T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KAOS TABANLI SİMETRİK ŞİFRELEME SİSTEMLERİNİN TASARIM VE ANALİZİ

FATİH ÖZKAYNAK

DOKTORA TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI
BİLGİSAYAR MÜHENDİSLİĞİ PROGRAMI

DANIŞMAN
YRD. DOÇ. DR. SIRMA YAVUZ

İSTANBUL, 2013

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KAOS TABANLI SİMETRİK ŞİFRELEME SİSTEMLERİNİN TASARIM VE ANALİZİ

Fatih ÖZKAYNAK tarafından hazırlanan tez çalışması 16.09.2013 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalı'nda **DOKTORA TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Yrd. Doç. Dr. Sırma YAVUZ

Yıldız Teknik Üniversitesi

Eş Danışman

Doç. Dr. A. Bedri ÖZER

Fırat Üniversitesi

Jüri Üyeleri

Yrd. Doç. Dr. Sırma YAVUZ

Yıldız Teknik Üniversitesi

Prof. Dr. Ercan SOLAK

Işık Üniversitesi

Yrd. Doç. Dr. M. Fatih AMASYALI

Yıldız Teknik Üniversitesi

Yrd. Doç. Dr. Nihan KAHRAMAN

Yıldız Teknik Üniversitesi

Doç. Dr. Müştak Erhan YALÇIN

İstanbul Teknik Üniversitesi

ÖNSÖZ

Kaotik sistemeler bilimin birçok dalında uygulama alanı bulunan bir konudur. Bilgisayar bilimlerindeki en yaygın kullanım alanlarından biri ise kaotik sistemlerin sahip olduğu dinamikleri kullanarak çeşitli şifreleme algoritmalarının tasarlanmasıdır. Ancak geçen yıllar boyunca kaos tabanlı kriptoloji çalışmaları ana kriptoloji literatürüne çok fazla katkı sağlamamıştır. Bu tip bir sonucun ortaya çıkmasındaki en önemli etkenlerden biri tasarım önerilerinin güvenlik analizi çalışmalarına yeterince önem verilmemesinden dolayı zayıf önerilerin kolayca kırılmasından kaynaklanmaktadır. Bu tez çalışmasında bu eksikliği gidermek için öncelikle son zamanlarda önerilmiş bazı şifreleme algoritmalarının güvenlik analizleri verilmiştir. Elde edilen sonuçların mevcut saldırı birikimine katkı sağlaması ve yeni önerilerin analizinde bir değerlendirilme kriteri olarak kullanılabileceği düşünülmektedir. Analiz çalışmalarının ardından kriptolojik uygulamalarda bir rasgelelik kaynağı olarak kullanılan kaotik sistemlerin rasgelelik özellikleri incelenmiş ve kaotik sistemlerin standart bir rasgele fonksiyondan daha kötü rasgelelik özelliklerine sahip olduğu deneysel sonuçlar ile gösterilmiştir.

Bu çalışmanın her aşamasında desteğini gördüğüm doktora tez danışmanım Yrd. Doç. Dr. Sırma YAVUZ'a teşekkürlerimi sunarım. Tezimin eş danışmanı olan ve benim için bir danışmandan çok bir ağabey gibi her konuda desteğini gördüğüm Doç. Dr. A. Bedri ÖZER'e teşekkür ederim. Kaos tabanlı kriptoloji literatürü için sayılı uzmanlardan biri olup tezin şekillenmesinde büyük katkısı olan Prof. Dr. Ercan SOLAK'a, kısa bir süre yöneticiliğimi yapmasına rağmen doktora ders dönemi sürecinin tamamlanmasında büyük desteğini gördüğüm Öğr. Gör. E. Engür AKARSU'ya ve oda arkadaşım M. Rıza SARAÇ'a teşekkür ederim.

Hayatım boyunca üzerimdeki emeklerini ödeyemeyeceğim Anne ve Babama minnettar olduğumu özellikle belirtmek isterim. Beni her durumda desteklediği için kardeşime teşekkür ederim. Son olarak eşim ve biricik oğlum Osman'a ayrıca teşekkür ederim.

Eylül, 2013

Fatih ÖZKAYNAK

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

A	Saldırgan
C	Şifreli metin
D	Şifre çözme algoritması
E	Şifreleme algoritması
K	Anahtar
P	Açık metin (orijinal veri)
R	Alıcı
S	Gönderici

KISALTMA LİSTESİ

IEEE	Institute of Electrical and Electronics Engineers
S-box	Substitution box

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

ÖZET

KAOS TABANLI SİMETRİK ŞİFRELEME SİSTEMLERİNİN TASARIM VE ANALİZİ

Fatih ÖZKAYNAK

Bilgisayar Mühendisliği Anabilim Dalı

Doktora Tezi

Tez Danışmanı: Yrd. Doç. Dr. Sırma YAVUZ

Eş Danışman: Doç. Dr. A. Bedri ÖZER

Modern bilgisayar, ağ ve bilgi teknolojilerindeki hızlı gelişmelerle birlikte sayısal verilerin güvenliği gittikçe önem kazanmıştır. Multimedya verilerinin sahip olduğu özel özelliklerden dolayı klasik şifreleme algoritmaları multimedya verilerinin etkili bir şekilde korunmasında başarısız kalmaktadır. Bu problemin üstesinden gelmek için araştırmacılar doğrusal olmayan teorilerle bağlantılı multimedya verilerine özel şifreleme algoritmaları geliştirmeye çalışmaktadır.

Kaos ve kriptoloji arasındaki benzerlik sonucu güvenli ve hızlı şifreleme algoritmalarını kaotik sistemler kullanarak nasıl tasarlanacağı konusu geniş bir araştırma alanına sahip olmuştur. 1990'lardan beri, kaos tabanlı birçok şifreleme algoritması önerilmiştir. Fakat bazı algoritmaların kriptolojik olarak güvenli olmadığı bulunmuş ve daha güvenli algoritmaları geliştirmek için bazı genel önerilerde bulunulmuştur.

Bu tez çalışması kaos tabanlı simetrik şifreleme algoritmalarının tasarım ve güvenlik analizi ile ilgilidir. Algoritmaların güvenliğine karşı kaba kuvvet saldırısı, bilinen/seçilen açık metin saldırısı ve diferansiyel saldırı gibi bazı genel saldırı yöntemleri teorik analizler ve deneysel doğrulamalar ile detaylı olarak araştırılmıştır. Ek olarak bazı özel tasarım kriterleri kümesi açığa çıkarılmıştır. Tezde kriptolojik protokollerin tasarımında rasgele benzeri bir süreç olarak tanımlanan kaotik sistemlerin kullanılması durumunda hesaplama duyarlılığına bağlı olarak kaotik sistemlerin gösterdiği davranışın şifreleme

sistemi üzerine olan etkisi analiz edilmiştir. Modern kriptolojik tasarımlar çalışma alanı olarak tamsayıların sonlu bir kümesini kullanırken kaotik sistemler reel sayıların bir kümesini kullanmaktadır. Bu yüzden sayısal bilgisayarlar üzerinde kaotik sistemlerin benzetimi yapılırken yuvarlama, kesme gibi işlemlerden dolayı bir sayısal kötüleşme meydana gelmektedir. Bu da kaostan beklenen rasgele benzeri bir davranış yerine periyodik bir davranış göstermesine sebep olmakta ve sonuç olarak kriptolojik tasarıların temel gereksinimleri olan karıştırma ve yayılma özellikleri sağlanamamaktadır. Bu sonuçlar ile sayısal kaosun yeni kriptolojik tasarımlar yapmak için uygunluğu kaotik kriptoloji literatürü tarafından yeniden değerlendirilmelidir.

Bu tez çalışmasında katkımız sayısal kaos tabanlı şifreleme sistemlerinin aşağıdaki üç yönünü içermektedir: sayısal kaotik sistemlerin rasgelelik özelliklerinin deneysel analizleri, kaos tabanlı şifreleme sistemlerinin kriptanalizi ve kaos tabanlı yerine koyma tablolarının yeni tasarımları. Tezde gerçekleştirilen temel başarımlar aşağıdaki gibidir.

- Üç farklı kaos tabanlı yerine koyma tablosu algoritması önerilmiştir. Önerilen yeni tasarımların literatürdeki benzerlerine kıyasla daha iyi kriptolojik özelliklere sahip olduğu görülmüştür.
- Kaos tabanlı şifreleme sistemlerinin kriptanalizi için genel bir saldırı senaryosu önerilmiştir.
- Önerilen saldırı senaryosu kullanılarak 11 farklı şifreleme algoritmasının güvenlik analizi yapılmıştır.
- Birçok şifreleme algoritmasında rasgelelik kaynağı olarak kullanılan lojistik harita standart rasgelelik testlerini geçmesine rağmen rasgelelik özellikleri standart bir rasgele fonksiyondan daha kötü olduğunu deneysel sonuçlar göstermiştir.

Anahtar Kelimeler: Kaos, kriptoloji, simetrik şifreleme, kriptanaliz, kaos tabanlı kriptoloji

ABSTRACT

DESIGN AND ANALYSIS OF CHAOS BASED SYMMETRIC ENCRYPTION SYSTEMS

Fatih ÖZKAYNAK

Department of Computer Engineering

Ph. D. Thesis

Adviser: Assist. Prof. Dr. Sırma YAVUZ

Co-Adviser: Assoc. Prof. Dr. A. Bedri ÖZER

The security of digital data becomes more and more important due to the rapid development of the modern computer, networking and information technologies. Notably, the traditional encryption schemes fail to protect the multimedia data efficiently because of the special properties of multimedia data. To overcome this difficulty, researchers tried to develop special encryption schemes for multimedia data adopting some related nonlinear theories.

The similarity between chaos and cryptography promoted the wide investigation on how to use chaotic systems to design secure and fast encryption schemes. A great number of chaos based encryption schemes have been proposed since 1990s. However, some new schemes have been found to be insecure from the viewpoint of cryptography, and some general recommendations have been drawn to facilitate the design of more secure encryption schemes.

This thesis is concerned with the design and security analysis of chaos based symmetric encryption schemes. The security of the schemes against some common attack methods, such as brute-force attack, known/chosen-plaintext attack and differential attack, is investigated in detail with theoretical analyses and experimental verifications. In addition, some special design defects of the schemes are revealed and

discussed. In this thesis, analyses the effects of chaotic system behaviors over cryptography systems depending on computational precision, when definite chaotic systems are used as pseudo random processes during cryptologic protocol design. While cryptologic designs use a finite set of integers as the workspace, chaotic systems use a set of real numbers. As a result, simulations of chaotic systems on digital computers suffer from truncation and round-off errors. In consequence, random behavior expected from chaos is replaced with periodical behavior which does not meet the confusion and diffusion requirements of the cryptologic designs. With these results, suitability of digital chaos in new cryptologic designs should be re-evaluated by the chaotic cryptology literature.

Our contributions in this dissertation involve the following three aspects about digital chaos based cryptographic systems ciphers: experimental analyses of randomness properties of digital chaotic systems, cryptanalyses of chaos based cryptographic systems, and new designs of chaos based substitution boxes. The main achievements contained in this dissertation are as follows:

- Three different chaos based substitution box algorithm have been proposed. The performance of the proposed substitution box design has been compared to other chaos based substitution box designs and new designs have been demonstrated to provide a stronger substitution box design.
- A general attack scenario has been proposed for chaos based cryptographic systems.
- Security analyses of eleven different encryption algorithms have been done using proposed attack scenario.
- Experimental results show that logistic map, which are used as a source of randomness in many encryption algorithms, successfully pass the standard statistical tests, but its cryptographic randomness properties are worse than any standard random function.

Key words: Chaos, cryptography, symmetric encryption, cryptanalysis, chaos based cryptography

BÖLÜM 1

GİRİŞ

Ülkemizde bilişim teknolojileri alanındaki hızlı gelişmelere rağmen etkin bir şekilde kullanılması konusunda birçok yetersizlik söz konusudur. Toplumumuzda bilişim teknolojilerinin temel bileşeni olan bilginin önemi tam olarak anlaşılmış değildir. Bilginin sahip olduğu önem ve potansiyelin tam olarak anlaşılamamasından bilgi güvenliğine yeterli derecede önem verilmemektedir [1].

"Vizyon 2023: Bilim ve Teknoloji Stratejileri" raporunda [2] tanımlandığı şekliyle bilgi güvenliği; kişilere ilişkin bilgiyi saklı tutma ve iletilen herhangi bir bilginin alıcısından başkasına gitmemesini sağlama şeklinde iki başlık altında özetlenmiştir. Buradan hareketle ulusal çıkarlar doğrultusunda mevcut şifreleme algoritmalarının analiz edilmesi ve elde edilen bulgular doğrultusunda yeni şifreleme sistemlerin tasarlanmasının önemi büyüktür.

1.1 Literatür Özeti

Kriptoloji haberleşen iki veya daha fazla tarafın bilgi alışverişini emniyetli olarak yapmasını sağlayan temeli matematiksel zor problemlere dayanan tekniklerin ve uygulamaların bütünüdür. Kriptoloji biliminin kriptografi ve kriptanaliz olarak adlandırılan iki temel alt dalı bulunmaktadır. Kriptografi belgelerin şifrelenmesi ve şifresinin çözülmesi için kullanılan yöntemleri araştırırken; kriptanaliz ise kriptolojik sistemlerin kurduğu mekanizmaları inceler ve kırmaya çalışır [3-7].

Kaos doğrusal olmayan dinamik sistemlerde bulunan gerekirci (deterministik) ve rasgele benzeri bir süreçtir. Kaotik sistemler periyodik değildir ve sonlu olmalarına rağmen bir değere yakınsamazlar. Kaotik sistemlerin en belirgin özelliği başlangıç

koşulları ve kontrol parametrelerine oldukça bağımlı olmasıdır. Kaosun doğası görünürde rasgele 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 rasgeleliği olarak tanımlanabilir [8-13, 21].

Kaos ve kriptoloji bilimleri arasındaki yakın ilişkinin ortaya koyulması kaotik sistemleri kullanarak kriptolojik sistemlerin güvenliğinin artırılıp artırılamayacağı düşüncesini ortaya koyulmuştur [17-20, 26, 28]. İki disiplin arasındaki bu ilişki Shannon'un [25] herhangi bir şifreleme sisteminin güvenilir olması için sahip olması gereken özellikler olan karıştırma (confusion) ve yayılma (diffusion) özellikleri ile kaotik sistemlerin başlangıç koşullarına hassas duyarlı olması ve doğrusal olmaması özellikleriyle örtüşmesinden ortaya çıkmaktadır.

Kaosun kriptolojik uygulamalar için teorik olarak ideal bir aday olmasından dolayı literatürde birçok kaos tabanlı şifreleme algoritma önerisi bulunmaktadır [28-98]. Bu algoritmalarda kaotik sistemler bir rasgelelik kaynağı olarak düşünülmüş ve kaotik sistemin çıkışı aracılığıyla bilginin karılması sağlanmıştır. Ancak bu algoritmaların bir kısmının zayıflıkları gösterilmiştir [99-119]. Kaos tabanlı kriptoloji literatürünün ilginç bir özelliği, araştırmacıların var olan sistemleri analiz etmekten ziyade, yeni sistem tasarlama çalışmalarına ağırlık vermeleridir. Yeterli analiz çalışması yapılmadığından dolayı da, yeni tasarımlar hala bazı basit saldırılara karşı bile dayanıksız olmaktadır. Bu eksikliği göstermek için literatürde birçok kriptanaliz çalışması gerçekleştirilmiş ve kaos tabanlı şifreleme algoritmaları için bir tasarım kriterleri kümesi önerisinde bulunulmuştur [17-20, 23, 24, 26].

1.2 Tezin Amacı

Tez çalışmasının üç temel amacı bulunmaktadır. Bunlar:

- Kaotik sistemleri bir rasgelelik kaynağı olarak kullanarak yeni kriptolojik yerine koyma tabloları tasarımları gerçekleştirmek.
- Mevcut kaos tabanlı kriptolojik tasarımların zayıflıklarını inceleyerek mevcut saldırı birikimine katkı sağlamak.

- Bir rasgelelik kaynağı olarak kaotik sistemlerin rasgelelik özelliklerini inceleyerek kaos tabanlı rasgele fonksiyonların kriptolojik tasarımlar için uygunluğunu incelenmek.

olarak belirlenmiştir.

1.3 Bulgular

Tez çalışmasında ilk olarak kaotik sistemler bir rasgelellik kaynağı olarak ele alınmış ve başarı ölçütleri net olarak ölçülebilecek bir kriptolojik yapı taşı olan yerine koyma tablolarının tasarımları üzerine odaklanılmıştır. Farklı türde kaotik sistemler (ayrık zamanlı, sürekli zamanlı, zaman gecikmeli) farklı tasarım algoritmaları ile kullanılarak çeşitli yerine koyma tabloları tasarlanmıştır. Yeni önerilerin performans ölçütlerinin literatürdeki kaos tabanlı tasarımlardan daha iyi olduğu görülmüştür. Ancak en iyi kaos tabanlı tasarımın bile matematiksel tabanlı yerine koyma tablolarından daha kötü olduğu görülmüştür. Bu sonucun elde edilmesi ile kriptanaliz çalışmalarına ağırlık verilmiştir.

Analiz çalışmalarında ilk olarak literatürdeki kaos tabanlı şifreleme algoritmalarının zayıflıkları incelenmiştir. 11 farklı tasarımın güvenlik analizleri yapılmıştır. Yapılan analizler sonucunda cebirsel bağımlılığın yeni şifreleme algoritmalarının tasarımında bir analiz parametresi olarak değerlendirilmesi gerektiği vurgulanmıştır. Ayrıca yeni tasarımların güvenlik analizinde kullanılabilecek genel bir saldırı senaryosu verilmiştir.

Yapılan analiz çalışmaları sonucunda birçok kaos tabanlı kriptolojik tasarımının güvenliğinin sadece istatistiksel testler kullanılarak analiz edildiği görülmüştür. Bu alandaki en önemli problem istatistiksel testlerde başarılı sonuçların elde edilmesinin birçok tasarımcı tarafından kriptolojik sistemin güvenlik analizi için yeterli olduğunun düşünülmesidir. Bu tip bir algıyı ortadan kaldırmak için tezin son kısmında istatistiki testlerin problemleri ve kaosun rasgelelik özellikleri incelenmiştir. Yapılan çalışmalarda lojistik harita çıkışlarının istatistiki testleri geçmesine rağmen hesaplama duyarlılığına bağlı olarak çıkışların rasgelelik özelliklerinin standart bir rasgele fonksiyondan daha kötü olduğu gösterilmiştir. Bu sonuç ile sayısal kaosun yeni kriptolojik tasarımlar

yapmak için gerçekten uygun olup olmadığı sorusunun kaotik kriptoloji literatürü tarafından yeniden değerlendirilmesi gerektiği ön plana çıkmıştır.

1.4 Tezin Organizasyonu

Tez çalışması yedi bölümden oluşmaktadır. İkinci bölümde modern kriptolojinin temelleri özetlenmiştir. Bölümün ilk kısmında bir kriptolojik tasarım yapılırken dikkat edilmesi gereken unsurlar verilmiştir. Birçok tasarım önerisi bilinen basit saldırılara karşı zayıf bir yapıya sahip olduğundan ileride sunulan güvenlik analizi çalışmalarında kullanılacak temel kriptanaliz yöntemleri açıklanmıştır. Bölümün sonunda bir kriptolojik sistem tasarlanırken dikkat edilmesi gereken bazı temel kriterlerde verilmiştir.

Üçüncü bölümde kaos teorisi açıklanmaya çalışılmıştır. İlk olarak kaotik dinamiklerin temel karakteristikleri açıklanmış ardından bir sistemde kaos gözlemlenebilmesi için oluşması gereken gerek ve yeter koşulların neler olduğu gösterilmiştir. Bölümün son kısmında bir sistemde kaosun varlığını gösteren analiz yöntemleri tartışılmıştır.

Dördüncü bölümde kaotik kriptolojinin ilk örneklerinin görüldüğü 1990'lardan günümüze kadar kaos tabanlı kriptoloji literatürünün gelişimi incelenmiştir. Bölümün ilk kısmında literatürdeki tasarım çalışmalarına yer verilirken ikinci kısımda kriptanaliz çalışmaları incelenmiştir. Bu bölümde tezde gerçekleştirilen kaos tabanlı yerine koyma tabloları ile alakalı tasarım çalışmalarına da değinilmiştir.

Beşinci bölümde tez çalışması boyunca yapılan çeşitli kriptanaliz çalışmalarına yer verilmiştir. Bu bölümde 11 farklı kaos tabanlı şifreleme algoritma önerisinin güvenlik analizi yapılmıştır.

Altıncı bölümde öncelikle kaotik sistemlerin sayısal bilgisayarlar üzerinde gerçekleştirildiğinde hesaplama duyarlılığına bağlı olarak sistemin gösterdiği davranıştaki değişimler ve bunun kriptolojik uygulamalara olan etkileri incelenmiştir. Elde edilen sonuçlar ile kriptolojik uygulamalar için sadece istatistiki analizlerin güvenilir olmadığı gösterilmiştir.

Son bölümde tezde yapılan çalışmalar değerlendirilmiş ve gelecek çalışmalara ışık tutması için yeni öneriler sunulmuştur.

BÖLÜM 2

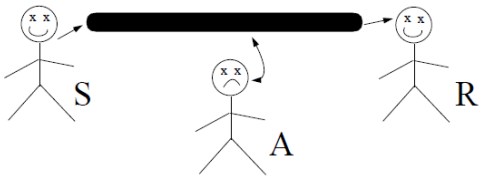
MODERN KRİPTOLOJİNİN TEMELLERİ

Tarihsel olarak kriptoloji gönderici ve alıcı tarafları arasında bir iletişim kanalı boyunca herhangi bir saldırganın müdahalesine karşı bilgi gizliğinin temel alınması anlamına gelmektedir. Gizliliğin sağlanmasındaki temel amaç diğerlerinin erişimine karşı iletişim güvenliğini sağlamak için genişletilmiş bir alanın sağlanmasına ek olarak iletişim bütünlüğünü ve yetkilendirmesini sağlamayı garanti etmektir [3-7].

