4856 | 12 |
| **YDK\_151** | 100 | 106 | 103,5 | 0,4987 | 102,79 | 0,4062 | 0,5938 | 0,5034 | 12 |
| **YDK\_152** | 98 | 108 | 103,5 | 0,5005 | 103,79 | 0,4219 | 0,6094 | 0,5049 | 12 |
| **YDK\_153** | 102 | 106 | 103,75 | 0,4923 | 103,71 | 0,3906 | 0,5938 | 0,5015 | 10 |
| **YDK\_154** | 96 | 106 | 102 | 0,4997 | 104,29 | 0,4062 | 0,5781 | 0,5012 | 12 |
| **YDK\_155** | 98 | 104 | 101,5 | 0,5016 | 103,57 | 0,375 | 0,625 | 0,4954 | 12 |
| **YDK\_156** | 100 | 108 | 104,5 | 0,5042 | 103,79 | 0,3906 | 0,5781 | 0,4973 | 10 |
| **YDK\_157** | 102 | 108 | 105,5 | 0,502 | 104,86 | 0,4062 | 0,5781 | 0,5078 | 12 |



54

**Tablo E3.1.** Değişen YDK (Devamı)

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  |  |  |  |  | **I/O XOR** |
|  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** |
|  |  |  |  |  |  |  |  |  |  |
| **YDK\_158** | 102 | 108 | 105,5 | 0,505 | 103,79 | 0,4062 | 0,5938 | 0,4998 | 12 |
| **YDK\_159** | 96 | 110 | 104,75 | 0,5014 | 103,29 | 0,4062 | 0,5781 | 0,5012 | 12 |
| **YDK\_160** | 100 | 106 | 103,75 | 0,4999 | 102,93 | 0,4062 | 0,5938 | 0,4912 | 12 |
| **YDK\_161** | 96 | 106 | 103 | 0,5012 | 103,07 | 0,375 | 0,5938 | 0,5005 | 10 |
| **YDK\_162** | 102 | 108 | 104,5 | 0,4991 | 104,14 | 0,4219 | 0,5938 | 0,501 | 10 |
| **YDK\_163** | 100 | 106 | 103,5 | 0,4971 | 103,36 | 0,4062 | 0,6094 | 0,4944 | 10 |
| **YDK\_164** | 100 | 108 | 104 | 0,5036 | 103,93 | 0,375 | 0,6094 | 0,4929 | 10 |
| **YDK\_165** | 102 | 108 | 104,5 | 0,503 | 103,5 | 0,4219 | 0,5781 | 0,4976 | 12 |
| **YDK\_166** | 98 | 108 | 104,25 | 0,5027 | 104,21 | 0,4219 | 0,625 | 0,5056 | 10 |
| **YDK\_167** | 98 | 108 | 103,25 | 0,4944 | 102,79 | 0,4219 | 0,6094 | 0,5 | 12 |
| **YDK\_168** | 94 | 106 | 102,5 | 0,5028 | 103,71 | 0,375 | 0,6562 | 0,4968 | 14 |
| **YDK\_169** | 102 | 108 | 104,75 | 0,4941 | 103,57 | 0,3906 | 0,6562 | 0,498 | 12 |
| **YDK\_170** | 100 | 106 | 104 | 0,5008 | 103,21 | 0,4062 | 0,5938 | 0,5044 | 12 |
| **YDK\_171** | 102 | 106 | 104 | 0,4948 | 103,21 | 0,4219 | 0,5938 | 0,5063 | 12 |
| **YDK\_172** | 102 | 106 | 104,75 | 0,4972 | 103,14 | 0,375 | 0,6094 | 0,5081 | 12 |