Kriptoloji yazının icadından beri kullanılmaktadır. Uzun yıllar boyunca, kriptoloji kişiye özel tasarımlar ve bu tasarımlara karşı gerçekleştirilen saldırıların karşılıklı etkileşimi olan bir sanat olarak kalmıştır. Günümüzde ise şifreleme sanatı bir bilim dalı olarak desteklenmektedir. Modern kriptoloji dikkat çekici bir disiplindir. Bilgisayar ve iletişim güvenliğinin köşe taşlarından biridir. Ayrıca sayı teorisi, hesaplama teorisi, karmaşıklık teorisi ve olasılık teorisi gibi matematiğin değişik dallarıyla ilişkilidir. Bu bölümde birçok uygulama alanına sahip olan bu bilim dalının temelleri kısaca özetlenmiştir.

2.1 Modern Kriptolojinin Amaçları

Modern kriptoloji bilimindeki en temel sorun güvensiz bir ortam boyunca iletişim güvenliğinin sağlanmasını garanti etmektir. Gönderici ve alıcı haricinde hiç kimsenin erişimi olmadığı atanmış bir kanal boyunca tarafların haberleştiği mükemmel bir ortam ideal iletişim kanalı olarak adlandırılmaktadır. Şekil 2.1'de bu tip bir ideal iletişim kanalının genel görünümü verilmiştir. İletişim ortamında gönderici S, alıcı R ve bu iletişim kanalındaki herhangi bir kimseyi göstermek için A sembolü kullanılmıştır [7].



Şekil 2.1 İdeal iletişim kanalının genel görünümü

Gerçek yaşamda iletişim kuracak tarafları birbirine bağlayacak ideal iletişim kanalları yoktur. Genellikle gönderici ve alıcılar internet benzeri genel herkese açık bir ağ üzerinden iletişimi sağlamaktadır. Kriptolojinin temel amacı iletişim kuracak tarafların kullandıkları kanalın güvenlik özelliklerinin ideal bir iletişim kanalının sahip olduğu güvenlik özelliklerine benzemesini sağlamaktır. İdeal bir iletişim kanalı tüm yönleriyle taklit edilemeyeceğinden kriptoloji uzmanlarının temel amacı iletişim için kritik öneme sahip olan bazı güvenlik gereksinimlerini sağlamaktır.

İletişim güvenliğinin sağlanması için göz önünde bulundurulması gereken temel gereksinimler gizlilik, kimlik doğrulama ve bütünlük olarak sıralanabilir. Gizliliğin sağlanması iletişim içeriğinin saldırgandan gizlenmesi anlamına gelmektedir. Kimlik doğrulama gereksiniminde alıcı kendisine gelen mesajın geçerli bir göndericiden geldiğini garanti etmektedir. Bütünlük gereksiniminde ise alıcı iletişim kanalından gelen mesajın içeriğinin değişmediğini garanti etmektedir [3-7].

Gizlilik, kimlik doğrulama ve bütünlük gibi güvenlik gereksinimlerini sağlamak için kriptoloji bilimi gönderici ve alıcılara çeşitli protokoller sağlamaktadır. Protokol aslında bir programlar (algoritmalar, yazılımlar) koleksiyonudur [4, 7]. Bu programlardan bazıları gönderici tarafında çalıştırılırken diğer programlar alıcı tarafında aktif olmaktadır. Göndericinin kullandığı programlar iletişim kanalında iletilecek verinin nasıl paketleneceğini (verinin hangi tekniklerle kodlanacağını) göstermektedir. Alıcının kullandığı programlar ise iletişim kanalından alınan paketten orijinal veriyi nasıl geri elde edeceğini (verinin kodunu nasıl çözeceğini) göstermektedir. Hem gönderici hem de alıcı tarafında çalışan programlar çeşitli kriptolojik anahtarları kullanmaktadır.

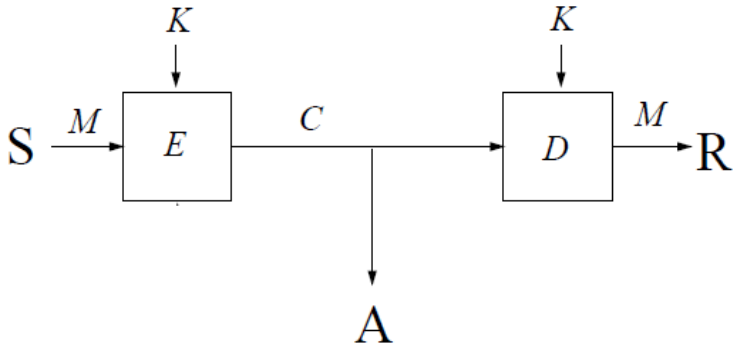
Kriptolojide, iletişim güvenliğinin sağladığını göstermek için çeşitli güven modelleri kullanılmaktadır. Bu güven modelleri tarafların (gönderici, alıcı) ne yapabileceklerini ya da ne yapamayacaklarını göstermektedir. Güven modelleri hangi tip anahtarların

kullanıldığına bağlı olarak sınıflandırılmaktadır. Simetrik (gizli anahtarlı) ve asimetrik (açık anahtarlı) olmak üzere iki tip temel güven modeli bulunmaktadır.

2.1.1 Simetrik Güven Modeli

Simetrik güven modeli olarak adlandırılan yapıda gönderici ve alıcı şifreleme ve şifre çözme için aynı anahtarı kullanmaktadır. Anahtar değerini saldırgan bilmemektedir. Anahtarın genellikle düzgün bir dağılıma sahip rasgele bir karakter topluluğu olduğu varsayılmaktadır. Veri iletişimine başlamadan önce gönderici ve alıcı saldırganın bilmediği bir anahtar değeri üzerinde anlaşırlar. Bu anahtar değerinin güvenli bir şekilde iletildiği varsayılır.

Simetrik güven modelinde veri gizliliğini sağlamak için kullanılan protokol genellikle simetrik (gizli anahtarlı) şifreleme algoritması olarak adlandırılmaktadır. Algoritmanın yapısı Denklem (2.1)'de verilmiştir. Simetrik şifreleme algoritması (π) üç elemandan oluşmaktadır. Burada K gizli anahtarı E gönderici tarafında verinin paketlenmesi için kullanılacak algoritmayı, D alıcı tarafında iletişim kanalından alınan veriden orijinal veriyi elde ederken kullanılacak algoritmayı göstermektedir. Taraflar arasında iletilecek orijinal veri M ile iletişim kanalı boyunca aktarılan şifreli veri ise C ile gösterilmektedir. Şekil 2.2'de simetrik şifreleme algoritmasının genel görünümü verilmiştir.



Şekil 2.2 Simetrik şifreleme algoritmasının genel görünümü

$$\pi(K, E, D) \tag{2.1}$$

2.1.2 Asimetrik Güven Modeli

Asimetrik güven modelinde iletişim yapacak taraflar biri açık (pk) diğeri gizli (sk) olmak üzere iki anahtara sahiptir. Kullanıcının sahip olduğu açık anahtar kendisinin gizli anahtarı ile bağlantılıdır. İletişim yapacak tarafların açık anahtarları (saldırgan da dâhil olmak üzere) herkes tarafından bilinmektedir.

Asimetrik güven modelinde kullanılan protokol genellikle asimetrik (açık anahtarlı) şifreleme algoritması olarak adlandırılmaktadır. Gönderici tarafında çalışan algoritmada veri iletişimi kurulacak alıcının açık anahtarı kullanılarak veri paketlenir ve iletişim kanalıyla alıcıya gönderilir. Verinin şifrelenme süreci Denklem (2.2)'de verilmiştir. Alıcı tarafında kullanılan algoritmada ise iletişim kanalından elde edilen paketlenmiş veriden alıcının gizli anahtarı kullanılarak orijinal veri elde edilir. Verinin şifresinin çözülmesi süreci Denklem (2.3)'de verilmiştir. Asimetrik şifreleme algoritmasının genel görünümü ise Şekil 2.3'de verilmiştir.

$$C = E_{pk_R}(M) \tag{2.2}$$

$$M = D_{sk_R}(C) \tag{2.3}$$

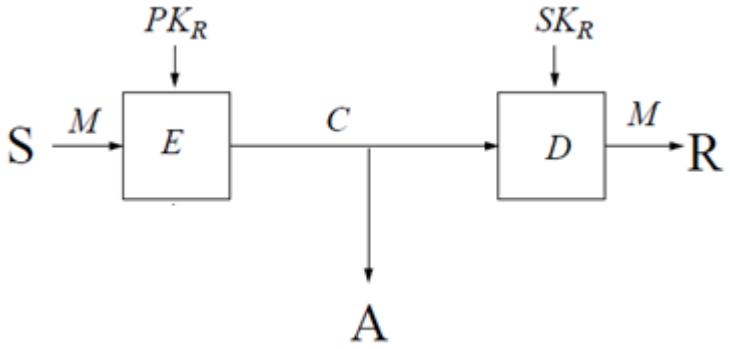
2.2 Modern Kriptolojinin Bileşenleri

2.2.1 Protokoller

Kısa bir tanım ile ifade edilmek istenirse; kriptoloji bilimi saldırganın olumsuz etkilerinin üstesinden gelmek için kullanılacak protokolün kurulması ve analizi edilmesi olarak özetlenebilir [7]. Protokollerin kriptoloji bilimi için bu kadar önemli bir yere sahip olmasından dolayı bu bölümde protokol kavramı detaylı olarak incelenmiştir.

Bir kriptolojik problem çözülmeye çalışıldığında öncelikle problemin tarafları belirlenmelidir. Her ne kadar kriptoloji ile alakalı kaynaklarda basit anlaşılması açısından gönderici ve alıcı herhangi bir kişi olarak gösterilse de aslında iletişim kuracak tarafların çok çeşitli (bir insan, bir cep telefonu, bir bilgisayar, bilgisayar üzerinde çalışan bir süreç, bir uydu alıcısı vb.) olabileceği unutulmamalıdır. Genellikle iletişim kuracak tarafların güvenli bir iletişim sağlamak için gerekli özeni gösterdiği

varsayılmaktadır. Ancak gerçek hayatta durum tahmin edilenden farklıdır. Bu yüzden iletişim güvenliğini sağlamak için protokollerin kullanılması bir zorunluluktur.



Şekil 2.3 Asimetrik şifreleme algoritmasının genel görünümü

Protokoller aslında iletişim kuracak tarafların nasıl davranacağını söylemektedir. Temel olarak protokol bir programdır. Gerekirci, ardışık sonlu komutlar kümesidir (algoritmadır). Protokolün önemli özelliklerinden biri olasılıksal olmasıdır. Bunun anlamı protokol rasgele seçimler yapabilmelidir. Daha biçimsel bir dille ifade edecek olursak protokolde kullanılacak bir değişkene rasgele değer atanırken değişkenin alabileceği tüm değerlerin eşit olasılıklı olması istenmektedir [4, 5, 7].

Protokolleri analiz ederken iletişim kuracak tarafların problemlerini ifade ederken belirtikleri amaçlar ve bu amaçlara yönelik tehditler anlaşılmaya çalışılmalıdır. Protokoller gönderici ve alıcı taraflarının nasıl davranması gerektiğini söylerken saldırganın nasıl davranacağı hakkında bir bilgi vermez. Saldırganın tüm kaynakları tehdit edebileceği varsayılmalıdır [3-7]. Protokol tasarımcısı, iletişim kuracak tarafların güvenliğini sağlamak için kriptolojik problemi katı biçimsel formüllerle ifade ederken; saldırgan bu formüller üzerinde bir açıklık bulmaya çalışır. Aslında protokol tasarımı; saldırgan ve protokol tasarımcısı arasındaki bir oyundur.

Sonuç olarak; güvenli hesaplama sistemleri oluşturmak için sağlam protokoller temel araçlardan biridir. Kötü tasarlanmış protokoller bilgisayar sistemlerinde kolaylıkla fark edilmekte ve kişiye özel tasarlanmış protokoller birçok hata ile sonuçlanmaktadır. Güvenliğin birçok yönü olduğu unutulmamalıdır. Kriptoloji sadece büyük resmin küçük bir parçasıdır ancak en ufak bir açıklık bütün sistemi etkilemektedir.

2.2.2 Kriptoloji Biliminin Kuralları

Kriptoloji bilimi bazı kurallara sahiptir. İlk kural sadece protokoller aracılığıyla saldırgan etkisinin ortadan kaldırılmaya çalışılmasıdır. Yasal yaptırımlar, baskı ve korkutma gibi caydırıcı yöntemler kullanılarak saldırganın sisteme zarar vermesi önlenmeye çalışılabilir. Ancak bu tip yöntemlerin kullanılması kriptoloji biliminin dışındadır. Kriptoloji bilimi sadece etkin bir protokol tasarımı ile alakalıdır [7].

Kriptoloji uzmanlarının uyması istenen diğer önemli bir kural protokol tasarımlarının açık bir şekilde yapılmasıdır. Protokollerin açık olarak tasarlanmasının birkaç farklı sebebi bulunmaktadır. Yetenekli bir saldırgan protokolün ne olduğunu herhangi bir şekilde bulabilir. Çünkü protokoller birçok programda veya çeşitli makinelerde kullanılmaktadır. Bu yüzden protokol tanımının gizlenmeye çalışılması hem maliyetli hem de mantıksızdır. Ek olarak protokol tasarımlarının gizli yapılması kriptolojik sistemin sağlanması gereken güvenlik unsurlarının sağlanıp sağlanmadığının değerlendirilmesini engellemektedir. Hem akademik çalışmalar hem de ticari uygulamalar için önerilen protokoller açık bir şekilde ortaya koyulduğunda kullanıcılar kriptolojik sistemi bütün yönleriyle değerlendirebilir ve sistemin her bir aşamasının nasıl işlediğine dair şüpheler ortadan kaldırılarak sistemin güvenilirliği ortaya koyulmuş olur. Kriptolojik sistem tasarımında protokollerin açık olmasına rağmen anahtarların gizli olması istenmektedir. Bu tip bir ayrımın yapılmasının nedeni protokoller bir algoritma iken anahtarların ise algoritmada kullanılan bir veri olmasıdır [3-7].

2.3 Kriptolojik Tasarım Yaklaşımları

Kriptoloji çalışmalarının tarihi üç temel döneme ayrılabilir. Bu dönemlerden birincisi olan kriptoloji çalışmalarının ilk örneklerinin görüldüğü dönemlerde şifreleme sistemleri sadece kâğıt ve kalem ile gerçekleştirilmektedir. Bu dönemin diğer şifreleme örnekleri ise yer değiştirme şifreleme sistemleri olarak görülmektedir. Bu tip şifreleme sistemlerinde anahtar değeri bir permutasyondur $\pi: \sum \rightarrow \sum$. Herhangi bir $\sigma \in \sum$ sembolü $\pi(\sigma)$ permutasyonu ile şifrelenmektedir. Şifre çözme algoritması ise şifreleme permutasyonunun tersi π^{-1} kullanılarak gerçekleştirilmektedir. İfadelerin basit yapısından görülebileceği gibi bu tip şifreleme sistemleri kolayca kırılabilir.

Kriptoloji çalışmalarının ikinci döneminde kriptolojik makineler görülmektedir. İkinci dünya savaşıyla bağlantılı olan bu dönemdeki en önemli şifreleme örneklerinden biri Alman Enigma makinesi olarak görülmektedir. Ancak bu tip tasarımlarında zayıflıkları gösterilmiş hatta savaşın sonlanmasında önemli bir etken olmuştur.

Kriptoloji çalışmalarının son dönemi modern kriptoloji olarak adlandırılmakta ve bu dönemin temel karakteristiği tasarımların matematik, elektronik ve bilgisayar bilimleri ile iç içe olmasıdır. Bu dönem ile birlikte kriptolojik tasarım çalışmaları bir bilim olarak devam etmiştir.

Bu bölümde temel iki tip kriptolojik tasarım yaklaşımı açıklanmıştır. Öncelikle kriptanaliz destekli tasarım yaklaşımı ardından kanıtlanabilir tasarım yaklaşımları kısaca açıklanmıştır. Tasarım çalışmalarından önce simetrik şifreleme sistemleri için Shannon teorisi, hesaplama ve karmaşıklık teorisinin önemine de kısaca değinilmiştir.

2.3.1 Simetrik Şifreleme için Shannon Teorisi

Kriptolojik yaklaşımlarda sistematik bir yöntem izlendiğinde protokoller ve tanımlamalar önemli bir yer tutmaktadır. Bilgi teorisinin babası olarak kabul edilen Claude Shannon [25] yayınladığı çalışmasında önerdiği sistematik yaklaşımla bir anlamda modern kriptolojinin de babası olarak kabul edilmektedir.

Shannon çalışmasında herhangi bir şifreleme sisteminin güvenilir olması için sahip olması gereken bazı temel özellikleri tanıtmıştır. Karıştırma ve yayılma özellikleri olarak bilinen bu temel özellikler bir şifreleme sisteminin sağlaması gereken temel kriterlerdir.

Karıştırma özelliğine sahip şifreleme sistemlerinde; her anahtar için şifreleme fonksiyonu öyle olmalıdır ki, orijinal veri ve şifreli veri arasında istatistiksel bağlılık olmamalıdır. Bu özelliğin olabilmesi için anahtar ve orijinal verinin her bitinin şifreli veriyi etkilemesi gerekmektedir.

Yayılma özelliğine sahip bir şifreleme sistemi için ise; şifreli veri ile anahtar arasındaki ilişki mümkün olduğunca karmaşık olmalıdır. Diğer bir deyiş ile yayılma, anahtarın orijinal ve şifreli veriye bağlılığının kriptanaliz için faydalı olmayacak kadar karmaşık olması demektir. Yani şifreleme sistemini tanımlayan eşitliklerin doğrusal olmaması ve

karışık olması sağlanmalı böylece $C = E(P, K)$ denkleminden anahtarın bulunması imkânsız olmalıdır.

2.3.2 Hesaplama ve Karmaşıklık Teorisi

Modern kriptolojik tasarımlar yapılırken göz önünde bulundurulması gereken önemli noktalardan biri saldırganın ulaşabileceği hesaplama gücü kapasitesinin değerlendirilmesidir. Eğer saldırganın ulaşabileceği maksimum hesaplama gücü şifreleme sisteminin kırılması için gereken hesaplama gücünden daha düşük ise bu durumda saldırılar mantıksız olacaktır [3-7].

Kriptoloji bilimi bilgi teorisi, bilgisayar bilimi ve özellikle karmaşıklık teorisi ile etkileşimli olmalıdır. Çünkü kriptolojik tasarımlar genellikle zor problemle alakalıdır ve bu problemi çözmek için kullanılacak fonksiyonların tüketeceği kaynaklar (zaman, bellek) araştırılmalıdır.

Kriptolojik tasarımlar yapılırken hesaplama/karmaşıklık teorisinin kullanılması kriptolojik sisteme yapılacak saldırının başarısını değerlendirirken olasılıksal ifadelerde bulunma imkânı tanır. Kriptolojik sistemler olasılıksal denklemler ile ifade edildiği zaman saldırı karmaşıklığı saldırganın kullanacağı algoritmanın (tekniğin) ne olduğundan veya saldırganın ne bildiğinden bağımsız olarak ifade edilebilir. Bu da bu tip bir ifade tarzının ne kadar güçlü olduğunu göstermektedir [7].

Pratikte saldırgan algoritmanın kırılması için gerekli yüksek bir hesaplama yeteneğine sahip olamayacağından; saldırgan ne kadar çabalarsa çabalasın sistemi kıramayacaktır. Bu yüzden bu kadar etkin bir protokol tasarımı için ne yapılması gerektiği sorgulanmalıdır.

2.3.2.1 **Atomik Temeller**

Etkin protokoller oluşturmak için kullanılabilecek en iyi yaklaşımlardan biri en alt seviyedeki atomik temellerin yüksek seviyede protokollere dönüştürülmesidir. Başlangıçta atomik temeller ve protokoller arasındaki bağlantı çok fazla kişinin dikkatini çekmiyordu ancak tek kullanımlık şifreleme algoritması (one time pad)

düşünüldüğünde atomik temeller protokol tasarımında tek nesne olarak gözükmektedir.

Atomik temeller mühendislik yapıları ve matematiksel problemleri gibi iki farklı kaynaktan gelmektedir. Mühendislik yapılarından gelen atomik temellere verilebilecek en iyi örneklerden biri DES blok şifreleme algoritmasında kullanılan yerine koyma tablolarıdır. Matematik problemlerinden gelen atomik temellere verilebilecek en bilinen örneklerden biri ise RSA şifreleme algoritmasıdır.

Kriptolojinin hesapsal doğası gereği kriptolojik tasarım yaklaşımı hesapsal zor bir problemin bulunması prensibine dayanmaktadır. Bu kullanışlı bir yöntem olmasına rağmen yaygın kullanılan yöntemlerden biri değildir. Hesapsal zor bir problem bulunmasında kullanılabilecek ilk yaklaşımlardan biri NP-tam problemler olabilir. NP-tam problemler başlangıçta bazı kriptolojik sistemlerin tasarlanmasında (sırt çantası problemini kullanan şifreleme sistemi gibi) kullanılmıştır. Ancak bu tasarımlar genellikle başarısızlıkla sonuçlanmıştır. Çünkü NP-tam problemler en kötü durum için çözülmesi zor gözükür iken ortalama durum göz önünde bulundurulduğunda kolaylıkla çözülebilmektedir.

Daha kullanışlı bir atomik temel olarak tek yönlü fonksiyonlar kullanılabilir. Tek yönlü fonksiyon $f: D \rightarrow R$ eşlemi aşağıdaki özellikleri sağlamalıdır.

- f fonksiyonu kolayca hesaplanabilmelidir. Yani $x \in D$ için $y = f(x) \in R$ çıktısını veren efektif bir algoritma bulunmalıdır.
- f fonksiyonunun tersinin bulunması zor olmalıdır. Yani saldırganın sahip olduğu rasgele bir $y \in R$ değeri için $f(x) = y$ eşitliğini sağlayan bir x değerinin bulunması saldırganın hesaplama yetenekleri sınırlı olduğu sürece zor olmamalıdır.

2.3.3 Kriptanaliz Destekli Tasarım Yaklaşımı

Geleneksel olarak kriptolojik mekanizmalar tasarlanırken mevcut saldırılara odaklanılmaktadır. Bu tip bir kriptanaliz destekli tasarım yaklaşımı aşağıda verilen adımları izleyerek gerçekleştirilmektedir.

Adım 1. İletişim güvenliğinin sağlanması için gerekli kriptolojik amaçlar belirlenir.

Adım 2. Bu amaçları gerçekleştirmek için bir çözüm yöntemi önerilir.

Adım 3. Önerilen çözüm yöntemini değerlendirmek için saldırı yöntemleri araştırılır.

Adım 4. Önerilen çözüm önerisinin bir kusuru veya eksikliği bulunursa daha iyi bir çözüm bulmak için Adım 2'den devam edilir.

Kriptanaliz destekli tasarım yaklaşımının bazı problemleri vardır. Öncelikle önerilen çözüm yönteminin doğru bir çözüm yöntemi olup olmadığı bilinemez. Diğer bir problem tasarım çalışması sonlandırılamaz. Çünkü saldırı tehdidi devam ettiği sürece çözüm yöntemi değişebilir. Eğer bir ticari ürün ortaya koyulacaksa ürünün yeterli olup olmadığı veya en iyi çözüm olup olmadığı değerlendirilemez. En önemli problemlerden biride tasarım için gizli (açıklanmayan) bir saldırının olmasıdır. Bu durumda kriptolojik çözüm önerisi hatalı olmasına rağmen kullanılmaya devam etmektedir [7].

2.3.4 Kanıtlanabilir Güvenlik Yaklaşımı

Kriptolojide protokollerin kullanılması en etkili yöntemlerden biridir. Ancak kullanılacak protokollerin geçerliliğinin kanıtlanması gerekmektedir. Kanıtlanabilir güvenlik yaklaşımı ilk kez 1982 yılında Goldwasser ve Micali'nin çalışmalarında ortaya çıkmıştır. Goldwasser ve Micali yaptıkları çalışmada açık anahtarlı şifreleme sistemini bilimsel bir temele oturtmayı istemişlerdir.

Daha önce ifade edildiği gibi iyi protokollerin tasarlanabilmesi için atomik temellerin protokollere dönüştürülmesi gerekmektedir. Kriptolojideki önemli çabalardan biri yeni atomik temellerin tasarlanmasıdır. Bu kriptolojinin bir parçası olmamasına rağmen gelecekte kriptoloji uzmanlarının atomik temelleri protokollere çeviren motorlar gibi davranacağı düşünülmektedir [7]. Yani kriptolojik tasarım yaklaşımında amacın iyi bir atomik temelin olduğu varsayımı altında protokol tasarlanmasına odaklanmak olduğu söylenebilir. Zayıf bir şekilde tasarlanmış bir protokol güçlü bir atomik temel kullanmasına rağmen kolayca kırılabilir. Ancak buradaki problem atomik temellerden değil bunların kullanım biçiminden kaynaklanmaktadır.

Kanıtlanabilir güvenlik yaklaşımında öncelikle kriptolojik problemin ortaya koyulmasının ardından problemin biçimsel bir tanımı yapılır. Bu problemi çözmek için kullanılacak atomik temeller belirlenir. Atomik temellerin belirlenmesinin ardından bu atomik temelleri kullanan protokol tasarlanır. Protokolün güvenli olduğunu göstermek için protokol atomik temele indirgenir. Atomik temel güvenli olduğu sürece önerilen protokolün güvenliği ispatlanmış olur.

2.4 Kriptanaliz

Kriptanaliz (kripto-analiz); kriptolojik tasarım çalışmalarının ayrılmaz bir parçasıdır. Kriptanaliz çalışmasının temel amacı iletişim güvenliği sağlamak için önerilen kriptolojik tasarımının ne kadar güvenli olduğunun test edilmesidir [14-16]. Kriptanaliz çalışmaları yapılırken analistin şifreleme algoritmasının bütün detaylarına ulaşabileceği ve sistemde sadece anahtar bilgisinin gizli olduğu varsayılmaktadır. Analist şifreleme sisteminin gizli anahtarını bilmeksizin şifrelenmiş verilerden orijinal verileri elde etmeye çalışır. Aslında analistin asıl amacı gizli anahtarın tamamı veya belli bir kısmını elde etmektir. Analiz yönteminin ne kadar güçlü ve efektif olduğu analiz işlemi için gerekli olan önbilgi (bilinmesi gereken açık/şifreli metin çifti sayısı gibi) ve yapılacak iş miktarı (saldırının gerçekleştirilmesi için gerekli zaman ve bellek miktarı) ile orantılıdır.

2.4.1 Saldırı Çeşitleri

- Sadece Şifreli Metin Saldırısı (Ciphertext-Only Attack) : Saldırgan sadece iletişim kanalını pasif olarak dinleyip (müdahale edilmeden) yeterince şifreli metin elde etmeye çalışır. Elde edilen şifreli metinler incelenerek anahtar hakkında bilgi edinilmeye çalışılır.
- Bilinen Açık Metin Saldırısı (Known Plaintext Attack): Bir miktar açık-şifreli metin çifti bilinerek yapılan saldırıdır. Pasif bir saldırı tipidir. Mesajların bir kısmı tahmin edilebilir veya açık gönderilen mesajlar toplanarak saldırı uygulanabilir. Doğrusal kriptanaliz en tipik örneklerinden biridir.
- Seçilmiş Açık Metin Saldırısı (Chosen Plaintext Attack): Aktif bir saldırı tipidir. Analizcinin istediği (seçtiği) veriyi şifreleme imkânına sahip olduğu kabul edilen

saldırı senaryosudur. Analizci şifreleme algoritmasının güvenli olarak yerleştirildiği mekanizmayı elde edebilir. Analizci aktif olarak haberleşme sisteminde rol alır. Bu tür saldırının tipik bir örneği diferansiyel kriptanalizdir.

- Seçilmiş Şifreli Metin Saldırısı (Chosen Ciphertext Attack): Şifre çözme makinasına ulaşılarak yapılan saldırı çeşididir. Bir önceki senaryoya benzemektedir.
- Uyarlamalı Açık veya Kapalı Metin Saldırısı (Adaptive Chosen Plaintext or Ciphertext Attack): Bu saldırı senaryosunda analizcinin istediği mesajı açma veya kapatma konusunda sınırsız kapasiteye sahip olduğu kabul edilir. Önceki iki senaryonun teorik olarak daha güçlendirildiği saldırı çeşididir. Böyle bir saldırının en tipik örneği Wagner'in boomerang saldırısıdır.
- İlişkili Anahtar Saldırısı (Related-Key Attack): Bu saldırı türünde saldırgan şifreleme ve şifre çözmede kullanılan anahtarlar arasında matematiksel bir ilişkiyi bilmekte veya seçebilmekte olup anahtarların değerlerini bilmemektedir.

2.4.2 Kriptanaliz Saldırılarının Amaçları

Saldırı sırasında elde edilen bilgiye göre kriptanaliz saldırılarının amaçları aşağıdaki gibi sınıflandırmıştır:

- Tamamen Kırma (Total Break): Saldırgan şifreleme algoritmasının gizli anahtarını elde eder.
- Evrensel Türetim (Global Deduction): Saldırgan gizli anahtarın asıl değerini bilmeden şifreleme veya şifre çözme algoritmalarına eşdeğer bir algoritma bulur. Evrensel türetim blok şifreleme algoritmalarının blok yapıları içerdiği durumlarda olasıdır. Örneğin şifreli metnin belirli bir bölümünün, açık metnin belirli bölümünden tamamen bağımsız olduğu durumlarda uygulanabilir. Böyle bir blok şifreleme algoritması anahtar uzunluğunu önemsenmeksizin bilinen açık metin saldırılarında evrensel türetim yöntemine karşı zayıftır. Başka bir saldırıda döngü alt anahtarları evrensel türetim ile elde edilebilir. Bu durumda anahtar planlama algoritmasında tek yönlü fonksiyonların kullanılması gereklidir.

- Yerel Türetim (Local Deduction): Saldırganın elde ettiği şifreli metinden açık metni, açık metni elde ettiyse şifreli metni bulmasıdır. Açık metin veya şifreli metin sayısı azsa yerel türetim, tümüyle kırma kadar tehlikelidir.
- Ayırt Edici Saldırı (Distinguishing Attack): Saldırgan şifreleme algoritmasının çıkışını düzgün (uniform) olarak rastgele seçilmiş bir permütasyon mu yoksa gizli anahtar tarafından belirtilmiş permütasyonlardan biri mi olduğunu söyleyebilir. Ayırt edici saldırı çok tehlikeli gibi görünmese de bazen tümüyle kırmayla sonuçlanan anahtar elde etme saldırılarına dönüşebilir.
- Bilgi Türetim Saldırısı (Information Deduction Attack): Saldırgan önceden bilmediği gizli anahtar, şifreli metin veya açık metin hakkında bazı bilgiler elde edebilir. Bilgi türetim açık metin ve şifreli metin düşük entropiye sahipse önemli bir sorundur.

2.4.3 Kriptanaliz Yöntemleri

Tipik kriptanaliz yöntemlerini aşağıdaki gibi sıralanabilir:

- Kaba Kuvvet Saldırısı (Brute Force Attack): Kaba kuvvet saldırısı, kriptolojik tasarımların analizinde uygulanabilecek en temel yöntemlerden biridir. Anahtar uzayını oluşturan tüm olası anahtarlar bilinen kısa açık/kapalı metin örnekleri üzerinde denenir. Doğru gizli anahtar bilinen açık bir metinden doğru şifreli metinin elde edilmesini sağlar. Günümüz hesaplama imkânlarına göre modern şifreleme sistemlerinin anahtar uzunlukların 128-bit ve yukarısı olması istenmektedir.
- Sözlük Saldırıları (Dictionary Attacks): Basit olmasına rağmen önemli bir saldırı çeşididir. Eğer şifrelenen metinlerin uzunlukları kısa ise saldıran birçok metin toplar ve farklı metinlerin tekrarlama analizini yapar.
- Eş Tanımlama (Equivalent Description): Bazen şifre sistemi tasarlayanlar sistemin veya parçalarının basit eşdeğer tanımlarını gözden kaçırmaları, bu saldırı tekniği tarafından kullanılmaktadır.

- Değişmezler için Devirlilik veya Arama (Periodicity or Search for Invariants): Değişmezler, şifreleme boyunca değişmeyen özellikler olarak düşünülebilir ve şifre sisteminin istenilmeyen bir özelliğidir. Eğer kriptanalist sistemin herhangi değişmezini yada yakınsamasını bulmayı başarırsa bir ayıran saldırı için malzeme edinmiş olur. Her çeşit devirli davranış veya şifrelenmeler arasındaki korelasyon mutlaka engellemelidir.
- Doğum Günü Paradoksu (Birthday Paradox): Blok şifreleme sistemlerinden açık anahtar şifre sistemlerine kadar uzanan sayılamayacak kadar önemli bir olasılık paradoksudur.
- Ortada Buluşma Saldırısı (Meet-in-the-Middle Attack): Bu yöntem şifreleme sistemini alt ve üst olmak üzere böler. Sonra kısmi tahmini ile yukarıdan ortaya ve baştan ortaya kısmi şifre çözme yapar. Sonuç karşılaştırılır ve eğer uyumlu ise aday anahtar saklanır. Aksi takdirde tahmin edilen anahtar yanlış olur.
- İstatiksel Yaklaşımlar (Statistic Approaches): Bu yöntemler şifreli ve açık metin arası ilişki veren istatiksel örnekleri arar. Bir tür ayıran saldırılar ve diğer ataklar için ilk adımdır. İstatiksel yaklaşımlar hem oluşması yüksek olasılıkta olayları hem de gerçekleşmesi imkânsız olayları bulmaya yöneliktir.
- Özel bir Atağa göre Zayıf Anahtarlar (Weak Keys with Respect to a Particular Attack): Bazı durumlarda bir zayıf anahtar kümesinin bir şifre sisteminin analizini özel bir saldırı modelini düşünüldüğünde kolaylaştırması mümkün olmaktadır. Eğer bir şifreleme sisteminin tüm anahtar uzayına göre yüksek bir oranda zayıf anahtarlara sahip ise tekrar tasarlanması bile söz konusu olabilir. Örnek olarak DES te dört tane zayıf ve on iki tane yarı-zayıf anahtar bulunmaktadır. Gizli anahtar k olmak üzere DES algoritmasını E_k olarak tanımlarsak dört tane zayıf anahtar için $E_k\big(E_k(m)\big) = m$ ve on iki tane yarı-zayıf anahtardan iki tanesi için $E_{k1}\big(E_{k2}(m)\big) = m$ sağlanmaktadır. IDEA blok şifre sistemi için 2^{128} anahtar uzayı üzerinde 2^{63} elemana sahip bir zayıf anahtar kümesi bulunmaktadır.

2.5 Özet

Bu bölümde modern kriptolojinin temelleri açıklanmaya çalışılmıştır. Bir kriptolojik sistem tasarlanırken sistemin tüm yönleriyle düşünülmesi gerektiği ve herhangi bir açıklığa imkân vermeyecek şekilde protokollerin tasarlanması gerektiği vurgulanmıştır. Protokol tasarım sürecinin zorluğu belirtilmiş ve güvenli bir sistem tasarlamak için kanıtlanabilir tasarım yaklaşımının ne kadar önemli olduğu gösterilmiştir. Son olarak kriptanaliz yaklaşımı açıklanmıştır.

BÖLÜM 3

KAOTİK DİNAMİKLER

Doğal olguların anlaşılması için yapılan çalışmalarda doğrusal olmayan sistemler önemli bir rol oynamaktadır. Doğrusal olmayan sistemlere olan ilgi son elli yılda oldukça artmıştır. Artan bu ilginin sebeplerinden biri kaos teorisinin keşfi olmuştur. Bilim çevrelerindeki en temel eğilimlerden biri; gerekirci sistemlerin zaman içindeki tüm davranışlarının başlangıç koşulları ve sistem denklemlerin verilmesi ile tahmin edileceği idi. Kaotik sistemlerin keşfi ile bu bakış acısı ortadan kalkmıştır [8-13]. Basitçe ifade edilecek olunursa kaotik sistemler gerekirci olmasına rağmen rasgele bir davranış göstermektedir. Garip davranış olarak da adlandırılan kaos teorisi sahip olduğu bu özelliklerinden dolayı doğrusal olmayan sistemlerle alakalı çalışmalarda ilgi odağı olmaktadır. Bu bölümde kaos kuramının tanımı, temel karakteristikleri ve kaos analiz yöntemleri verilmiştir.

3.1 Kaos Kuramı

Dinamik sistemlerin davranışları incelenirse genel olarak beş farklı durumla karşılaşılır [8-13, 21].

- Sistemin davranışı bir denge noktasına gidebilir. Denge noktası (equilibrium); akışın sabitlendiği ve öyle devam ettiği noktadır. Eğer sistem bu noktaya gelirse başka bir koşul olmadığı sürece orada kalır.
- Sistem periyodik bir davranış gösterebilir. Periyodik davranış; faz uzayındaki yörüngelerin aynı davranışı göstermesi olarak tanımlanır. Periyodik bir

yörüngenin akışı izlenirse kapalı bir yörünge görülür. Sistem aynı noktalar üzerinde sonsuza kadar tekrar eder

- Sistem periyodumsu (quasiperiodic) bir davranış gösterebilir. Farklı periyotlardan oluşan sistemlere periyodumsu sistemler denir.
- Sistemin cevabı sonsuza gidebilir.
- Sistem kaotik davranış gösterebilir.

Gelişigüzel ve tahmin edilemez davranış gösteren sistemlere kaotik sistemler denir. Kaosu tanımlayan en belirgin özellik, başlangıç şartları ve kontrol parametrelerine olan hassas bağımlılıktır. Bir kaotik sistem birbirine çok yakın noktalardan başlatıldığında sistemin izleyeceği yörüngeler tamamen birbiriyle ilişkisizdir. Bu yörüngeler gittikçe birbirinden uzaklaşır. Bu da sistemin rasgele benzeri bir davranış göstermesine sebep olmaktadır [8-13].

Tanım 3.1: Yörünge (orbit veya trajectory) faz uzayında bir başlangıç koşulundan başlayan ve sistemin dinamiğine göre hareket eden yol olarak tanımlanmaktadır.

Ancak kaotik sistemler matematiksel olarak gerekirci sistemlerdir, olasılıksal (stokastik) sistemler değildirler. Yani sistemin kaosa girme sebebi rasgele bir dış etki (gürültü vs.) değildir. Sistemin iç dinamiğidir.

Tanım 3.2: Gerekirci sistem; sistemin şimdiki durumunun, yalnızca geçmiş durumu kullanılarak belirlendiği sistemlerdir.

Ayrık zamanlı dinamik sistemler için fark denklemleri kullanılırken, sürekli zamanlı dinamik sistemler için ise diferansiyel denklemler kullanılır.

Tanım 3.3: Olasılıksal sistem; sistem çıkışının gelişigüzel olduğu veya şansa bağlı olduğu sistemlerdir.

Kaos kelimesi bazen karmaşıklık ve kargaşa olarak yanlış anlamlarda kullanılmaktadır. Kaos bir düzensizlik olarak görülmesine rağmen kaotik sistemler, birçok yeni düzenin ortaya çıkış nedeni olarak da görülmektedir. Karmaşıklık ve kargaşa olan sistemlerin,

kaotik sistemlerden farkları şunlardır; başlangıç koşullarına bağımlı değildirler ve hiçbir durumda kestirilemezler.

3.2 Kaotik Davranış için Gerek ve Yeter Koşullar

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.

Eğer sistem sürekli zamanlı bir dinamik sistem ise kaotik davranış için gerekli şartlar şunlardır:

- Sistem en az üç tane bağımsız dinamik değişkene sahip olmalıdır.
- Sistem denklemleri doğrusal olmayan bir terim içermelidir.

Eğer sistem ayrık zamanlı ise, sistemin doğrusal olmaması kaosun aranması için yeterlidir. Tek boyutlu ayrık zamanlı bir sistemde bile kaos aranabilir.

Yukarıda sayılan şartların varlığı sistemde kaosun var olduğu anlamına gelmez sadece kaosun varlığının olabileceği anlamına gelmektedir. Yani kaos için gerekli koşullardır fakat yeterli koşullar değildir. Kaosun gözlemlenebilmesi için yeterli koşul ise sistem uzayının sınırlı bir bölgede kalması koşulu ile başlangıç koşullarına hassas bağımlılıktır.

Başlangıç koşullarına hassas bağımlılık kaosun en ayırt edici özelliğidir. Sistem, çok küçük farklılıktaki iki komşu noktadan başlatıldığında bu etki kolaylıkla görülebilir. Başlangıç şartlarındaki bu çok küçük farkın sadece bir ölçüm hatası meydana getireceği düşünülebilir. Örneğin, kaotik olmayan bir sistemde bu belirsizlik, sonucun tahmininde zamanla doğrusal olarak artan bir hataya neden olur. Ancak kaotik sistemler için ise, bu fark, zamanla üstel olarak artar ve çok kısa bir zaman sonra sistemin durumu belirlenemez.

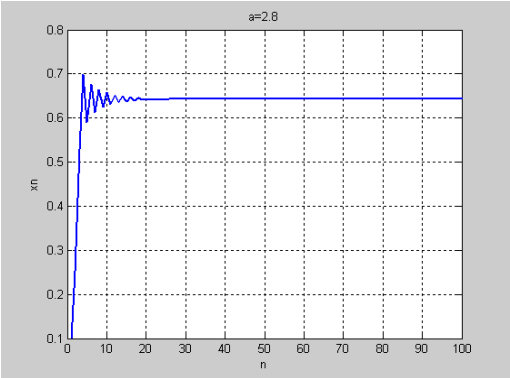
3.3 Kaos Analiz Yöntemleri

Kaos analizi için literatürde birçok farklı yöntem önerilmiştir. Bunlardan en yaygın olarak kullanılanları bu bölümde kısaca açıklanmıştır. Bu bölümde kaos analiz yöntemlerinin çalışma mantığını göstermek için en yaygın bilinen kaotik sistemlerden

biri olan lojistik harita kullanılmıştır. Lojistik haritaya ait dinamikler Denklem (3.1)'de verilmiştir.

$$x_{n+1} = ax_n(1 - x_n) \tag{3.1}$$

$0 \leq x_n \leq 1$ ve $0 \leq a \leq 4$ olmak koşuluyla, a parametresine göre sistem farklı davranışlar göstermektedir. $a = 2.8$ için sistem kaotik olmayan davranış göstermektedir. Bu parametre değeri için sistem bir denge noktasına gitmektedir. Şekil 3.1'de bu durum gösterilmiştir. $a = 4$ için ise sistem kaotik davranış göstermektedir. Bu durumda sistemin davranışı asla kendisini tekrar etmemektedir. Şekil 3.2'de ise $a = 4$ için sergilenen kaotik durum gösterilmiştir.



Şekil 3.1 $a = 2.8$ durumu için $x_n - n$ grafiği

3.3.1 Yörüngenin İzlenmesi Yöntemi

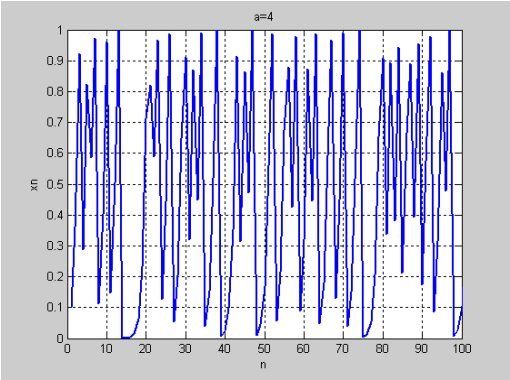
En basit analiz yöntemlerinden biridir. Sistemin durum değişkenlerinden herhangi biri zaman ekseninde gözlenerek sistemin kaosa girip girmediğine bakılabilir. Şekil 3.1 ve Şekil 3.2'de lojistik haritanın x_n durum değişkeninin yörüngesi verilmiştir.

3.3.2 Faz Uzayının İzlenmesi Yöntemi

Bu yöntemde, durum değişkenlerinin birbirine göre davranışları çizilerek sistemin kaosa girip girmediğine karar verilmektedir. Sistem periyodik ise, durum değişkenlerini birbirine göre çizdirildiğinde kapalı bir çevrim görülür. Buna limit çevrimi de denir ve sistemin periyodik davranış gösterdiği anlamına gelir. Sistemin davranışının düzensiz ve anlamsız bir şekil ile gösterilmesi ise kaosun olduğu anlamına gelmektedir.