| **YDK\_173** | 100 | 106 | 102,75 | 0,5036 | 104,14 | 0,4375 | 0,6094 | 0,5059 | 10 |
| **YDK\_174** | 102 | 108 | 104,75 | 0,5 | 102,07 | 0,4219 | 0,6094 | 0,5029 | 10 |
| **YDK\_175** | 94 | 106 | 103 | 0,4969 | 103,5 | 0,375 | 0,6094 | 0,4971 | 12 |
| **YDK\_176** | 98 | 106 | 102,5 | 0,4957 | 103,14 | 0,4062 | 0,625 | 0,5027 | 12 |
| **YDK\_177** | 98 | 108 | 103,5 | 0,4971 | 103,57 | 0,4062 | 0,5938 | 0,5056 | 12 |
| **YDK\_178** | 102 | 106 | 103,5 | 0,4987 | 103,79 | 0,375 | 0,6094 | 0,4956 | 10 |
| **YDK\_179** | 98 | 108 | 102,25 | 0,4995 | 102,86 | 0,3906 | 0,5781 | 0,5005 | 12 |
| **YDK\_180** | 100 | 106 | 103 | 0,4967 | 103,43 | 0,4219 | 0,5938 | 0,5073 | 12 |
| **YDK\_181** | 100 | 104 | 102,5 | 0,5 | 103,43 | 0,4375 | 0,5781 | 0,5 | 10 |
| **YDK\_182** | 100 | 108 | 104 | 0,5007 | 103,71 | 0,4062 | 0,5938 | 0,5059 | 12 |
| **YDK\_183** | 100 | 108 | 104,5 | 0,5022 | 104 | 0,375 | 0,625 | 0,5051 | 12 |
| **YDK\_184** | 102 | 106 | 104,5 | 0,4979 | 102,71 | 0,3906 | 0,5938 | 0,5027 | 10 |
| **YDK\_185** | 100 | 108 | 104 | 0,4923 | 104,43 | 0,4062 | 0,5781 | 0,5022 | 12 |
| **YDK\_186** | 100 | 106 | 103,75 | 0,4976 | 103,64 | 0,4062 | 0,6406 | 0,5029 | 10 |
| **YDK\_187** | 100 | 106 | 103,25 | 0,5038 | 103,71 | 0,3906 | 0,6094 | 0,5017 | 12 |
| **YDK\_188** | 102 | 106 | 103,75 | 0,5019 | 103,43 | 0,3906 | 0,5781 | 0,501 | 12 |
| **YDK\_189** | 100 | 106 | 103,75 | 0,4993 | 103,86 | 0,375 | 0,6094 | 0,5007 | 10 |
| **YDK\_190** | 98 | 106 | 103,5 | 0,499 | 103,93 | 0,4062 | 0,6094 | 0,4998 | 10 |
| **YDK\_191** | 100 | 108 | 104,25 | 0,5007 | 103,14 | 0,4062 | 0,6094 | 0,499 | 12 |
| **YDK\_192** | 98 | 108 | 103,5 | 0,5062 | 104,43 | 0,,4062 | 0,625 | 0,5012 | 12 |
| **YDK\_193** | 98 | 106 | 102,75 | 0,4989 | 103,93 | 0,4062 | 0,5938 | 0,5012 | 12 |
| **YDK\_194** | 98 | 106 | 102,25 | 0,5059 | 103,5 | 0,4062 | 0,6094 | 0,498 | 12 |
| **YDK\_195** | 102 | 108 | 105,75 | 0,4982 | 103,43 | 0,3906 | 0,5938 | 0,4966 | 12 |
| **YDK\_196** | 96 | 108 | 102,5 | 0,5011 | 104,43 | 0,4062 | 0,5938 | 0,5066 | 12 |
| **YDK\_197** | 100 | 106 | 103 | 0,5012 | 104,79 | 0,3906 | 0,6094 | 0,4971 | 12 |