3.3.3 Lyapunov Üstleri

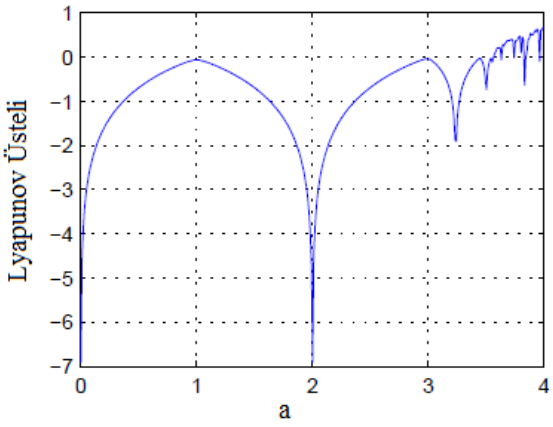
Bu yöntem, doğrusal sistemlerde kullanılan özdeğerlere (eigen value) benzetilir. Literatürde de özdeğerlerin doğrusal olmayan sistemlerdeki karşılığı olarak geçmektedir [8-13]. Başlangıçta iki komşu noktadan başlayan yörüngelerin, birbirinden hangi yönlerde ne kadar uzaklaşacağını belirleyen niceliksel bir yöntemdir. Dinamik sistem, sahip olduğu derece kadar Lyapunov üstüne sahiptir. Eğer sistemin tüm Lyapunov üstleri negatifse, yörüngeler her boyuttan birbirine yaklaşacaklardır. Yani sistem kaotik davranış göstermeyecektir. Fakat üstlerden en az biri pozitifse, yörüngeler pozitif olan üstün yönünde gittikçe birbirinden uzaklaşacaktır. Başlangıç şartları önemli olacak ve sistem doğal olarak kaotik davranış sergileyecektir. Lojistik harita tek boyutlu bir sistem olduğu için bir adet Lyapunov üstüne sahip. Bu değerin değişim Şekil 3.3'de verilmiştir.



Şekil 3.2 $a = 4$ durumu için $x_n - n$ grafiği

3.3.4 Poincare Haritalama Yöntemi

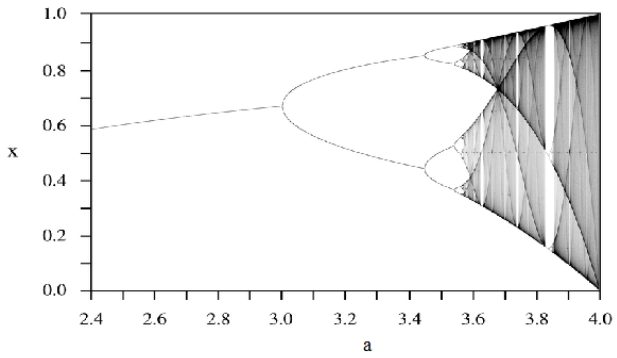
Aslında bu yöntem, n. dereceden sürekli zamanlı bir dinamik sistemi $(n-1)$. dereceden ayrık zamanlı bir dinamik sisteme dönüştürme işlemidir. Faz uzayı izlenirken belirli aralıklarla örnek alınarak elde edilir. Karmaşık sistemleri daha basit hale getirmek ve kararlılık analiz yapmak için elverişlidir. Periyodik bir davranış Poincare haritalama yöntemi ile incelenirse, sabit bir nokta görülür. Çünkü sistemin periyodu ile aynı zaman dilimlerinde örnekler alınırsa, hep aynı nokta alınacağından tek bir nokta görülür. Sistem periyodumsu, ise kapalı bir çevrim görülür. Fakat sistem kaotikse, kapalı olmayan, gelişigüzel bir fraktal şekil görülür.



Şekil 3.3 Lojistik harita için Lyapunov üstelinin değişimi

3.3.5 Güç Spektrumu ile Gösterim Yöntemi

Kaotik sinyaller geniş bantlı sistemlerdir. Dolayısıyla kaotik olan bir sinyalle, kaotik olmayan bir sinyal, güç spektrumuna bakarak ayrılabilir. Eğer sistem kaotikse, güç spektrumunda süreklilik vardır. Sistem kaotik değilse, sadece belli frekanslarda sıçramalar mevcuttur.



Şekil 3.4 Lojistik harita için çatallaşma diyagramı

3.3.6 Çatallaşma Diyagram Yöntemi

Bu yöntem, diğer yöntemlerden biraz farklıdır. y ekseninde durum değişkenlerinden birinin davranışı verilmektedir. x ekseninde ise parametrelerden birinin farklı değerleri verilmektedir. Şekil 3.4'de lojistik harita için a parametresindeki değişimin sistemin davranışını nasıl etkilediği çatallaşma diyagramı ile gösterilmiştir. Sistem periyodik davranış gösterdiği durumda grafikte tek çizgi, çift periyoda (periyodumsu) sahip

olduğu durumda grafikte çift çizgi ve sistemin kaosa girdiğinde bilmediğimiz kadar çok çizgi olduğu görülmektedir.

3.4 Özet

Klasik dönemdeki bilimsel yöntemler sistemlerdeki düzensiz, kararsız ve birbirleriyle bağlantısız gibi gözüken davranışları göz ardı etmiş, gürültü veya dış etki olarak adlandırmış ve tasarım yoluyla bunlardan kaçınmaya çalışmıştır.

Uygulamalı bilimdeki birçok araştırmacı, doğrusal olmayan sistemlerin zaman içerisindeki düzensiz ve kestirilemez davranışları ve anormallikleri açıklamak için kaostan faydalanmaktadır. Bu yüzden son yıllarda doğrusal olmayan sistemlerin kaotik davranışlarının incelenmesi birçok araştırmacının ilgisini çekmektedir.

Analizler sonucunda önceden açıklanmayan birçok bulgunun bilimsel açıklanması mümkün olmuştur. Bu sayede doğadaki birçok davranışın bilimsel bir temeli olduğu ortaya çıkmaktadır. Bilim ve mühendislikteki birçok yeni alanda araştırmalar yoğun olarak devam etmektedir.

BÖLÜM 4

KAOS TABANLI KRİPTOLOJİK SİSTEMLERİN GELİŞİMİ

Son yirmi yılda kaotik sistemlerin sahip olduğu özellikler kullanılarak kriptolojik sistemlerin tasarlanması birçok araştırmacının ilgisini çekmiştir. Araştırmacılar; kaotik sistemlerin rasgelelik kaynağı olarak sunmuş olduğu zengin dinamiklere odaklanarak çeşitli kriptolojik sistemler tasarlamıştır. Önerilen birçok tasarım çalışmasında kaotik sistemlerin en belirgin özelliği olan başlangıç koşulları ve kontrol parametrelerine aşırı bağımlığı sonucunda ortaya çıkan tahmin edilemez yörüngeler ile verinin gizlenmesi amaçlanmıştır [22, 26-28]. Önerilen algoritmaları daha karmaşık ve kırılması zor bir yapıya getirmek için tasarımlara çeşitli yapılarda (EKG sinyalleri, DNA işlemleri ve optimizasyon süreçleri gibi) eklenmiştir. Ancak yapılan kriptanaliz çalışmaları; tasarımlar yapılırken göz önünde bulundurulması gereken bazı temel kriterlere dikkat edilmediğini ve birçok algoritmanın kriptolojik olarak güvenli olmadığını basit saldırılarla göstermiştir [17-20].

Bu bölümde öncelikle kaos ve kriptoloji bilimleri arasındaki ilişki açıklanmıştır. Ardından kaos tabanlı kriptoloji alanında yapılan tasarım çalışmalarının karakteristikleri özetlenmiştir. Tasarım çalışmaları dört ana başlık altında toplanmıştır. Bunlar blok şifreleme algoritmaları, akan (stream) şifreleme algoritmaları, özetleme (hash) fonksiyonları ve son olarak tez çalışmasının temelini oluşturan görüntü şifreleme algoritmaları şeklinde sıralanmıştır. Kaos tabanlı açık anahtarlı şifreleme sistemleri ile ilgili tasarımlar tez konusunun dışında olduğundan bu tasarım çalışmalarına yer verilmemiştir.

4.1 Kaosun Kriptoloji için Uygunluğunun İncelenmesi

Bir şifreleme sistemin güvenli olarak nitelendirilebilmesi için karıştırma ve yayılma özelliklerini sağlaması gerektiği bilinmektedir. Kaotik sistemler kullanılarak kriptolojik sistemler tasarlanacak ise kaotik sistemlerin temel karakteristiklerin kriptolojik gereksinimler olan karıştırma ve yayılma özelliklerini sağladığı gösterilmelidir.

Karıştırma ve yayılma özellikleri dinamik sistemlerin sahip olduğu özelliklerdir. Kaotik sistemlerin başlangıç koşulları veya kontrol parametrelerine bağımlılığı bir kaotik sistemden üretilen yörüngeler boyunca yayılma özelliğini sağlar. Başka bir ifade ile herhangi bir yörünge üzerinde alınan her bir değer başlangıç koşulları veya kontrol parametrelerine bağımlıdır. Başlangıç koşulları veya kontrol parametrelerindeki en ufak bir değişiklik ile tamamen farklı yörüngeler oluşacağından bu bağımlılık çok güçlüdür. Sonuç olarak kaotik sistemler başlangıç koşulları veya kontrol parametrelerine bağımlılığı yayılma özelliğine sahiptir [22, 26-28].

Kaotik sistemlerin ergodiklik özelliği kaotik yörüngenin uzun vadeli davranışının başlangıç koşulları veya kontrol parametrelerine bağımlılığını ortaya koymaktadır. Buradan bir kaotik sistemden üretilen yörüngelerin bir kümesi ile istatistiki olarak başlangıç koşulları veya kontrol parametrelerinin tam değerlerinin çıkarılmasının mümkün olmadığı görülmektedir. Sonuç olarak kaotik sistemler karıştırma özelliğini sağlamaktadır [22, 26-28].

Özetleyecek olursak kaotik sistemlerin başlangıç koşullarına ve kontrol parametrelerine hassas duyarlılığı, doğrusal olmaması ve rasgele benzeri bir davranış göstermesi gibi özellikleri yeni kriptolojik sistemlerin tasarlanmasında kullanılabilir.

4.2 Kaos Tabanlı Kriptolojik Sistem Tasarım Çalışmaları

Kaos ve kriptoloji bilimleri arasındaki güçlü ilişkinin ortaya koyulmasının ardından literatürde burada listelenemeyecek kadar çok sayıda tasarım önerisi yayınlanmıştır. Bu yüzden bu bölümde ana tasarım kalıplarına kısaca değinilmiştir.

4.2.1 Kaos Tabanlı Blok Şifreleme Algoritmaları

Blok şifreleme algoritmaları temelde bir çarpım şifreleme sistemleridir. Çarpım şifreleme sistemleri bir dizi permutasyon ve yer değiştirme işlemlerini defalarca uygulayarak karıştırma ve yayılma gereksinimlerini sağlamaya çalışmaktadır. İteratif şifreleme sistemleri olarak da adlandırılan bu yapılarda orijinal veri sabit uzunlukta bloklara bölünür. Her bir veri bloğuna round fonksiyonu olarak adlandırılan işlemler uygulanır. Adım fonksiyonlarında ayrıca gizli anahtarından bir algoritma (anahtar planlama algoritması) aracılığı ile üretilen round anahtarları da kullanılmaktadır. Blok şifreleme algoritmaları bir şifreleme algoritması olmasının yanı sıra birçok tasarımda (akan şifreler, özet fonksiyonları ve rasgele sayı üreteçleri gibi) temel kriptolojik yapı taşı olarak da kullanılmaktadır. En iyi bilinen blok şifreleme algoritmalarına IDEA, DES, AES örnek olarak gösterilebilir [3-7].

Kaos tabanlı blok şifreleme algoritmaları ile ilgili yapılan tasarım çalışmaları [28-49] iki temel başlık altında toplanabilir. İlk grup tasarım çalışmalarında adım fonksiyonunda kullanılan yapıların kaotik sistemlerle değiştirilmesi ile şifreleme işlemi gerçekleştirilmiştir. İkinci grup tasarım çalışmalarında ise blok şifreleme sistemlerinin tasarımında önemli bir rol oynayan anahtar üreteci kaotik sistemler kullanılarak gerçekleştirilmiştir.

Tez çalışmasının başlangıç çalışmalarında blok şifreleme algoritmalarında önemli bir rol oynayan yerine koyma tablolarının (substitution box / S-box) kaotik sistemler kullanılarak tasarlanması çalışmalarına odaklanılmıştır. S-box DES, IDEA, AES gibi geleneksel blok şifreleme sistemlerindeki karıştırma özelliğini sağlayan doğrusal olmayan tek birleşendir. Bu yüzden güçlü şifreleme sistemlerinin tasarlanması için kriptolojik özellikleri iyi olan S-box'ların tasarlanması gerekmektedir. Matematiksel olarak $n\,x\,n$ boyutunda bir S-box $S:\{0,1\}^n \rightarrow \{0,1\}^n$ şeklinde doğrusal olmayan bir haritadır.

Yapılan ilk tasarım çalışmasında [35] S-box tasarımı için kaotik haritalar yerine sürekli zamanlı kaotik bir sistem olan Lorenz sisteminin kullanılabilirliği araştırılmıştır. Sistem yörüngesi oluşturulduktan sonra zaman ekseni üzerinde belirli aralıklarla örnekler alınarak sistem ayrıklaştırılmıştır. Ayrıklaştırma işleminin ardından çıkışlar bir

algoritmayla kodlanarak $8x8$ boyutunda bir S-box üretilmiştir. Önerilen yöntemin performans analizleri yapıldığında güçlü kriptografik özelliklere sahip olduğu kaos tabanlı diğer S-box'lar ile karşılaştırılarak gösterilmiştir. Algoritmanın detaylı yapısı aşağıda açıklanmıştır.

Adım 1. Lorenz sistemi seçilen başlangıç koşulları ve kaotik parametre değerleri için dört adımlı Runge-Kutta yöntemiyle çözülerek sistem yörüngeleri elde edilir.

Adım 2. Seçilen bir yörünge üzerinde (veri sayısı / 256) adımda bir örnekleme yapılır.

Adım 3. Alınan örnek değerlerine karşılık gelen çıkış değerleri sırayla 0'dan 255'e kadar kodlanır.

Adım 4. En küçük çıkış değerine karşılık gelen kod S-box'un ilk hücresi olmak üzere diğer çıkış değerlerine karşılık gelen kodlarda kullanılarak S-box oluşturulur.

Adım 5. S-box oluşturulduktan sonra satır bazında sola kaydırma işlemleri yapılır. İlk satırda kaydırma işlemi yapılmaz. Diğer satırlarda ise bir öncekinden bir fazla sayıdaki hücre sola kaydırılır.

Adım 6. Satılar kaydırıldıktan sonra sütün bazında döndürme yapılır. İşleme son sütundan başlanır Son sütün döndürülmez. Diğer sütunlar ise bir öncekinden bir fazla sayıdaki hücre döndürülür.

Bu tasarım çalışmasının ardından literatürde S-box tasarımında sürekli zamanlı sistemlerde yaygın şekilde kullanılmaya başlanmıştır. Yapılan ikinci tasarım çalışmasında çeşitli işlemlerle performansın nasıl geliştirilebileceği araştırılmıştır [159]. Son olarak zaman-gecikmeli kaotik sistemler kullanılarak bir tasarım çalışması gerçekleştirilmiştir [163]. Önerilen yeni tasarımda kaotik haritalara alternatif olabilecek zaman gecikmeli kaotik sistemleri temel alan yeni bir S-box tasarım algoritması önerilmiştir. Önerilen algoritma zaman gecikmeli kaotik sistemleri S-box tasarım algoritmasında kullanan ilk çalışmadır. Ayrıca önerilen algoritma basitlik ve verimlik (donanımda az yer kaplayarak hesaplanabilmesi) gibi kriterler göz önünde

bulundurulduğunda literatürdeki diğer algoritmalardan daha kullanışlıdır. Algoritmanın yapısı aşağıda detaylı olarak açıklanmıştır.

Adım 1. Belirlenen başlangıç koşulları ve kontrol parametreleri için zaman gecikmeli kaotik sistemin çıkışı hesaplanır.

Adım 2. Hesaplanan çıkış değeri A,$y_0y_1y_2y_3y_4y_5$ biçimindedir ve S-box tablosunun hücreleri virgülden sonraki 6 dijit kullanılarak hesaplanmaktadır.

Adım 3. Her adımda kaotik sistemin çıkışından belirlenen 6 dijit içerisinden 3 dijit seçilerek işleme devam edilir bu seçim aşağıdaki şekilde yapılır.

$$y_0y_1y_2 \rightarrow y_1y_2y_3 \rightarrow y_2y_3y_4 \rightarrow y_3y_4y_5 \rightarrow y_4y_5y_0 \rightarrow y_5y_0y_1 \rightarrow y_0y_1y_2$$

Adım 4. $y_py_qy_r$ şeklinde 3 dijit seçildikten sonra bu üç dijitin oluşturduğu decimal değerin 2^n'e göre kalanı (modu) hesaplanarak 0 ile 2^n arasındaki sayılara dönüştürülür.

Adım 5. Elde edilen sayı tabloda mevcut değilse tabloya eklenir. Aksi takdirde adım 1'e gidilerek yeni bir değer hesaplanır ve işleme devam edilir.

Adım 6. Tablodaki tüm hücrelerin değerleri hesaplanıncaya kadar adım 1'den işleme devam edilir.

Tasarlanan S-box yapılarının performans ölçütleri daha önceki kaos tabanlı tasarımlar ile karşılaştırıldığında daha iyi sonuçların elde edildiği görülmüştür. Ancak üretilen tablolar AES yerine koyma tablosu ile karşılaştırıldığında performans ölçütlerinin daha düşük olduğu görülmüştür. Bu sonuç kaosun kriptolojik uygulamalar için yeterli olup olmadığı sorusunu yeniden düşünmemiz gerektiğini ortaya çıkarmıştır. Bu doğrultuda tez çalışmasında kriptanaliz çalışmalarına ve kaosun rasgelelik özelliklerine odaklanılmıştır.

4.2.2 Kaos Tabanlı Akan Şifreleme Algoritmaları

Akan şifreleme sistemleri orijinal verinin her bir bit değerini bir birinden bağımsız olarak şifrelemektedir. Şifreleme işlemi için orijinal veri boyutunda bir anahtar dizisi üretilir. Anahtar dizisinin her bir bit değeri ile orijinal verinin her bir bit değeri iki tabanında toplanarak şifreli veri elde edilir. Akan şifreleme sistemleri eşzamanlı

(senkron) ve eşzamanlı olmayan (asenkron) olmak üzere iki temel sınıfa ayrılmaktadır. Eşzamanlı anahtar dizisi sadece şifreleme sisteminin gizli anahtarına bağımlı iken; eşzamanlı olmayan anahtar dizisi hem gizli anahtara hem de şifreli veriye bağımlıdır. Akan şifreleme sistemlerinin en büyük avantajı şifreleme sisteminin koşulsuz güvenli bir sistem olmasıdır. Çünkü uzunluğu n bit olan orijinal veriyi şifrelemek için n bitlik bir anahtar dizisi seçilir. Şifreli veriyi ele geçiren birisi olası bütün anahtarları (2^n) denese bile elinde n bitlik bütün kelimeler ve dolayısıyla birden fazla anlamlı veri olacağı için orijinal veriyi tahmin etmesi mümkün olmayacaktır. Ancak akan şifreleme sistemlerinin bu avantajlarına rağmen uzun bir veriyi şifreleyebilmek için uzun bir anahtar dizisinin üretilmesi gerekmektedir. Anahtarlar tek kullanımlık olduğu için her seferinde yeni bir anahtar üretmek, karşı tarafa iletmek ve saklamak bu sistemlerin en büyük dezavantajıdır [3-7].

Akan şifreleme sistemleri için anahtar dizisi önemli bir rol oynadığından birçok kaos tabanlı akan şifreleme sistemi için problem kaos tabanlı kriptolojik rasgele sayı üreteçlerinin tasarlanmasına dönüşmüştür [50-58]. Literatürde en yaygın tasarım kalıplarından biri Denklem (4.1)'de gösterildiği gibi basit bir niceleme algoritması kullanılarak kaotik sistem çıkışının istenilen değerlere dönüştürülmesi biçiminde olmuştur.

$$\begin{cases} 0 & f(x) < 0{,}5 \\ 1 & f(x) \geq 0.5 \end{cases} \tag{4.1}$$

Üretilen dizilerin kriptolojik karakteristiklerinin test edilmesi içini ise belirli istatistiki test yöntemleri kullanılmıştır [120-122].

Literatürdeki diğer yaygın tasarım kalıplarından bazıları aşağıdaki gibi listelenebilir.

- Akan şifreleme sistemi içerisindeki doğrusal olmayan fonksiyonların kaotik fonksiyonlar ile değiştirilmesi.
- Kaos tabanlı blok şifreleme algoritmaları kullanılarak tasarımların yapılması
- Kaos tabanlı oluşturulmuş kodlama tabloları aracılığıyla üreteçlerin tasarlanması

- Belirli kriptolojik yapılarla oluşturulmuş sistemlerin çıkışların kaotik sistemler aracılığı ile karıştırılması

4.2.3 Kaos Tabanlı Özetleme Fonksiyonları

Özetleme fonksiyonları bilgi güvenliğinde önemli bir yere sahiptir. Veri bütünlüğünün kontrol edilmesi için hata bulma fonksiyonlarında ve E-ticaret uygulamalarında sayısal imza planlarının gerçekleştirilmesi gibi uygulamada kullanılabilir. Bir özetleme fonksiyonu keyfi uzunluklu bir mesajı giriş olarak alır ve sabit uzunluklu özet değerini üretirler. Özetleme fonksiyonları anahtarlı ve anahtarsız olmak üzere iki sınıfa ayrılmaktadır. Özet değeri bazı zamanlar hash değeri veya mesaj özeti olarak da adlandırılmaktadır. Özet değeri mesajın tüm giriş bitlerini kullanarak üretilmektedir. Mesajda meydana gelecek bir bitlik bir değişim son özet değerinde büyük değişimlere neden olmalıdır [3-7].

Bir özetleme fonksiyonu $H: D \rightarrow R$ biçiminde tanımlanabilir. Burada D kümesinden alınan bir giriş değeri R kümesinde bir çıkış değerine eşleştirilir. Bu fonksiyon $|D| > [R]$ olmak üzere çoktan-bire tipinde bir ilişkiye sahiptir. Bir anahtarlı $h_k(.)$ özetleme fonksiyonunun güvenli olarak nitelendirilebilmeleri için aşağıdaki özellikleri sağlaması gerekmektedir. Bunlar:

- $h_k(.)$ fonksiyonu tek yönlüdür. Yani
    - Verilen k ve M için $h_k(M)$'in hesaplanması kolaydır.
    - k anahtar bilgisi bilinmeksizin $h_k(M)$ verildiği zaman M'i bulmak zordur.
    - k anahtar bilgisi bilinmeksizin, M verildiği zaman $hk(M)$'i bulmak zordur.
- $h_k(.)$ fonksiyonu karıştırma ve yayılma özelliklerini sağlamalıdır. Mesaj özet uzayı içerisinde mesaj özeti düzgün dağılmış olmalıdır. Bu istatistiksel saldırıları engellemektedir.
- $h_k(.)$ fonksiyonu çakışmadan bağımsız olmalıdır. Yani anahtar bilgisi olmaksızın iki farklı mesaj için çakışma bulmak zor olmalıdır.

- Doğum günü (Birthday) saldırılarına karşı $h_k(.)$ fonksiyonunun mesaj özeti en az 128 bit olmalıdır.
- Kaba kuvvet saldırılarına karşı $h_k(.)$ fonksiyonu yeterli anahtar uzayını sağlamalıdır.

Kaos tabanlı özetleme fonksiyonlarının tasarımına ilişkin literatürde birçok çalışma bulunmaktadır [59-70]. En yaygın kabul görmüş tasarım örneklerinden biri algoritmadaki sıkıştırma fonksiyonlarının kaotik sistemler kullanılarak gerçekleştirilmesidir. Bu tasarım kalıbında özet değeri üretilecek mesaj kaotik sistemin başlangıç koşulu olarak belirlenmektedir. Kaotik sistemler başlangıç koşullarına aşırı hassas olduklarından elde edilecek çıkışlar birbirinden farklı olacaktır.

4.2.4 Kaos Tabanlı Görüntü Şifreleme Algoritmaları

Literatürde kaos tabanlı şifreleme sistemlerinin en çok kullanıldığı tasarım çalışmaları kaos tabanlı görüntü şifreleme algoritmaları olmuştur [71-98]. Algoritmaların temel karakteristikleri kabaca aşağıdaki gibi özetlenebilir.

- Şifrelenecek görüntünün piksel pozisyonlarını kaotik sistem aracılığıyla yer değiştirmek.
- Şifrelenecek görüntünün piksel değerlerini kaotik sistem aracılığıyla değiştirmek.
- Kaotik sistemin iterasyonlarından faydalanılarak rasgele bir anahtar dizi üretmek ve bu anahtarlar ile piksel değerleri maskelemek.
- Şifreleme işleminde birden fazla kaotik sistem kullanmak.
- Birden fazla kaotik sistem kullanmak yerine kaotik sistemlerin kombinasyonuyla oluşturulmuş bir şifreleme algoritması kullanmak.
- Şifreleme sürecinin her bir adımında kullanılan kaotik sistemin başlangıç koşulları ve/veya kontrol parametrelerini pikselleri kullanarak değiştirmek.
- Piksellerin şifrelenmesi için daha önce şifrelenen piksellerin değerlerini kullanmak.

- Daha geniş anahtar uzayı üretebilecek kaotik sistemler kullanmak.
- Kaotik sistemlerin başlangıç koşulları ve/veya kontrol parametrelerini belirlemek için çeşitli cebirsel işlemler kullanmak. Bu yolla etkin anahtar uzayını artırmak.
- Klasik kaotik sistemler yerine uzaysal, hiper kaotik, zaman gecikmeli gibi daha kompleks kaotik sistemleri kullanmak.
- Algoritmada piksel bloklarını şifrelemek yerine bit bloklarını şifreleyen bir mimari benimsemek.

4.3 Kaos Tabanlı Kriptolojik Sistemlerin Kriptanalizi

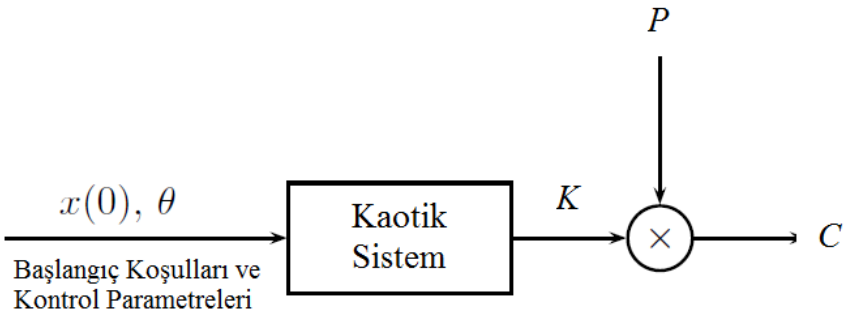
Bir önceki bölümde kaos ve kriptoloji bilimleri arasındaki güçlü ilişki kullanılarak birçok tasarımın yapılabileceği teorik olarak gösterilmiştir. Ancak iki disiplin arasında sadece bu ilişki üzerinden tasarımların yapılması yeterli değildir ve birçok zayıf öneriye sebep olmaktadır. Daha gürbüz, güvenli ve hızlı bir kriptolojik tasarım gerçekleştirebilmek için modern kriptolojik tasarım sürecine odaklanılmalıdır. Bölüm 2.3'de kriptolojik tasarım yaklaşımı detaylı olarak açıklanmıştır.

Kaos tabanlı kriptolojik tasarım çalışmaları kanıtlanabilir güvenlik tasarım sürecinin aksine kriptanaliz destekli bir tasarım sürecini benimsemiştir. Daha önce Bölüm 2.3.3'de kriptanaliz destekli tasarım sürecinin bazı problemleri açıklanmıştır. Ancak kaos tabanlı tasarımların asıl problemi kriptanaliz çalışmalarının çok basit bazı istatistiksel testler kullanılarak yapılması ve bunun neredeyse tüm çalışmalar için standart bir yaklaşım olarak benimsenmiş olmasıdır. Örnek olarak hemen hemen tüm kaos tabanlı görüntü şifreleme algoritmalarının diferansiyel ve lineer kriptanalizi için NPCR (number of pixels change rate) ,UACI (unified average changing intensity) ve histogram analizi gibi basit ve bütünü yansıtmayan ölçümlerin kullanması gösterilebilir.

Ayrıca birçok algoritmanın anahtar uzayının değerlendirmesinde sadece gizli anahtarı oluşturan parametre sayısı kullanılmış bu da etkin anahtar uzayının yanlış hesaplanmasına ve birçok algoritmanın kaba kuvvet saldırısına karşı dirençsiz olmasına sebep olmuştur.

Kriptanalist bakış açısıyla kaos tabanlı tasarımlara yaklaşıldığında birçok tasarımın Şekil 4.1'de gösterilen yapıda olduğu görülmektedir. Şekil 4.1'den kolayca görülebileceği gibi kaotik sistemin başlangıç koşulları ve kontrol parametreleri şifreleme sisteminin gizli anahtarı olarak kullanılmış ve kaotik sistemin iterasyonları sonucunda K gizli anahtarı üretilmiştir. Anahtar üretiminin ardından bu kaotik anahtarlar kullanılarak şifreleme işlemi gerçekleştirilmiştir.

Bu yapı içerisinde birçok araştırmacı kaotik sistemlerin rasgelelik kaynağı olarak sunmuş olduğu zengin dinamiklere odaklandığından bir kriptolojik sistem tasarlanırken göz önünde bulundurulması gereken temel kriterlere dikkat etmemişlerdir. Bu da birçok önerinin bilenen basit saldırılara karşı zayıf olmasına sebep olmuştur. Sonraki bölümde kaos tabanlı şifreleme sistemlerinin güvenlik analizi yapılırken dikkat edilmesi gereken genel durumlar kısaca açıklanmıştır.



Şekil 4.1 Kaos tabanlı şifreleme sistemlerinin genel görünümü

4.4 Kaotik Sistemlerin Bazı Genel Problemleri

Kaos tabanlı kriptolojik çalışmaların analiz eksikliğinden gelen problemlerine ek olarak değerlendirilmesi gereken diğer bir konu da kaotik sistemlerin sayısal bilgisayarlar üzerinde gerçekleştirilmesi ile sistemin kaotik davranışında meydana gelen değişmelerin kriptolojik sistemi olumsuz etkilemesidir.

Modern kriptolojik tasarımlar çalışma alanı olarak tamsayıların sonlu bir kümesini kullanırken kaotik sistemler reel sayıların bir kümesini kullanmaktadır. Bu yüzden sayısal bilgisayarlar üzerinde kaotik sistemlerin benzetimi yapılırken yuvarlama, kesme gibi işlemlerden dolayı bir sayısal kötüleşme meydana gelmektedir. Bu da kaostan beklenen rasgele benzeri bir davranış yerine periyodik bir davranış göstermesine sebep

olmakta ve sonuç olarak kriptolojik tasarıların temel gereksinimleri olan karıştırma ve yayılma özellikleri sağlanamamaktadır. Teorik ve pratik uygulamalar arasındaki bu etki önemli bir problem olduğu için ayrı bir bölüm olarak ele alınmıştır. Detaylar için Bölüm 6 incelenebilir.

4.5 Özet

Ağ ve iletişim teknolojilerindeki hızlı gelişmeler ile birlikte günlük yaşantımız büyük ölçüde sayısallaşmıştır. Sayısal ortamlarda kritik öneme sahip verilerin işlenmesi, depolanması ve iletilmesi ile bu verilerin güvenliğinin nasıl sağlanacağı sorusunu ön plana çıkarmıştır. Araştırmacılar güvenlik problemini çözebilmek için geleneksel kriptolojik çözümlere alternatif olabilecek etkili, hızlı ve gürbüz algoritmalar geliştirme arayışı içerisine girmiştir. Bu doğrultuda kaos tabanlı kriptoloji çalışmaları da son yirmi yılda önemli bir ilgi odağı olmuştur.

Kaotik sistemlerin doğrusal olmaması, gürültü benzeri periyodik olmayan bir davranış göstermesi ve başlangıç koşullarına hassas duyarlılığı gibi özellikleri kullanılarak kriptolojik protokollerin tasarlanması birçok araştırmacının ilgisini çekmiştir. Ancak protokollerin analiz çalışmaları ve kriptolojik tasarım süreci yeterince irdelenmediğinden birçok önerinin basit bilinen saldırılara karşı zayıf olduğu gösterilmiştir.

Kaotik kriptoloji için dikkat edilmesi gereken diğer bir nokta; iki disiplin arasındaki benzerliklerin yanı sıra farklılıklar da olduğudur. İki disiplin arasındaki en dikkat çekici ayrımlardan biri kaotik sistemlerin faz uzayının reel sayılar üzerinde tanımlı olmasına rağmen kriptolojik sistemlerin tam sayıların bir kümesini temel alarak tasarlanmasıdır. Dolayısıyla kaotik sistemler kriptolojik uygulamalarda kullanılacaksa bir ayrıklaştırma işlemine gereksinim duyulmaktadır. Ayrıklaştırma işlemi sonucunda bir sayısal kötüleşme meydana gelecektir.

Sonuç olarak kaotik sistemler yeni kriptolojik sistemlerin tasarımında kullanılacaksa hem iyi bir kriptanaliz çalışması yapılmalı hem de sayısal kötüleşmenin etkileri iyi incelenmelidir.

BÖLÜM 5

KAOS TABANLI ŞİFRELEME ALGORİTMALARININ GÜVENLİK ANALİZLERİ

Tez çalışmasının önemli katkılarından biri tüm kaos tabanlı kriptolojik sistemlerin güvenlik analizinde kullanılabilecek genel bir saldırı senaryosunun önerilmiş olmasıdır. Bu bölümde ilk olarak saldırı senaryosu verilmiş ardından bu saldırı senaryosu kullanılarak son zamanlarda önerilmiş 11 farklı kaos tabanlı şifreleme algoritmasının çeşitli zayıflıkları gösterilmiştir. Her bir şifreleme algoritması için öncelikle algoritmanın kısa bir tarifi yapılmış ardından algoritmanın güvenlik analizi verilmiştir.

5.1 Kaos Tabanlı Sitemler için Örnek Saldırı Senaryosu

Kriptolojik yapıların tasarımında kaotik sistemlerin temel birleşen olarak kullanılması durumunda şifreleme sisteminin güvenliğini değerlendirmek için sadece istatistiksel ve deneysel test yöntemleri kullanmak eksik bir analiz olacağından; kriptolojik olarak daha güçlü sistemler tasarlamak için aşağıdaki durumlar detaylı bir şekilde incelenmelidir.

Adım 1. Şifreleme mimarisinde kullanılan yapılar biçimsel bir matematiksel model ile ifade edilmelidir. Modelin daha basit eşitliklerle ifade edilip edilemeyeceği araştırılmalı varsa cebirsel bağımlılıklar ortaya çıkarılmalıdır.

Adım 2. Bir şifreleme sistemini güvenli olarak nitelendirebilmek için bilinen saldırılara karşı dirençli olduğu gösterilmelidir. Kerckhoffs prensibine göre; saldırganın şifreleme mimarisinde gizli anahtar dışında her şeyi bildiği varsayılmalı ve Bölüm 2.4.1'de verilen saldırı çeşitlerinden

kullanılabilecek olanları uygulanarak sistemin güvenliği değerlendirilmelidir.

Adım 3. Şifreleme algoritmasının güvenliği seçilen anahtar uzayına bağımlı olduğundan anahtar uzayı üzerinde yapılabilecek özelleştirmeler incelenmelidir. Anahtar tasarım algoritması matematiksel olarak ifade edilmeli, tasarımdan gelebilecek zayıf anahtarların varlığı araştırılmalıdır.

Adım 4. Şifreleme mimaride kullanılan kaotik sistemlerin topolojik özellikleri detaylı olarak incelenmelidir. Kriptolojik sistemlerin güvenli olması için gereksinim duyduğu karıştırma ve yayılma özellikleri şifreleme mimarisinde kullanılan sistemin kaotik rejimde bulunduğu durum ile sağlandığı unutulmamalıdır.

Adım 5. Kaotik sistemlerin sayısal bilgisayarlar üzerinde gerçekleştirildiğinde sayısal kötüleşmeden dolayı oluşabilecek problemler incelenmelidir. Çok güçlü kriptolojik yapılar kullanılsa bile en ufak bir açıklığın tüm sistemi etkileyeceği göz önünde bulundurularak tasarıma özel saldırılar araştırılmalıdır.

5.2 Zhu Şifreleme Algoritmasının Güvenlik Analizi

C. Zhu [123] hiper kaotik sistemleri kullanarak bir görüntü şifreleme algoritması önermiştir. Önerilen şifreleme algoritmasında hiper kaotik sistem aracılığıyla bir anahtar dizisi üretilmiştir. Üretilen kaotik anahtar dizisi iki aşamalı yayılma sürecinde kullanılarak görüntünün şifrelenmesi sağlanmıştır. Ancak şifreleme algoritmasının cebirsel bağımlılıklar içerdiği ve seçilen açık metin saldırısı uygulanarak algoritmanın gizli parametrelerinin nasıl elde edilebileceği gösterilmiştir [124].

5.2.1 Algoritmanın Tarifi

Şifreleme algoritması gizli anahtar olarak hiper kaotik sistemin başlangıç koşullarını kullanmaktadır. Kaotik sistemin hiper kaos göstermesi birden fazla pozitif Lyapunov üsteline sahip olmasından ortaya çıkmaktadır Seçilen hiper kaotik sistemin yapısı Denklem (5.1)'de verilmiştir. Denklem (5.1)'de verilen diferansiyel denklem sisteminde

a, b, c ve d sabit parametrelerdir. Burada $a = 35, b = 8/3, c = 55$ ve $d = 1.3$ olarak seçilmiştir. Şifreleme işlemi adım adım aşağıda açıklanmıştır.

$$\begin{cases} \dot{x} = a(y - x) + yz \\ \dot{y} = cx - y - xz + w \\ \dot{z} = xy - bz \\ \dot{w} = dw - xz \end{cases} \tag{5.1}$$

Adım 1. Şifrelenecek veri $L = MxN$ boyutlarında gri seviyeli bir görüntüdür. Burada M görüntünün satır sayısını N ise sütun sayısını göstermektedir. Başlangıçta iki boyutlu görüntü tek boyutlu vektöre dönüştürülür. $P = \{p_1, p_2, \dots, p_L\}$.

Adım 2. Denklem (5.1)'de verilen hiper kaotik sistemin iterasyonları sonucunda kaotik anahtar dizisi üretilir. $K = \{k_1, k_2, \dots, k_L\}$..

Adım 3. Yayılma işleminin ilk adımı için aşağıdaki işlemler uygulanır.

$$c_1 = p_1 \oplus (mod(C_0 + k_1, 256) \oplus k_1) \tag{5.2}$$

$$c_i = p_i \oplus (mod(c_{i-1} + k_i, 256) \oplus k_{i-1}),\ 2 \le i \le L \tag{5.3}$$

Adım 4. Yayılma işleminin ilk adımında elde edilen ara değerler yayılma işleminin ikinci adımında kullanılarak şifreli görüntü elde edilir.

$$c_1 = c_1 \oplus (mod(c_L + k_1, 256) \oplus k_1) \tag{5.4}$$

$$c_i = c_i \oplus (mod(c_{i-1} + k_i, 256) \oplus k_{i-1}),\ 2 \le i \le L \tag{5.5}$$

Adım 5. Bir boyutlu şifreli görüntü vektörü tekrar orijinal boyutlarına döndürülerek şifreli görüntü elde edilir.

5.2.2 Algoritmanın Kriptanalizi

Bir şifreleme algoritmasının tasarımında ne kadar güçlü kriptolojik yapılar kullanılsa da şifreleme mimarisindeki en ufak bir açıklık bütün şifreleme algoritmasının güvenliğini tehdit etmektedir. Bu yüzden bir şifreleme algoritması tasarlanırken öncelikle kullanılan yapı taşları matematiksel modeller ile ifade edilmeli ardından bu modellerin güvenli olduğu ispatlanmalıdır.

Kerckhoffs prensibine göre bir şifreleme algoritmasında gizli anahtar dışında her şey açık olmalıdır. Buna göre Denklem (5.2)'deki C_0 değeri gizli anahtar olmadığından

herhangi bir kişi bu değeri bilebilir. Algoritmada bu değer 3 olarak seçilmiştir. $K \in Z_{256}$ için *K* anahtarının alabileceği olası 256 farklı değer için $(mod(C_0 + k_1, 256) \oplus k_1)$ ifadesinin alabileceği tüm değerler hesaplanmıştır. Bu değerlerin küçükten büyüğe sırasıyla {3, 5, 7, 13, 15, 29, 31, 61, 63, 125, 127, 253} olduğu görülmüştür.

Saldırıda kullanılan diğer önemli bir özellik ise XOR işleminin birleşme özelliğinden gelmektedir. Denklem (5.6)'da XOR işleminin bu özelliği gösterilmiştir.

$$(a \oplus b) \oplus (c \oplus b) = (a \oplus c) \oplus (b \oplus b) = (a \oplus c) \oplus 0 = (a \oplus c) \quad (5.6)$$

Herhangi bir $P = \{p_1, p_2, \dots, p_L\}$. için $C = \{c_1, c_2, \dots, c_L\}$. değerlerini bildiğimizi varsayalım. Rahat anlaşılması için 2×2 boyutunda $(L = 4)$ küçük bir görüntünün şifreleneceğini varsayalım. Şifreleme algoritması için Kaynak [123]'de kullanılan gizli parametrelerinin aynısı seçilmiştir. Hiper kaotik sistem kullanılarak üretilen gizli anahtar dizisi $(137, 15, 14, 90)$ olarak hesaplanmıştır. Saldırıda açık görüntü olarak $(0, 0, 0, 0)$ piksel değerleri seçilmiştir. Şifreleme algoritması sonucunda şifreli görüntünün piksel değerleri $(245, 16, 181, 241)$ olarak elde edilmiştir.

Birinci adımda uygulanan yayılma süreci sonunda hesaplanan ara değerler aşağıdaki gibi hesaplanmıştır.

$$c_1 = 0 \oplus (mod(3 + k_1, 256) \oplus k_1) \quad (5.7)$$

$$c_2 = 0 \oplus (mod(c_1 + k_2, 256) \oplus k_1) \quad (5.8)$$

$$c_3 = 0 \oplus (mod(c_2 + k_3, 256) \oplus k_2) \quad (5.9)$$

$$c_4 = 0 \oplus (mod(c_3 + k_4, 256) \oplus k_3) \quad (5.10)$$

İkinci yayılma süreci sonunda hesaplanan şifreli görüntünün değerleri ise aşağıdaki gibi elde edilmiştir.

$$245 = c_1 \oplus (mod(c_4 \ + k_1, 256) \oplus k_1) \quad (5.11)$$

$$16 \ = c_2 \oplus (mod(245 + k_2, 256) \oplus k_1) \quad (5.12)$$

$$181 = c_3 \oplus (mod(16 \ + k_3, 256) \oplus k_2) \quad (5.13)$$

$$241 = c_4 \oplus (mod(181 + k_4, 256) \oplus k_3) \quad (5.14)$$

Denklem (5.12)'deki c_2 değeri için Denklem (5.8)'de hesaplanan değeri yerine yazarsak Denklem (5.15)'deki eşitliği buluruz. Denklem (5.6)'da gösterildiği gibi XOR işleminin birleşme özelliği kullanılarak eşitlik yeniden düzenlenirse son olarak Denklem (5.16) elde edilir.

$$16 = 0 \oplus (mod(c_1 + k_2, 256) \oplus k_1) \oplus (mod(245 + k_2, 256) \oplus k_1) \quad (5.15)$$

$$16 = mod(c_1 + k_2, 256) \oplus mod(245 + k_2, 256) \quad (5.16)$$

Denklem (5.16)'daki c_1 değerinin alabileceği farklı değerlerin sayısının 12 olduğunu daha önce gösterilmiştir. Olası (c_1, k_2) ikilileri Denklem (5.16)'da kullanılarak c_1 değeri tam olarak bulunur ($c_1 = 5$). c_1 değerinin bulunmasının ardından k_2 anahtarının değeri için ise Denklem (5.16) eşitliğini sağlayan birden fazla değer bulunur. Farklı açık metin şifreli metin çiftleri denenerek olası k_2 anahtar uzayı daraltılır. Yaklaşık 4 çift denenmesi sonucunda olası k_2 anahtarı sayısının iki olduğu görülmüştür. c_1 değerinin tam olarak bilinmesi ile k_1 anahtarı Denklem (5.7)'den çıkarılabilir. Saldırının bu aşaması sonucunda (c_1,k_1, c_2,k_2) gizli parametreleri açığa çıkarılmıştır. Bu parametreler diğer denklemlerde yerine yazılarak sistemin tüm gizli parametreleri açığa çıkarılabilir.