55

**Tablo E3.1.** Değişen YDK (Devamı)

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **YDK** |  | **Doğrusalsızlık** | | **Bit Bağımsızlık Kriteri** | | **Katı Çığ Kriteri** | | | **Maksimum** |
|  |  |  |  |  |  |  |  |  |  | **I/O XOR** |
|  |  | **min** | **mak** | **ort** | **KÇK** | **Doğ.** | **min** | **mak** | **ort** |
|  |  |  |  |  |  |  |  |  |  |  |
|  | **YDK\_198** | 98 | 108 | 104 | 0,505 | 104,21 | 0,4219 | 0,5781 | 0,5017 | 12 |
|  | **YDK\_199** | 100 | 108 | 103,5 | 0,4973 | 103,93 | 0,3906 | 0,5938 | 0,5032 | 10 |
|  | **YDK\_200** | 98 | 106 | 103,25 | 0,4987 | 104,21 | 0,3906 | 0,625 | 0,51 | 10 |
|  | **YDK\_201** | 98 | 106 | 102 | 0,5052 | 103,71 | 0,4062 | 0,6094 | 0,5024 | 12 |
|  | **YDK\_202** | 102 | 108 | 104,75 | 0,501 | 104 | 0,375 | 0,5938 | 0,5073 | 12 |
|  | **YDK\_203** | 98 | 108 | 103,25 | 0,4984 | 103,29 | 0,3906 | 0,625 | 0,5032 | 12 |
|  | **YDK\_204** | 92 | 108 | 102,25 | 0,4974 | 103 | 0,4062 | 0,625 | 0,4988 | 12 |
|  | **YDK\_205** | 100 | 106 | 102,75 | 0,499 | 103,93 | 0,4219 | 0,5938 | 0,5044 | 12 |
|  | **YDK\_206** | 102 | 108 | 105,5 | 0,4972 | 103,21 | 0,375 | 0,5781 | 0,4905 | 12 |
|  | **YDK\_207** | 98 | 108 | 103 | 0,5035 | 104,14 | 0,4062 | 0,6094 | 0,5046 | 10 |
|  | **YDK\_208** | 102 | 108 | 104,75 | 0,4978 | 104,14 | 0,4062 | 0,5938 | 0,4946 | 10 |
|  | **YDK\_209** | 100 | 108 | 104,25 | 0,4985 | 103,29 | 0,3906 | 0,6094 | 0,5095 | 12 |
|  | **YDK\_210** | 98 | 108 | 103,5 | 0,5022 | 103,93 | 0,3906 | 0,6094 | 0,4983 | 10 |
|  | **YDK\_211** | 96 | 106 | 102,75 | 0,502 | 103,14 | 0,375 | 0,6094 | 0,4971 | 12 |
|  | **YDK\_212** | 100 | 108 | 104,5 | 0,4924 | 102,43 | 0,4219 | 0,6094 | 0,5012 | 10 |
|  | **YDK\_213** | 100 | 108 | 103,75 | 0,496 | 104,36 | 0,3906 | 0,5938 | 0,4983 | 10 |
|  | **YDK\_214** | 94 | 108 | 103,25 | 0,4979 | 104,07 | 0,4219 | 0,625 | 0,5056 | 12 |
|  | **YDK\_215** | 96 | 108 | 102,5 | 0,5 | 103,5 | 0,375 | 0,6094 | 0,5002 | 12 |
|  | **YDK\_216** | 100 | 108 | 105,25 | 0,4978 | 103,79 | 0,3906 | 0,5938 | 0,4907 | 12 |
|  | **YDK\_217** | 98 | 106 | 103,25 | 0,5007 | 103,14 | 0,3594 | 0,6094 | 0,5056 | 12 |
|  | **YDK\_218** | 100 | 106 | 103 | 0,4977 | 103,86 | 0,3594 | 0,5781 | 0,498 | 12 |
|  | **YDK\_219** | 94 | 108 | 102,75 | 0,4957 | 104 | 0,3906 | 0,5938 | 0,5105 | 12 |
|  |  |  |  |  |  |  |  |  |  |  |



56

**ÖZGEÇMİŞ**

|  |  |
| --- | --- |
|  | **Yaşar Selim BAHÇECİ** |
| **KİŞİSEL BİLGİLER** |  |
|  |  |
| **Doğum Yeri** | **:** Pertek |
| **Doğum Yılı** | **:** 1986 |
| **Uyruğu** | **:** T.C. |
| **Adres** | **:** İzzetpaşa Mah., Kubilay Sok., Şahin Apt.,No:11/8, Merkez/ELAZIĞ |
| **E-posta** | **:** yasarselimbahceci@gmail.com |
| **Yabancı Diller** | **:** İngilizce(Düzey:Orta) |
| **EĞİTİM BİLGİLERİ** |  |
|  |  |
| **Lisans** | **:** Fırat Üniversitesi, Teknik Eğitim Fakültesi, Elektronik Bilgisayar Eğitimi |
| Bölümü, Bilgisayar Öğretmenliği, 2007 | |
| **Lisans** | **:** Fırat Üniversitesi,TeknolojiFakültesi, YazılımMühendisliği Bölümü,2015 |
| **Lise** | **:** Mustafa Kemal Çok ProgramlıLisesi,Pertek/TUNCELİ, 2003 |
| **İŞ DENEYİMİ** |  |
|  |  |
| **2008 – Halen** | **:** MEBÖğretmen/Yönetici |



**AKADEMİK FAALİYETLER**

**Makaleler:**

1. Bahceci, Y. S., Özkaynak, F.(2019). Rasgele Seçim Tabanlı Yer Değiştirme Kutularının Performans İyileştirmesi için Son İşlem Algoritmaları. Bilgisayar Bilimleri ve

Teknolojileri Dergisi, 1(1), 16-21.

**Bildiriler:**

1. Bahceci Y. S., Özkaynak F., (2019), A new method for performance improvement of chaotic s-box structures International Conference on Engineering Technologies, 25-27 October 2019 Konya, Turkey
2. Bahceci Y. S., Özkaynak F., (2020), A New Substitution Box Structure Based on Nose– Hoover Chaotic System , 13th CHAOS2020 Tuesday 9 - Friday 12 June 2020, Florence, Italy