Bu saldırı senaryosunun yayınlanmasının ardından Li ve arkadaşları [125] önerilen saldırı mantığını matematiksel olarak ispat etmiş ve saldırı mantığını bir adım daha geliştirerek sadece bir adet açık/şifreli görüntü çifti kullanarak anahtarı elde etmiştir.

5.3 Chen Şifreleme Algoritmasının Güvenlik Analizi

Chen ve arkadaşları [126] EKG sinyalleri ve kaotik fonksiyonlarla verinin şifrelenmesini sağlayan bir şifreleme algoritması önermişlerdir. Chen algoritmasında metin ve görüntü verileri aynı anda şifrelenebilmektedir. Metin şifreleme için lojistik harita, görüntü şifreleme için ise Henon harita kullanılmıştır. Şifreleme algoritmasında kullanılan kaotik fonksiyonların başlangıç koşullarını belirlemek için kullanıcıdan toplanan EKG sinyallerinden yararlanılmıştır. Bu yolla şifreleme algoritmasının kişiselleştirilmesi amaçlanmıştır. Çeşitli istatistiksel testler ve deneysel sonuçlarla önerilen algoritmanın güvenlik analizi yapılmıştır.

Önerilen algoritmayı daha karmaşık ve kırılması zor bir yapıya getirmek için kaotik haritaların başlangıç koşullarının EKG sinyalleriyle belirlendiği bir süreç şifreleme

sistemine eklenmiştir. Ancak yapılan kriptanaliz çalışmasında şifreleme algoritmasının anahtar uzayının yeterli güvenlik düzeyini sağlayabilecek kapasitede olmadığı gösterilmiştir. Ayrıca seçilen açık metin saldırısı ile sadece bir açık/şifreli veri çifti ile algoritmanın gizli parametresi olan anahtarın elde edilebileceği gösterilmiştir.

5.3.1 Algoritmanın Tarifi

Bu bölümde analiz edilen şifreleme algoritmasının çalışması detaylı bir şekilde açıklanmıştır. Şifreleme algoritması iki temel kısımdan oluşmaktadır. İlk kısımda kullanıcılardan EKG sinyallerini toplamak için bir araç geliştirilmiştir. Bu araç aracılığıyla kullanıcının bireysel özelliklerinin EKG sinyallerinden çıkarımı yapılmaktadır. Şifreleme algoritmasının ikinci aşamasında EKG sinyallerinden çıkarılan bireysel özellikler kaotik fonksiyonların yörüngelerini üretmek için başlangıç koşulu olarak kullanılmaktadır. Şifreleme işlemi üretilen kaotik yörüngeler aracılığıyla verinin karılması işlemiyle gerçekleştirilmektedir. Algoritmanın çalışması adım adım aşağıda verilmiştir.

Adım 1. EKG çıkarım programı kullanılarak kullanıcının bireysel özelliklerini içeren EKG sinyalleri toplanır.

Adım 2. EKG sinyalleri kaotik haritaların başlangıç koşulu olarak kullanılarak kaotik yörüngeler elde edilir.

Adım 3. Kaotik yörüngelerin çıkışında elde edilen veriler şifreleme algoritmasının gizli anahtarı olarak kullanılır.

Adım 4. Şifrelenecek veri hem metin hem de görüntü verisi içeriyorsa bu veriler birbirinden ayrılır.

Adım 5. Görüntü verilerini şifrelemek için Henon harita kullanılır. İki boyutlu Henon map'in yörüngesi kullanılarak şifrelenecek görüntünün yatay ve dikey koordinatlarının karılması sağlanır.

Adım 6. Metin verilerinin şifrelenmesi için lojistik harita kullanılır. Şifreleme işlemi metin içerisindeki her bir karaktere karşılık gelen ASCII değerin lojistik haritayla karılmasıyla gerçekleştirilir.

Adım 7. Şifrelenmiş metin ve görüntü verilerinin birleştirilmesi ile şifreleme işlemi tamamlanır.

5.3.2 Algoritmanın Kriptanalizi

Öncelikle şifreleme algoritması Denklem (5.17)'de gösterildiği gibi basit bir matematiksel model ile ifade edilmiştir. Matematiksel modelde *E* şifreleme algoritmasını, *K* kaotik yörünge ile üretilen gizli anahtarı, *P* orijinal veriyi ve *C* şifrelenmiş veriyi göstermektedir. Analiz edilen algoritmada gizli anahtar olarak kaotik fonksiyonların kontrol parametreleri, başlangıç koşulu ve iterasyon sayısı kullanılmıştır. Ancak Denklem (5.17)'den görüldüğü gibi aslında şifreleme işleminin ne EKG sinyalleriyle nede kaotik fonksiyonların sistem parametreleri ile bağlantısı vardır. K parametresine sahip herhangi bir kişi bir veriyi şifreleyip şifresini çözebilir. Yani K parametresi şifreleme algoritmasının gizli anahtarına denktir. Bu durumda *K* verisinin nasıl elde edilebileceği araştırılmalıdır.

$$C = E(K, P) \tag{5.17}$$

K parametresinin elde edilebilmesi için seçilen açık metin saldırısı kullanılabilir. Seçilen açık metin saldırısında saldırgan özel seçtiği açık veriyi şifreleyerek şifreli veriyi elde eder. Açık/şifreli veri çiftlerini analiz ederek anahtarı elde etmeye çalışır. Tüm sembolleri aynı karakterden oluşan bir metin verisi veya tüm pikselleri aynı değere sahip olan bir görüntü için şifrelenmiş veriler elde edildiğinde K parametresi kolaylıkla elde edilebilir.

Şifreleme algoritmasının diğer bir zayıflığı algoritmada gizli anahtarları üreten kaotik haritaların kontrol parametrelerinin EKG verileri ile belirlenmesinden kaynaklanmaktadır. Hem lojistik harita hem de Henon harita belirli parametre değerleri arasında kaotik davranış göstermektedirler. EKG verilerinden elde edilen parametre değerlerinin kaotik davranış göstermemesi durumunda şifreleme algoritmasının temel gereksinimleri olan karıştırma ve yayılma özellikleri sağlanmayacaktır. Sonuç olarak açık/şifreli veriler arasındaki ilişki kolaylıkla ortaya çıkarılabilecektir. Bu tip bir durum çalışması daha önce Arroyo ve arkadaşları tarafından yapılmıştır. Detaylı analiz için Kaynak [127] incelenebilir.

5.4 Zhang Şifreleme Algoritmasının Güvenlik Analizi

Zhang ve arkadaşları [128] güvenli ve etkili görüntü şifreleme için bir algoritma önermişlerdir. Önerilen algoritmada şifreleme işlemi kaotik fonksiyonlar ve DNA toplama operatörü ile gerçekleştirilmiştir. Ancak yapılan kriptanaliz çalışmasında şifreleme algoritmasının etkin anahtar uzayının belirtilenden daha kısa olduğu gösterilmiştir.

5.4.1 Algoritmanın Tarifi

Şifreleme algoritmasında gizli anahtar olarak $(x_1, y_1, \mu_1, \mu_2, \mu_3, \mu_4)$ parametreleri kullanılmaktadır. (x_1, y_1, μ_1, μ_2) parametreleri Denklem (5.18)'de yapısı verilen iki boyutlu lojistik haritanın başlangıç koşulları ve kontrol parametrelerini göstermektedir. (x_1, y_1, μ_3, μ_4) parametreleri ise Denklem (5.19)'da yapısı verilen bir boyutlu iki farklı lojistik haritanın başlangıç koşulları ve kontrol parametreleridir.

$$\begin{cases} x_{i+1} = \mu_1 x_i(1 - x_i) + \gamma_1 y_1^2 \\ y_{i+1} = \mu_2 y_i(1 - y_i) + \gamma_2(x_i^2 + x_i y_i) \end{cases} \tag{5.18}$$

$$x_{n+1} = \mu x_n(1 - x_n) \tag{5.19}$$

Şifreleme algoritmasının işlem adımları aşağıda verilmiştir.

Adım 1. P açık görüntüsü $M \times N$ boyutlarında gri seviyeli bir görüntüdür. Görüntünün her bir pikseli bir byte ile gösterilmektedir. İlk olarak şifrelenecek görüntü binary matrise dönüştürülür. Ardından DNA kodlama kuralı kullanılarak binary matris DNA matrisine dönüştürülür. DNA matrisi *Ab* sembolü ile gösterilmektedir. DNA kodlama kuralı Çizelge 5.1'de gösterilmiştir.

Adım 2. DNA matrisi $4x4$ uzunluğunda eşit bloklara bölünür.

Adım 3. İki boyutu lojistik harita (x_1, y_1, μ_1, μ_2) başlangıç koşulları ve kontrol parametreleri kullanılarak itere edilir. Kaotik iterasyonlar sonucunda $X = \{x_1, x_2, \dots, x_{m/4}\}$ ve $Y = \{y_1, y_2, \dots, y_n\}$ gibi iki farklı kaotik dizi elde edilir.

Adım 4. Üretilen kaotik diziler sıralanarak iki farklı yeni dizi elde edilir (X' ve Y').

Adım 5. X dizisi içerisinde X' değerinin pozisyonu bulunarak $TX = \{tx_1, tx_2, \dots, tx_{m/4}\}$ dönüşüm matrisi elde edilir. Ab DNA matrisinin satırları *TX*'e göre yeniden sıralanır. Y dizisi içerisinde Y' değerinin pozisyonu bulunarak $TY = \{ty_1, ty_2, \dots, ty_n\}$ dönüşüm matrisi elde edilir. Ab DNA matrisinin sütunları *TY*'e göre yeniden sıralanır. Sonuç olarak Ab' dönüşüm matrisi elde edilir.

Adım 6. Ab ve Ab' matrislerine DNA toplama operasyonu uygulanarak $B(i,j)$.matrisi elde edilir. DNA toplama operasyonu Çizelge 5.2'de gösterilmiştir.

Adım 7. $B(i,j)$ blokları birleştirilerek $C(i,j)$ matrisi elde edilir.

Adım 8. Bir boyutlu iki farklı lojistik harita (x_1, y_1, μ_3, μ_4) başlangıç koşulları ve kontrol parametreleri ile kullanılarak $z_1(m,1), z_2(1, n \times 4)$ gibi iki farklı kaotik dizi üretilir. z_1, z_2 matrisleri çarpılarak $Z(m, n \times 4)$ matrisi elde edilir. Daha sonra Denklem (5.20)'de verilen $f(x)$ fonksiyonu kullanılarak binary dizi matrisi elde edilir.

$$f(x) = \begin{cases} 0, & 0 < x_n \leq 0.5 \\ 1, & 0.5 < x_n < 1 \end{cases} \tag{5.20}$$

Adım 9. $Z(i,j) = 1$ olduğu pozisyondaki $C(i,j)$ matrisinin değerinin tümleyeni alınır. Aksi taktirde bir değişiklik yapılmaz.

Adım 10. $C(i,j)$ matrisi DNA kodlama kuralı kullanılarak binary matrise çevrilir. Son olarak şifreli görüntü elde edilir.

Çizelge 5.1 DNA kodlama kuralı

Bit Değeri	**DNA Kod Değeri**
00	C
01	A
10	T
11	G

5.4.2 Algoritmanın Kriptanalizi

Şifreleme algoritmasının kriptanalizi için seçilen açık metin saldırısı kullanılmıştır. Saldırıda seçilen açık görüntünün tüm piksel değerlerinin aynı ve değerlerinin 0 olması gerekmektedir. Şifreleme algoritmasının ilk adımında piksel değerleri DNA kodlarına dönüştürülür. Seçilen görüntünün tüm piksel değerleri 0 olduğundan algoritmanın birinci adım çıkısında elde edilen Ab DNA matrisinin tüm elemanları C kod değerlerinden oluşmaktadır. Algoritmanın 3, 4 ve 5. adımlarında kaotik diziler aracılığıyla Ab DNA matrisinin satır ve sütunlarının karıştırılması sağlanmaktadır. Ab matrisinin tüm elemanları aynı değere sahip olduğundan satır ve sütun karıştırma işlemleri çıkışa bir etki yapmayacaktır ($Ab = Ab$'). Algoritmanın 6. adımında DNA toplama operasyonu gerçekleştirilmektedir. Ab ve Ab' matrislerinin tüm elemanları C kod değerlerinden oluştuğundan toplama işlemi sonucunda elde edilen $B(i,j)$ matrisinin de tüm elemanları C kod değerlerinden oluşacaktır. Algoritmanın 7. adımında $B(i,j)$ matrisinin blokları birleştirilerek $C(i,j)$ matrisi elde edilir. Algoritmanın 9. adımında şifreli görüntüyü elde etmek için; 8. adımında üretilen kaotik dizi aracılığıyla $C(i,j)$ matrisinin tümleyinin alınması işlemi gerçekleştirilmektedir.

Çizelge 5.2 DNA toplama operasyonu

+	**T**	**A**	**C**	**G**
T	C	G	T	A
A	G	C	A	T
C	T	A	C	G
G	A	T	G	C

Saldırı için seçtiğimiz açık görüntüye karşılık gelen şifreli görüntüyü bildiğimize göre şifreli görüntüye denk gelen $X(i,j)$ DNA matrisini elde edebiliriz. $C(i,j)$ ve $X(i,j)$ dizilerinin elemanları birer birer karşılaştırılır. Aynı ise 0 farklı ise 1 eklenerek algoritmanın 8. adımı çıkışındaki Z dizi elde edilir.

Z dizisi bir boyutlu iki farklı lojistik harita ile üretilmiştir. Bu diziyi üretmek için algoritmada (x_1, y_1, μ_3, μ_4) paramtereleri gizli anahtar olarak kullanılmıştır. Z dizisinin elde edilmesiyle gizli anahtarın bu kısmının bilinmesine gerek yoktur. Sonuç olarak gizli

anahtarı oluşturan parametre sayısı 6 dan 2'ye anahtar uzayı ise 10^{72}'den 10^{24}'e düşmüştür. Yeni anahtar uzayı güvenli iletişim için kabul edilebilir seviyede değildir

5.5 Wang Şifreleme Algoritmasının Güvenlik Analizi

Wang ve arkadaşları [129] kaos teorisini temel alan bir görüntü şifreleme algoritması önermişlerdir. Önerilen kaos tabanlı görüntü şifreleme algoritmasının temel mantığı bir grup kaotik harita yardımıyla üretilen sözde rasgele bir dizi aracılığıyla verinin şifrelenmesine dayanmaktadır. Şifreleme işlemi adım fonksiyonlarının defalarca uygulanması ile gerçekleştirilmektedir. Önerilen algoritma simetrik bir şifreleme algoritması olduğu için başlangıçta gönderici ve alıcı arasında bir gizli anahtar belirlenir. Anahtar uzunluğu adım sayısını etkilemektedir. Her bir adımda anahtar verisinin 8 bitlik kısmı kullanılmaktadır. Adım fonksiyonları iki kısımdan oluşmaktadır. İlk kısımda görüntüdeki piksellerin pozisyonu değiştirilmektedir. İkinci kısımda ise piksellerin değerleri değiştirilmektedir. Adım fonksiyonları ile karıştırma özeliği sağlanırken, adım fonksiyonlarının defalarca uygulanması ile yayılma özelliğinin sağlanması amaçlanmaktadır.

5.5.1 Algoritmanın Tarifi

Algoritmanın yapısı adım adım aşağıda verilmiştir.

Adım 1. Şifreleme işlemine başlanmadan önce gönderici ve alıcı arasında 128 bit'den kısa olmamak üzere bir gizli anahtar üzerinde anlaşır.

Adım 2. Algoritmada kullanılacak kaotik harita grubu belirlenir. Önerilen algoritmada kaotik harita grubu olarak üç farklı lojistik harita kullanılmıştır. Seçilen kaotik harita grubu için başlangıç koşulları Denklem (5.21) kullanılarak belirlenmektedir. Kaotik harita grubunun kontrol parametrelerinin $\mu = 4$ olduğu varsayılmıştır. Kaotik harita grubunun kaç kez itere edileceği ise Denklem (5.22) kullanılarak belirlenmektedir.

$$x_{i,0} = (A + key_{(k+i-1)\%(I/8)})/(key_{(k+i-1)\%(I/8)} + 255) \quad (5.21)$$

$$k_i = \begin{cases} A + key_{(k+i-1)\%(I/8)}, \ if \ A + key_{(k+i-1)\%(I/8)} \geq 200 \\ A + key_{(k+i-1)\%(I/8)} + 200, \ if \ A + key_{(k+i-1)\%(I/8)} < 200 \end{cases} \quad (5.22)$$

$$A = key_0 \oplus key_1 \oplus key_2 \oplus \ \dots \oplus key_{I/8-1}; k = 0,1,2, \dots, n-1 \quad (5.23)$$

Adım 3. Kaotik haritaların iterasyonu sonucunda elde edilen çıkışlar kullanılarak şifrelenecek görüntüdeki piksellerin pozisyonları değiştirilir. Bu işlem için Denklem (5.24) kullanılmaktadır.

$$\begin{cases} r = \left(x_{p1,t1} \times 10^{14} + C\right)\%H \\ g = \left(x_{p2,t3} \times 10^{14} + C\right)\%G \\ b = \left(x_{p3,t3} \times 10^{14} + C\right)\%(W/G) \end{cases} \quad (5.24)$$

$$C' = ROL(A, (A + key_k)\%8) \quad (5.25)$$

Adım 4. Kaotik haritalar bir kez daha itere edilir. Elde edilen çıkışlar Denklem (5.26) ve Denklem (5.27)'de kullanılarak bir T değeri hesaplanır. Denklem (5.28)'da gösterildiği gibi T değeri ile piksel değerine XOR işlemi uygulanarak şifreli görüntü elde edilir.

$$T = \begin{cases} r = \left(x_{p1,t1} \times 10^{14} + C\right)\%256, \ if \ P_{i,W/g\times j+k} \ kırmızı \ bileşen \\ g = \left(x_{p2,t3} \times 10^{14} + C\right)\%256, \ if \ P_{i,W/g\times j+k} \ yeşil \ bileşen \\ b = \left(x_{p3,t3} \times 10^{14} + C\right)\%256, \ if \ P_{i,W/g\times j+k} \ mavi \ bileşen \end{cases} \quad (5.26)$$

$$T = \left(x_{p,t} \times 10^{14} + C\right)\%256, p = 0,1,2, \dots \quad (5.27)$$

$$C_{r,W/G\times g+c} = P_{i,W/G\times j+k} \oplus \mathrm{T} \quad (5.28)$$

Adım 5. Tüm piksel değerleri şifreleninceye kadar her bir piksel için adım 3 ve 4 tekrarlanır.

Adım 6. Adım sayısına ulaşılıncaya kadar adım 2, 3 ve 4 tekrarlanır.

5.5.2 Algoritmanın Kriptanalizi

İlk olarak şifreleme mimarisini bir matematiksel model ile ifade edelim. Önerilen algoritma simetrik bir şifreleme algoritması olduğu için basitçe Denklem (5.29)'deki gibi ifade edilebilir. Matematiksel modelde *E* şifreleme algoritmasını, *K* gizli anahtarı, *P* orijinal veriyi ve *C* şifrelenmiş veriyi, R adım sayısını göstermektedir. Önerilen algoritmada anahtar uzunluğu ile adım sayısı arasında ilişki olduğu daha önce

belirtilmiştir. Kerckhoffs prensibine göre bir şifreleme algoritmasında anahtar dışında her şey açık olmalıdır. Algoritmanın anahtar uzunluğu bilineceğine göre adım sayısı parametresine gerek yoktur. Algoritmanın tasarım parametreleri arasında cebirsel bağımlılıkların bulunması göz çarpan zayıflıklardan biridir.

$$C = E^R(P, K) \tag{5.29}$$

Denklem (5.29)'de verilen E fonksiyonu Denklem (5.30)'daki gibi detaylandırılabilir. Denklem (5.30)'da f fonksiyonu görüntüdeki piksellerin pozisyonlarının değiştirilmesini, g fonksiyonu ise piksel değerlerinin değiştirilmesi işlemini temsil etmektedir.

$$E(P, K) = g(f(P, K), K) \tag{5.30}$$

Açık metin P, $N \times M$ boyutlarında gri skalalı bir görüntüdür. Her piksel bir bayt ile gösterilir. Görüntü satır satır taranarak $p \in S^n$ vektörü elde edilir. Burada $S = \{0,1, \dots ,255\}$ ve $n = NM$. Bu halde açık metin $p = [p_1, p_2, \dots, p_n]$.

Aslında f fonksiyonu; her bir renk kanalı (R,G,B) için farklı bir kaotik harita kullanılarak oluşturulmuş permütasyonlar aracılığıyla görüntünün karılması işlemini göstermektedir. Literatürde bu tip sadece permutasyon tabanlı şifreleme sistemleri için birçok saldırı gerçekleştirilmiştir. Kriptanaliz çalışmaları sonucunda, sadece permutasyon tabanlı şifreleme algoritmalarının bilinen/seçilen açık metin saldırısına karşı güvenli olmadığı gösterilmiştir. Açık metnin düzgün bir dağılım gösterdiği varsayımı için sadece $n = log_L(MN)$ bilinen/seçilen açık metin kullanılarak $O(n \cdot (MN)^2)$ hesapsal karmaşıklığında şifreleme algoritmasının kırılabileceği gösterilmiştir [130, 131].

Şifreleme mimarisinin sadece permutasyon tabanlı mimariye dönüştürülmesi için g fonksiyonun yapısının elde edilmesi gerekmektedir. Denklem (5.28)'den kolayca görülebileceği gibi şifreli görüntü g fonksiyonun çıkışıdır. f fonksiyonunun çıkış olan karılmış görüntü ise g fonksiyonunun giriş parametresidir. K parametresi tüm piksel değerleri 0 olarak seçilmiş özel bir açık görüntüye denk gelen şifreli görüntüsünün bilinmesiyle elde edilebilir. Tüm piksel değerleri 0 olduğundan karma işlemi bir şifreleme sürecine bir etki yapmayacaktır. 0 değeri XOR işlemi için etkisiz eleman olduğundan şifrelenmiş veri K parametresine eşit olacaktır. K parametresi elde

edildikten sonra herhangi bir şifreli görüntüyle K parametresi elde edilerek f fonksiyonun çıkışı olan karılmış görüntü elde edilebilir.

5.6 Liu Şifreleme Algoritmasının Güvenlik Analizi

Liu ve arkadaşları [132] DNA kodlama işlemi ve kaotik fonksiyonlar yardımıyla bir görüntü şifreleme algoritması önerisinde bulunmuşlardır. Algoritma içerisinde kullanılan yapılar ile kırılması zor bir şifreleme sistemi tasarımını amaçlamışlardır. Ancak yapılan kriptanaliz çalışması algoritmanın güvenli iletişim için yeterli güvenlik düzeyini sağlamadığını göstermiştir [161].

5.6.1 Algoritmanın Tarifi

Algoritmada gizli anahtar olarak $(x_0, x_1, \mu_0, \mu_1, key_1, key_2)$ parametreleri kullanılmaktadır. Gizli anahtardaki (x_0, x_1, μ_0, μ_1) parametreleri iki farklı lojiktik haritanın başlangıç değerleri ve kontrol parametreleridir. key_1, key_2 parametreleri ise DNA kodlama ve kod çözme kuralları için kullanılan anahtarlardır. Şifreleme algoritmasının çalışması aşağıda adım adım gösterilmiştir.

Adım 1. $m \times n$ boyutlarındaki renkli görüntünün her bir renk bileşeni binary bit dizisi matrisine dönüştürülür. $R(m, n \times 8), G(m, n \times 8)$ and $B(m, n \times 8)$.

Adım 2. key_1 anahtar değerinin gösterdiği DNA kodlama kuralı kullanılarak binary matrisler DNA matrislerine dönüştürülür. $Ar(m, n \times 4)$, $Ag(m, n \times 4)$ and $Ab(m, n \times 4)$.

Adım 3. Piksel değerleri arasındaki korelasyonu ortadan kaldırmak için farklı renk bileşenlerine DNA toplama işlemi uygulanır. DNA toplama işlemi sonucunda $Ar'(i,j), Ag'(i,j)$ ve $Ab'(i,j)$ matrisleri elde edilir. Hangi renk bileşenlerinin toplama işleminde kullanılacağı Denklem (5.31)'de gösterilmiştir.

$$Ar'(i,j) = Ar(i,j) + Ag(i,j)$$
$$Ag'(i,j) = Ag(i,j) + Ab(i,j) \quad (5.31)$$

$$Ab'(i,j) = Ag'(i,j) + Ab(i,j)$$

Adım 4. Birinci lojiktik harita gizli anahtarla belirlenen x_0 başlangıç değeri ve μ_0 kontrol parametresi kullanılarak $l = m \times n \times 4$ defa itere edilir. Kaotik iterasyon sonucunda elde edilen x_n kaotik dizisine Denklem (5.32)'de verilen $f(x)$ fonksiyonu uygulanarak $z(m, n \times 4)$ binary matrisi elde edilir. $z(i,j) = 1$ olduğu pozisyondaki $Ar'(i,j), Ag'(i,j)$ ve $Ab'(i,j)$ matrislerinin elemanlarının tümleyeni alınır.

Adım 5. key_2 gizli anahtarının gösterdiği DNA kod çözme kuralı kullanılarak $Ar'(i,j), Ag'(i,j)$ ve $Ab'(i,j)$ DNA matrisleri binary matrislere dönüştürülür. $R'(m, n \times 8), G'(m, n \times 8)$ and $B'(m, n \times 8)$.

Adım 6. İkinci lojiktik harita gizli anahtarla belirlenen x_1 başlangıç değeri ve μ_1 kontrol parametresi kullanılarak $l = m \times n$ defa itere edilir. Kaotik iterasyon sonucunda elde edilen $\{0,1\}$ arasındaki değerler $\{0,1,2, \dots ,255\}$ aralığına eşleştirilerek $c(m, n \times 8)$ matrisi elde edilir.

Adım 7. R', G' ve B' matrisleri ile $c(m, n \times 8)$ matrisine XOR uygulanarak R'', G'' ve B'' matrisleri elde edilir. Son olarak elde edilen R'', G'' ve B'' bileşenleri elde edilerek şifreli görüntü elde edilir.

5.6.2 Algoritmanın Kriptanalizi

Analiz edilen şifreleme algoritmasının güvenliği algoritmada kullanılan iki farklı kaotik haritanın başlangıç koşulları ve kontrol parametrelerine bağımlıdır. Şifreleme sistemine yapılabilecek en basit saldırılardan biri bu gizli parametrelerin açığa çıkarılması olabilir. Fakat bu parametre değerlerini açığa çıkarmak yerine bu parametre değerleri kullanılarak üretilen kaotik dizilerin açığa çıkarılması daha mantıklı bir analiz olabilir. Üretilen kaotik dizileri bilen biri istediği herhangi bir veriyi şifreleyebilir veya şifresini çözebilir. Önerilen görüntü şifreleme algoritmasına yapılan saldırıda bu kaotik dizilerin açığa çıkarılması amaçlanmıştır.

Algoritmanın analizinde kullanılacak görüntülerin R, G ve B bileşenlerinin tüm piksel değerlerinin aynı olması istenmektedir. Saldırı için dört farklı özel görüntü kullanılmıştır. Bu görüntülerin tüm piksel değerleri sırasıyla 0, 85, 170 ve 255

değerlerinden oluşmaktadır. Seçilen dört farklı görüntü ve olası key_1 ve key_2 anahtarları için elde edilecek şifreli görüntülerin yapısı sırasıyla Çizelge 5.3, Çizelge 5.4, Çizelge 5.5 ve Çizelge 5.6'da verilmiştir. Tabloların önemli bir özelliği şifreleme algoritmasında kullanılan diğer gizli parametrelerden bağımsız olmasıdır. Tablonun her bir hücresinde gösterilen üçlüler şifreli görüntünün R, G ve B bileşenlerini göstermektedir. Tablolarda kullanılan a, b, c ve d sembolleri farklı matrisleri göstermektedir. ($d = a'$ ve $c = b'$). Her bir matrisin boyutu $m \times n$ dir.

Çizelge 5.3 $P = 0$ ve olası key_1, key_2 için şifreli görüntülerin yapısı

$P = 0$		**Key1**							
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Key2	**1**	(a,a,b)	(a,a,b)	(c,c,c)	(c,c,c)	(b,b,b)	(b,b,b)	(c,c,a)	(c,c,a)
	2	(a,a,c)	(a,a,c)	(c,c,c)	(c,c,c)	(c,c,c)	(c,c,c)	(b,b,a)	(b,b,a)
	3	(b,b,a)	(b,b,a)	(d,d,d)	(d,d,d)	(a,a,a)	(a,a,a)	(d,d,b)	(d,d,b)
	4	(c,c,a)	(c,c,a)	(d,d,d)	(d,d,d)	(a,a,a)	(a,a,a)	(d,d,c)	(d,d,c)
	5	(b,b,d)	(b,b,d)	(a,a,a)	(a,a,a)	(d,d,d)	(d,d,d)	(a,a,b)	(a,a,b)
	6	(c,c,d)	(c,c,d)	(a,a,a)	(a,a,a)	(d,d,d)	(d,d,d)	(a,a,c)	(a,a,c)
	7	(d,d,b)	(d,d,b)	(c,c,c)	(c,c,c)	(c,c,c)	(c,c,c)	(c,c,d)	(c,c,d)
	8	(d,d,c)	(d,d,c)	(c,c,c)	(c,c,c)	(c,c,c)	(c,c,c)	(b,b,d)	(b,b,d)

Çizelge 5.4 $P = 85$ ve olası key_1, key_2 için şifreli görüntülerin yapısı

$P = 85$		**Key1**							
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Key2	**1**	(c,c,c)	(b,b,b)	(a,a,b)	(c,c,a)	(a,a,b)	(c,c,a)	(c,c,c)	(b,b,b)
	2	(b,b,b)	(c,c,c)	(a,a,c)	(b,b,a)	(a,a,c)	(b,b,a)	(b,b,b)	(c,c,c)
	3	(d,d,d)	(a,a,a)	(b,b,a)	(d,d,b)	(b,b,a)	(d,d,b)	(d,d,d)	(a,a,a)
	4	(d,d,d)	(a,a,a)	(c,c,a)	(d,d,c)	(c,c,a)	(d,d,c)	(d,d,d)	(a,a,a)
	5	(a,a,a)	(d,d,d)	(b,b,d)	(a,a,b)	(b,b,d)	(a,a,b)	(a,a,a)	(d,d,d)
	6	(a,a,a)	(d,d,d)	(c,c,d)	(a,a,c)	(c,c,d)	(a,a,c)	(a,a,a)	(d,d,d)
	7	(c,c,c)	(b,b,b)	(d,d,b)	(c,c,d)	(d,d,b)	(c,c,d)	(c,c,c)	(b,b,b)
	8	(b,b,b)	(c,c,c)	(d,d,c)	(b,b,d)	(d,d,c)	(b,b,d)	(b,b,b)	(c,c,c)

Çizelge 5.5 $P = 170$ ve olası key_1, key_2 için şifreli görüntülerin yapısı

$P = 170$		**Key1**							
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Key2	**1**	(b,b,b)	(c,c,c)	(c,c,a)	(a,a,b)	(c,c,a)	(a,a,b)	(b,b,b)	(c,c,c)
	2	(c,c,c)	(b,b,b)	(b,b,a)	(a,a,c)	(b,b,a)	(a,a,c)	(c,c,c)	(b,b,b)
	3	(a,a,a)	(d,d,d)	(d,d,b)	(b,b,a)	(d,d,b)	(b,b,a)	(a,a,a)	(d,d,d)
	4	(a,a,a)	(d,d,d)	(d,d,c)	(c,c,a)	(d,d,c)	(c,c,a)	(a,a,a)	(d,d,d)
	5	(d,d,d)	(a,a,a)	(a,a,b)	(b,b,d)	(a,a,b)	(b,b,d)	(d,d,d)	(a,a,a)
	6	(d,d,d)	(a,a,a)	(a,a,c)	(c,c,d)	(a,a,c)	(c,c,d)	(d,d,d)	(a,a,a)
	7	(b,b,b)	(c,c,c)	(c,c,d)	(d,d,b)	(c,c,d)	(d,d,b)	(b,b,b)	(c,c,c)
	8	(c,c,c)	(b,b,b)	(b,b,d)	(d,d,c)	(b,b,d)	(d,d,c)	(c,c,c)	(b,b,b)

Çizelge 5.6 $P = 255$ ve olası key_1, key_2 için şifreli görüntülerin yapısı

$P = 255$		**Key1**							
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Key2	**1**	(c,c,a)	(c,c,a)	(b,b,b)	(b,b,b)	(c,c,c)	(c,c,c)	(a,a,b)	(a,a,b)
	2	(b,b,a)	(b,b,a)	(c,c,c)	(c,c,c)	(c,c,c)	(c,c,c)	(a,a,c)	(a,a,c)
	3	(d,d,b)	(d,d,b)	(a,a,a)	(a,a,a)	(d,d,d)	(d,d,d)	(b,b,a)	(b,b,a)
	4	(d,d,c)	(d,d,c)	(a,a,a)	(a,a,a)	(d,d,d)	(d,d,d)	(c,c,a)	(c,c,a)
	5	(a,a,b)	(a,a,b)	(d,d,d)	(d,d,d)	(a,a,a)	(a,a,a)	(b,b,d)	(b,b,d)
	6	(a,a,c)	(a,a,c)	(d,d,d)	(d,d,d)	(a,a,a)	(a,a,a)	(c,c,d)	(c,c,d)
	7	(c,c,d)	(c,c,d)	(c,c,c)	(c,c,c)	(c,c,c)	(c,c,c)	(d,d,b)	(d,d,b)
	8	(b,b,d)	(b,b,d)	(c,c,c)	(c,c,c)	(c,c,c)	(c,c,c)	(d,d,c)	(d,d,c)

Çizelge 5.3 ve Çizelge 5.6'da $P \in \{0, 255\}$ ve $key_1 \in \{3, 4, 5, 6\}$ için R, G ve B bileşenleri aynıdır. Benzer şekilde Çizelge 5.4 ve Çizelge 5.5'de $P \in \{85, 170\}$ ve $key_1 \in \{1, 2, 7, 8\}$ için R, G ve B bileşenleri aynıdır. Ek olarak $key_1 \in \{3, 4\}$, $key_1 \in \{5, 6\}$, $key_1 \in \{1,\ 2\}$, ve $key_1 \in \{7, 8\}$ için aynı sonuçların üretildiği görülmüştür. Sonuç olarak açık görüntünün R, G ve B bileşenlerinin piksel değerlerinin aynı olup olmaması incelenerek key_1 anahtar uzayı olası sekiz farklı durumdan iki farklı duruma indirgenebilir.

Şifreli görüntüde R, G ve B bileşenlerinin aynı olduğu durumları kullanarak şifreleme algoritmasının ikinci adımı olan piksel değerlerinin DNA kodlarına dönüştürüldüğü adım çıkışının C veya G kodlarından biri olduğu da söylenebilir. Çünkü şifreleme algoritmasının üçüncü adımı olan DNA kodu toplama işleminde sadece C ve G kodlarının kendisiyle toplanması yine aynı değerleri verir. Dolayısıyla şifreli görüntülerde R, G ve B bileşenleri aynı olduğu durum için şifreleme algoritmasının üçüncü adımı olan DNA kodu toplama işlemi sonucunda elde edilen kodların tamamının C veya G kod değerlerinden biri olacağı söylenebilir.

Algoritmanın dördüncü adımında birinci lojistik harita kullanılarak üretilen $z(i,j)$ dizisi ile tümleme işlemi yapılmaktadır. Bu adımda $z(i,j)$'de 1 olan değerlere karşılık gelen DNA kodlarının tümleyeni alınmaktadır. C kodlarının tümleyeni G ve G kodlarının tümleyeninin C olduğu algoritmada belirtilmiştir.

Algoritmanın beşinci adımında ise key_2 kullanılarak DNA kodları piksel değerlerine dönüştürülmektedir. Her bir piksel değeri 0 ile 255 arasında olduğu için 8 bit ile ifade edilmektedir. Her bir DNA kodu ise 2 bit ile ifade edildiğinden bir piksel dört DNA kodundan oluşturmaktadır. DNA kodları için C veya G kod değeri olmak üzere iki farklı olasılık mümkündür. C ve G kodları birbirinin tümleyeni olduğu ve ardışık iki kod değeri kendisinden önceki kodun aynısı yada tümleyeni olacağı için ardışık iki kod sözcüğü arasındaki Hamming mesafesi 0 veya 2 olacaktır.

Algoritmanın altıncı adımında ikinci lojistik harita kullanılarak üretilen $c(m, n \times 8)$ dizisi ile beşinci adım çıkışı olan piksel değerlerine XOR işlemi uygulanmaktadır. $c(m, n \times 8)$ dizisinin her bir elemanı 0 ile 255 arasında değişen bir sayı dizisidir. Bu adım çıkışında şifreli görüntüler elde edilmektedir.

Seçilen açık metin saldırısı sonucunda şifreli görüntü değerlerini bildiğimize göre; bu değerlere olası 256 farklı anahtar değeriyle XOR işlemi uygulayarak beşinci adım çıktısındaki değerleri bulmaya çalışırız. Her bir piksel için olası 256 farklı anahtar değeri için 256 farklı sonuç elde ederiz. Her bir piksel için olası anahtar uzayını daraltmak için elde ettiğimiz piksel değerini 8 bit olarak ifade ederiz. Her bir sekiz biti iki bitlik gruplara ayrılır. Çünkü her bir piksel değeri 2 bit uzunluğunda dört DNA kodundan oluşmaktadır. Her bir iki bitlik grup arasındaki Hamming mesafesi hesaplanır. Gruplar arasındaki mesafe 0 veya 2'den farklı olan piksel değerlerini veren anahtar değerleri elenir. Anahtar uzayını daha küçültmek için ikinci aşamada R, G ve B bileşenlerinin seçilen hangi piksel değerleri için aynı olduğuna göre iki farklı durum incelenir. İlk durumda tüm piksel değerleri 0 veya 255 olan görüntüler için R, G ve B bileşenleri aynı ise iki bitlik gruplarda her bir grubu oluşturan iki bitin bir birinden farklı ise bu durumu sağlayan piksel değerlerini veren anahtarlar elenir. İkinci durumda ise tüm piksel değerleri 85 veya 170 olan görüntüler için R, G ve B bileşenleri aynı ise iki bitlik

gruplarda her bir grubu oluşturan iki bit aynı ise bu durumu sağlayan piksel değerlerini veren anahtarlar elenir.

5.6.3 Benzetim Sonuçları

Seçilen açık metin saldırısı için açık metin olarak R, G ve B bileşenlerinin tüm piksel değerleri 0, 85, 170 ve 255 değerlerinden oluşan görüntülerinin şifrelenmiş biçimleri sırasıyla Denklem (5.32), (5.33), (5.34) ve (5.35)'de verilmiştir.

$$\begin{aligned} R'' &= [120,\ 8,\ \ 116,\ 196] \\ G'' &= [120,\ 8,\ \ 116,\ 196] \\ B'' &= [210,\ 162,\ 222,\ 110] \end{aligned} \tag{5.32}$$

$$\begin{aligned} R'' &= [120,\ 8,\ 116,\ 196] \\ G'' &= [120,\ 8,\ 116,\ 196] \\ B'' &= [120,\ 8,\ 116,\ 196] \end{aligned} \tag{5.33}$$

$$\begin{aligned} R'' &= [135,\ 247,\ 139,\ 59] \\ G'' &= [135,\ 247,\ 139,\ 59] \\ B'' &= [135,\ 247,\ 139,\ 59] \end{aligned} \tag{5.34}$$

$$\begin{aligned} R'' &= [210,\ 162,\ 222,\ 110] \\ G'' &= [210,\ 162,\ 222,\ 110] \\ B'' &= [135,\ 247,\ 139,\ 59] \end{aligned} \tag{5.35}$$

Seçilen görüntülerin şifreli biçimleri incelenirse R, G ve B bileşenlerinin 85 ve 170 durumları için aynı piksel değerlerini aldığı görülmektedir. Bu durumda $key_1 \in \{1,2,7,8\}$ olacaktır. Seçilen görüntülerden R, G ve B bileşenleri aynı olan iki görüntüye daha önce açıklanan anahtar uzayını azaltma algoritması uygulanarak olası $c(m, n \times 8)$ değerleri elde edilebilir. Anahtar uzayı azaltma algoritması uygulandıktan sonra

anahtar uzayının 256 farklı değerden 16 farklı değere düştüğü görülmüştür. Hesaplanan olası değerler Denklem (5.36)'da verilmiştir.

$$c(.) = \{17, 18, 29, 30, 33, 34, 45, 46, 209, 210, 221, 222, 225, 226, 237, 238\} \quad (5.36)$$

R, G ve B bileşenleri aynı olduğu durumlarda şifreleme algoritmasındaki DNA kodlarının sadece C veya G kod sözcüklerinden biri olduğunu bildiğimize göre elde ettiğimiz $c(m, n \times 8)$ değerlerine karşılık gelen $z(i, j)$değerlerini de kolayca elde edebiliriz.

Saldırının bu aşamasında anahtar şifreleme algoritmasının gizli anahtarları olan kaotik $z(i, j)$, $c(m, n \times 8)$ ve key_1 değerleri için azaltılmış bir anahtar uzayına sahibiz. Anahtar uzayının azaltılmış bu alt kümesi üzerinde kaba kuvvet saldırısı başarılı bir şekilde uygulanarak anahtar değeri tam olarak bulunabilir.

5.7 Bigdeli Şifreleme Algoritmasının Güvenlik Analizi

Bigdeli ve arkadaşları [133] görüntü şifreleme algoritması için Hopfield sinir ağı ve Arnold Cat harita kaotik sisteminden yararlanan hibrit bir yöntem önermişlerdir. Ancak önerilen yöntem daha önce Çokal ve Solak [114] tarafından kriptanalizi yapılan Guan algoritmasıyla [72] büyük benzerlikler içermektedir ve önceki kriptanaliz çalışması uygulanarak bu şifreleme algoritmasının da kolayca kırılabileceği gösterilmiştir [134].

5.7.1 Algoritmanın Tarifi

Hem Guan algoritması hem de Bigdeli algoritması ilk aşamada Arnold Cat harita aracılığıyla görüntünün karılması prensibine dayanmaktadır. İkinci aşamada Guan algoritması Chen kaotik sisteminden üretilen anahtar ile karılmış görüntüyü XOR işlemine tabi tutarak şifreli görüntüyü elde ederken, Bigdeli algoritması anahtar üreteci için Chen kaotik sistemi yerine Hopfield sinir ağı kullanılmaktadır. Algoritmanın şifreleme adımları aşağıda açıklanmıştır.

Adım 1. İlk olarak lojiktik harita iterasyonları kullanılarak Arnold Cat haritasının başlangıç koşulları ve kontrol parametreleri elde edilir. Arnold Cat harita orijinal görüntünün piksel değerlerinin karılmasında kullanılır. P orijinal görüntüsüne karma işlemi uygulanarak S karılmış görüntü elde edilir. Orijinal görüntünün $N \times N$ boyutlarında olduğu varsayılmıştır.

Görüntünün piksel koordinatlarını göstermek için $l = \{(x, y)|x, y = 0, 1, 2, \dots, N-1\}$ kullanılmaktadır. Arnold's Cat haritanın yapısı Denklem (5.37)'de verilmiştir. Denklem (5.37)'de p, q pozitif tamsayılar ve x', y' karılmış görüntünün koordinat değerleridir.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ mod\ N \quad (5.37)$$

Adım 2. Hiper kaotik Hopfield sinir ağının başlangıç koşulları ve kontrol parametrelerini belirlemek için lojistik harita kullanılır. Hiper kaotik sistem $N_0 = (N \times N)/4$ defa itere edilir ve x_i, y_i, z_i, t_i $(1 \leq i \leq N_0)$ değerleri elde edilir.

Adım 3. Denklem (5.38) kullanılarak $B = \{B_1, B_2, \dots, B_{N \times N}\}$ kaotik anahtar dizisi üretilir.

$$B_{4(i-1)} = mod\big(round((abs(x_i) - floor\big(abs(x_i)\big)) \times 10^{14} + S_{4(i-1)}\big), 256\big)$$

$$B_{4(i-1)+1} = mod\big(round((abs(x_i) - floor\big(abs(x_i)\big)) \times 10^{14} + S_{4(i-1)}\big), 256\big)$$

$$B_{4(i-1)+2} = mod\big(round((abs(x_i) - floor\big(abs(x_i)\big)) \times 10^{14} + S_{4(i-1)}\big), 256\big)$$

$$B_{4(i-1)+3} = mod\big(round((abs(x_i) - floor\big(abs(x_i)\big)) \times 10^{14} + S_{4(i-1)}\big), 256\big) \quad (5.38)$$

Adım 4. Denklem (5.39) kullanılarak $C = \{c_1, c_2, \dots, c_{N \times N}\}$ şifreli görüntü vektörü elde edilir.

$$c_i = s_i \oplus b_i \quad (5.39)$$

Adım 5. C şifreli görüntü vektörü yeniden düzenlenerek $N \times N$boyutlarında şifreli görüntü elde edilir.

5.7.2 Algoritmanın Kriptanalizi

Saldırının kolay anlaşılması için 5×5 boyutlarında küçük bir görüntü üzerinde analiz yapılmıştır. İlk olarak iki farklı görüntü seçilmiştir. Seçilen ilk görüntü olan P_1 tüm piksel değerleri 0 olan bir görüntüdür. Seçilen ikinci görüntü olan P_2 ise sadece iki piksel değeri sıfırdan ve birbirinden farklı olan bir görüntüdür. Seçilen görüntüler Denklem

(5.40)'da gösterilmiştir. Saldırının ikinci aşamasında seçilen görüntülere karşılık gelen C_1, C_2 şifreli görüntüleri elde edilmiştir.

$$P_1 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix}, P_2 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (5.40)$$

P_1 görüntüsü için Arnold Cat harita kullanılarak yapılan karma işlemi çıkışa bir etki yapmayacaktır çünkü seçilen görüntünün tüm piksel değerleri sıfırdır. Bu yüzden karılmış görüntü orijinal görüntüye denk olacaktır ($S_1 = P_1$). Saldırgan bu olguyu Denklem (5.39)'da kullanarak şifreli görüntünün gizli anahtara eşit olduğunu bulabilir. Anahtar değerinin nasıl bulunabileceği Denklem (5.41)'de gösterilmiştir.

$$C_1 = S_1 \oplus \mathrm{B} = P_1 \oplus \mathrm{B} = 0 \oplus \mathrm{B} = B. \quad (5.41)$$

Saldırgan algoritmanın gizli parametresi olan B değerini bildiğine göre Denklem (5.39) kullanılarak şifreli görüntü C_2'ye denk gelen karılmış görüntü S_2'yi elde edebilir.

$$C_2 = S_2 \oplus \mathrm{B} \quad (5.42)$$

Saldırının bu aşamasında saldırgan orijinal görüntü P_2 ve onun karılmış biçimine S_2 sahiptir. S_2 görüntüsünün piksel değerleri içerisinde sıfırdan farklı olan piksel değerlerini arayarak karılmış koordinatları (x_1', y_1') ve (x_2', y_2') bulabilir. Denklem (5.37) kullanılarak aşağıdaki eşitlikler elde edilebilir.

$$\begin{bmatrix} x_1' \\ y_1' \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \end{bmatrix} \ mod\ N$$

$$\begin{bmatrix} x_2' \\ y_2' \end{bmatrix} = \begin{bmatrix} a_1 & a_2 \\ a_3 & a_4 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} \ mod\ N \quad (5.43)$$

Bu denklem sistemi çözülerek saldırgan A matrisinin değerlerini elde edebilir. Böyle şifreleme algoritmasının bütün gizli parametreleri açığa çıkarılmış olunur.

5.8 Ahmad Şifreleme Algoritmasının Güvenlik Analizi

Ahmad ve arkadaşları [135] ses verilerini şifrelemek için kaos tabanlı bir algoritma önermişlerdir. Şifreleme algoritmasında Lorenz ve Chen kaotik sistemleri kullanılarak kaotik bir anahtar dizisi üretilmiştir. Ancak yapılan güvenlik analizi çalışmasında

algoritmanın gizli anahtarının orijinal ve şifreli ses verisinden bağımsız olduğu gösterilmiştir [136].

5.8.1 Algoritmanın Tarifi

Şifreleme algoritmasında gizli anahtar olarak Lorenz ve Chen kaotik sistemlerinin başlangıç koşulları ve kontrol parametreleri kullanılmıştır. Şifreleme algoritması iki kısımdan oluşmaktadır. İlk kısımda Lorenz ve Chen kaotik sistemleri kullanılarak bir anahtar dizisi üretilmektedir. İkinci kısımda ise üretilen anahtar dizsi kullanılarak ses sinyalleri değiştirilmektedir. Şifreleme aşamaları aşağıda adım adım açıklanmıştır.

Adım 1. Lorenz ve Chen kaotik sistemleri *N* defa itere edilir. Burada *N* değeri şifrelenecek ses sinyalinin uzunluğuna eşittir.

Adım 2. Denklem (5.44) ve Denklem (5.45) kullanılarak kaotik sistemlerin çıkışları düzenlenir.

$$\dot{x}_k(i) = x_k(i) \times 10^5 - floor(x_k(i) \times 10^5) \tag{5.44}$$

$$\dot{y}_k(i) = y_k(i) \times 10^5 - floor(y_k(i) \times 10^5) \tag{5.45}$$

Adım 3. Denklem (5.46) ve Denklem (5.47) kullanılarak kaotik sistemlerden elde edilen çıkışlar bit dizilerine dönüştürülür.

$$\omega_k(i) = \begin{cases} 0 & \dot{x}_k(i) < 0.5 \\ 1 & \dot{x}_k(i) \geq 0.5 \end{cases} \tag{5.46}$$

$$\varphi_k(i) = \begin{cases} 0 & \dot{y}_k(i) < 0.5 \\ 1 & \dot{y}_k(i) \geq 0.5 \end{cases} \tag{5.47}$$

Adım 4. Kriptolojik olarak daha iyi diziler elde etmek için Denklem (5.48) kullanılarak çıkışlar karıştırılır.

$$\begin{cases} \theta_1 = \omega_1 \oplus \varphi_2 \oplus \omega_3 \\ \theta_2 = \varphi_3 \oplus \omega_1 \oplus \varphi_1 \\ \theta_3 = \omega_2 \oplus \varphi_1 \oplus \varphi_2 \\ \theta_4 = \omega_3 \oplus \omega_2 \oplus \varphi_3 \end{cases} \tag{5.48}$$

Adım 5. Çoklayıcı kullanılarak bir bitlik veri seçilir.

Adım 6. Seçilen bit değeri ile ses verisine XOR işlemi uygulanarak şifreli veri elde edilir.

$$c_i = p_i \oplus k_i \tag{5.49}$$

5.8.2 Algoritmanın Kriptanalizi

Önerilen şifreleme algoritmasında birçok kriptolojik eleman kullanıldıktan sonra bir anahtar dizisi elde edilmiştir. Anahtar üretim algoritmasının ne kadar karmaşık olursa olsun tüm değerleri sıfır olan bir ses verisine karşılık gelen şifreli ses verisi biliniyorsa algoritma Denklem (5.50)'deki eşitlik kullanılarak kırılabilir.

$$C{=}P \oplus K{=}0 \oplus K = K \tag{5.50}$$

5.9 François Şifreleme Algoritmasının Güvenlik Analizi

Sadece kaotik permütasyonlar aracılığıyla yapılan görüntü şifreleme algoritmalarının zayıflıklarının ortaya çıkmasının ardından son yıllarda bilginin bit düzeyinde kaotik olarak karıldığı yeni şifreleme algoritmaları önerilmiştir. François ve arkadaşları [137] buradan hareketle yeni bir görüntü şifreleme algoritması önerisinde bulunmuşlardır. Önerilen algoritmada bit düzeyinde kaotik fonksiyonlar aracılığıyla karılan dizilere XOR işleminin uygulanmasıyla şifreleme işlemi gerçekleştirilmektedir.

5.9.1 Algoritmanın Tarifi

Önerilen algoritmada şifreleme işlemine başlanmadan önce $M \times N$ boyutlarındaki orijinal görüntü tek boyutlu bit dizisine dönüştürülür. Şifreleme algoritması orijinal görüntüyü şifrelemek için iki farklı bit dizisi üretir. İlk dizi orijinal görüntünün tek boyutlu bit dizisine dönüştürülmüş biçiminin bir kopyasıdır. İkinci diziyi oluşturmak için orijinal bit dizisi kaotik fonksiyon kullanılarak karılır. Karma işlemi kaotik fonksiyonun çıkış değerinin gösterdiği pozisyondaki bit değerinin yeni üretilecek diziye eklenmesiyle gerçekleştirilir. Şifreli görüntüyü oluşturmak için üretilen iki diziye XOR işlemi uygulanır. Bu işlemler adım sayısı kadar tekrarlanır. Şifreleme algoritmasının çalışma mantığı aşağıda adım adım açıklanmıştır.

Adım 1. $M \times N$ boyutlarındaki orijinal görüntü bir boyutlu binary bit dizisi matrisine dönüştürülür. Oluşturulan bit dizisi matrisi Z_1 ile

gösterilmektedir. Z_1 matrisinin bir kopyası da Z_2 matrisine atılır. Oluşturulan bit dizisi matrislerinin uzunluğu $L = 8 \times M \times N$ dir.

Adım 2. Denklem (5.51) yapısı verilen kaotik fonksiyon kullanılarak X değişkeni ile gösterilen bir pozisyon değeri elde edilir.

Adım 3. $0 \leq i \leq L$ için $Z_2[i]$ pozisyonundaki bit dizisi matrisinin değeri; $Z_1[j]$ pozisyonundaki bit dizisi matrisinin değeriyle belirlenir. Burada $j \leftarrow i + 1 + X$ dir.

Adım 4. $Z_3 \leftarrow Z_1 \oplus Z_2$ işlemi uygulanarak yeni bir bit dizisi oluşturulur.

Adım 5. Bu işlemlere adım sayısına ulaşılıncaya kadar devam edilir.

5.9.2 Algoritmanın Kriptanalizi

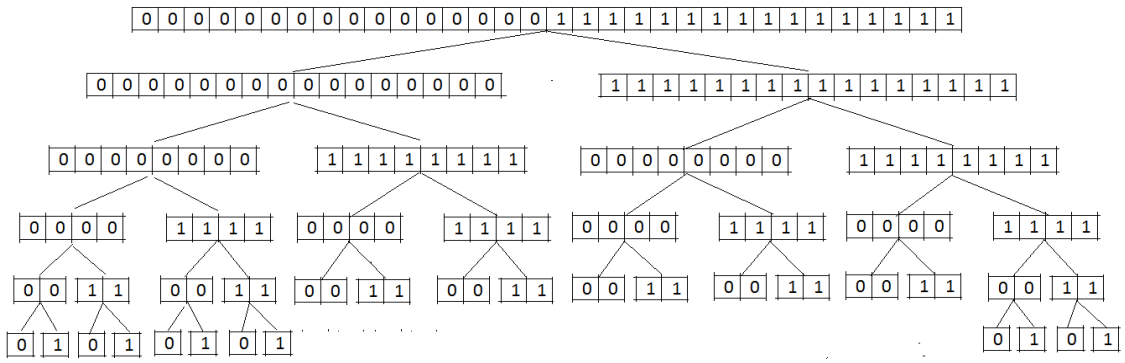
Saldırıda kullanılmak üzere seçilen açık metinler böl ve yönet mantığına göre seçilmiştir. Saldırıda kullanılacak açık metin sayısı; $L = 8 \times M \times N$ için $log_2 L$ dir. Seçilecek ilk açık metinin tek boyutlu bit dizisine dönüştürülmüş biçiminde bitlerinin ilk yarısının tümünün 0; kalan yarısının tümünün 1 olması istenmektedir. Diğer seçilecek açık görüntüler için ise kendinden bir önce seçilen bit dizisi ikiye bölünür ve yine ilk yarısının 0; ikinci yarısının 1 olması istenir. Bölme işlemine tek bit kalana kadar devam edilir.

Çizelge 5.7 Saldırı için böl ve yönet mantığına göre seçilen açık verilerin yapısı

Seçilen açık verilerin bit değişimleri																															
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1	0	0	0	0	1	1	1	1
0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1	0	0	1	1
0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1

Saldırının çalışma mantığı rahat açıklanması için $2x2$ boyutunda bir görüntü şifrelemek için seçilecek açık görüntülerin bir boyutlu bit dizisine dönüştürülmüş biçimleri Çizelge

5.7'de gösterilmiştir. Bu görüntülerin piksel karşılıkları sırasıyla {0,0,255,255}, {15,15,15,15}, {51, 51, 51, 51}, {85, 85, 85, 85} şeklindedir.



Şekil 5.1 Saldırı ağacının genel görünümü

Seçilen açık metin saldırısının doğası gereği seçilen bu görüntülere karşılık gelen şifreli görüntüler elde edilir. Daha önce açıklandığı gibi şifreli görüntü; kaotik olarak karıştırılmış görüntü ile orijinal görüntüden elde edilen bit dizilerine XOR işleminin uygulanmasıyla elde edilmiştir. Kriptanalist hem orijinal görüntüye hem de şifreli görüntüye sahip olduğundan kaotik olarak karılmış görüntüyü elde edebilir. Bu aşamada karılmış görüntünün orijinal görüntünün hangi pozisyonlardaki değerlerin alınarak elde edildiğini gösteren kaotik fonksiyonun çıkışı olan X değerleri belirlenmelidir. Bunun için böl ve yönet mantığına göre oluşturulmuş açık/şifreli görüntü çiftlerinden yararlanılır. Örneğin karılmış görüntülerin birinci bit değerinin orijinal görüntüdeki hangi pozisyondaki bit değeriyle oluşturulduğunu bulmak için seçilen açık/şifreli görüntülerin ilk bitleri incelenir. Seçilen bütün açık görüntülerin ilk bitleri 0 olduğuna göre şifreli görüntülerin değerini karışmış görüntülerin değerleri belirlemektedir. Seçilen ilk açık görüntü için elde edilen şifreli görüntü 1 olduğuna göre ilk X değeri Şekil 5.1'deki ağacın sol alt ağacındadır. İkinci açık görüntünün ilk bitine karşılık gelen görüntünün şifrelenmiş hali yine 1 olduğundan alt ağacın sol alt ağacından devam edilir. Üçüncü açık görüntü için bulunan şifreli görüntünün değeri 1 olduğundan yine alt ağacın sol alt ağacından devam edilir. Dördüncü ve beşinci açık görüntüler için ise elde edilen şifreli görüntüler 0 olduğundan bu durumlar içinde sağ alt ağaçlardan devam edilerek ilk X değerinin pozisyon bilgisi bulunur. Tüm bit dizisi için aynı işlemler tekrar edilerek bütün X değerleri bulunur. Bulunan X değerleri

şifreleme algoritmasının anahtarına eş değerdir. Bu bilgiye sahip bir kişi herhangi bir veriyi şifreleyebilir veya şifresini çözebilir.

Özetle yapılan analiz çalışasında şifreleme algoritmasının gizli anahtarı bilinmeksizin sadece $log_2 L$ tane böl ve yönet mantığına göre seçilmiş açık/şifreli görüntü kullanılarak şifreleme algoritmasının kırılabileceği gösterilmiştir.

5.10 Machicao Şifreleme Algoritmasının Güvenlik Analizi

Machicao ve arkadaşları [138] hücresel otomatanın kaotik davranış göstermesinden yola çıkarak yeni bir kaos tabanlı şifreleme algoritması önermişlerdir. Önerilen yöntemin güvenlik analizleri çeşitli istatistiki testler ile yapılmıştır. İstatistiki analizler sonucunda önceki önerilere göre daha iyi sonuçlar elde edilmiştir. Ancak istatistiki testler bir şifreleme algoritmasının sağlaması gereken unsurlardan biri olmasına rağmen tek başına yeterli değildir. Bu bölümde Machicao ve arkadaşları tarafından önerilen algoritmanın detaylı güvenlik analizleri yapılmıştır. İlk saldırıda; sadece bir adet açık/şifreli veri çifti kullanılarak şifreleme algoritmasının gizli anahtarının nasıl elde edilebileceği gösterilmiştir. İkinci saldırıda ise algoritmada rasgele sayı üreteci için çekirdek değerleri üretmede kullanılan lojistik haritanın anahtar uzayının nasıl indirgeneceği gösterilmiştir. Bu saldırı ile üretilebilecek olası bütün çekirdek değerleri açığa çıkarılmıştır. İkinci saldırı Bölüm 6'da konuya ilişkin bilgi verildikten sonra gösterilmiştir. Yapılan analiz çalışmaları sonucunda önerilen yöntemin güvenli iletişim için uygun olmadığı gösterilmiştir.

5.10.1 Algoritmanın Tarifi

Machicao ve arkadaşları kabaca bir blok şifreleme algoritması önermişlerdir. Algoritmada her bir blok şifrelenirken anahtar ve kendinden önce şifrelenen blok kullanılmaktadır. Algoritmanın matematiksel gösterimi Denklem (5.51) ve Denklem (5.52)'de verilmiştir. Önerilen algoritmanın yeniliği ise her bir bloğun şifrelenmesinde kullanılan anahtarların üretim mantığında gizlidir. Machicao ve arkadaşları anahtar üretimi için üç aşamalı bir yöntem kullanmışlardır. Her bir aşamada gerçekleştirilen işlemlerin listesi aşağıda adım adım verilmiştir.

$$y_1 = k_1 \oplus x_1 \quad (5.51)$$

$$y_i = k_i \oplus x_i \oplus y_{i-1}, i > 1 \quad (5.52)$$

Birinci aşama içerinde yapılan işlemler

- Şifreleme algoritmasının gizli anahtarı olarak 128 bit uzunluğunda bir değer belirlenir.
- Denklem (5.53), (5.54) ve (5.55) kullanılarak $\vec{\pi}$ gizli anahtarından kaotik sistemin başlangıç koşulu X_0 belirlenir.

$$\Omega := \sum_{i=1}^{size(\vec{\pi})} 2^{8*(i-1)} \pi_i \quad (5.53)$$

$$\Omega = \frac{\Omega}{2^{(8*size(\vec{\pi})+1)}} \quad (5.54)$$

$$X_0 = \Omega + 0.00001 \quad (5.55)$$

- Lojistik harita itere edilir. İlk 1000 iterasyon geçici etkilerin ortadan kalkması için alınmaz.
- Denklem (5.56)'da verilen niceleme mantığı kullanılarak [0,1] aralığında üretilen sürekli değerler binary değerlere ayrıklaştırılır.

$$\begin{cases} 1 & if\ X_k < 0.5 \\ 0 & if\ X_k \geq 0.5 \end{cases} \quad (5.56)$$

- Lojistik haritanın iterasyonları sonucunda $m \times n$ boyutunda binary bir dizi üretilir.

İkinci aşama içerisinde yapılan işlemler

- $m \times n$ boyutundaki binary dizi hücresel otomatın başlangıç değerleri olarak atanır.
- Doğal hücresel olguları modellemede kullanılan "Gam-of-Life" kuralları kullanılarak yeni jenerasyonlar üretilir. Farklı kuralların kullanılması farklı jenerasyonların elde edilmesine sebep olmaktadır. Detaylar için kaynak [138] incelenebilir.
- Şifreleme algoritmasında yeni popülasyonların üretilmesi için 64×64 boyutunda bir hücresel otomata ve B1357/S2468 kuralı kullanılmıştır

Üçüncü aşama içerisinde yapılan işlemler

- 64×64 boyutundaki hücresel otomat bloklara ayrılır.
- Elde edilen bloklara XOR işlemi uygulanarak her bir bloğun şifrelenmesinde kullanılacak anahtar değeri üretilir.

Anahtar değerinin üretilmesinin ardından Denklem (5.51) ve Denklem (5.52)'de verilen yapı kullanılarak her bir bloğun şifrelenmesi işlemi gerçekleştirilir.

5.10.2 Algoritmanın Kriptanalizi

Machicao ve arkadaşları da kaos, hücresel otomata ve Game-of-Life süreçlerini kullanarak şifreleme algoritmasının her bir bloğunda kullanılmak üzere bir anahtar üreteci tasarlamışlardır. Üretilen anahtarlar istatistiki olarak birçok rasgelelik testini geçmesine rağmen şifreleme siteminin cebirsel bağımlılıklar içermesi sonucunda sadece bir adet açık/şifreli veri çiftinin bilinmesi durumunda anahtar değeri elde edilebileceği gösterilmiştir. Denklem (5.51) ve Denklem (5.52)'de genel yapısı verilen şifreleme algoritması daha açık biçimde denklem 7'deki gibi yazılabilir. Denklem (5.57)'de XOR işleminin birleşme özelliği kullanılarak yeniden düzenlenirse Denklem (5.58)'deki gibi şifreleme algoritmasının daha basit bir ifadesi ortaya çıkmaktadır.

$$y_i = k_i \oplus x_i \oplus k_{i-1} \oplus x_{i-1} \oplus \dots \oplus k_2 \oplus x_2 \oplus k_1 \oplus x_1 \tag{5.57}$$

$$y_i = (k_i \oplus k_{i-1} \oplus \dots \oplus k_2 \oplus k_1) \oplus (x_i \oplus x_{i-1} \oplus \dots \oplus x_2 \oplus x_1) \tag{5.58}$$

En basit saldırı yöntemlerinden biri bilinen açık metin saldırısıdır. Bu saldırıda, saldırgan özel seçtiği bir açık metine karşılık gelen şifreli metni bulur. Açık/şifreli veri çiftlerini kullanarak algoritmanın gizli parametresi olan anahtarı elde etmeye çalışır. Denklem (5.58)'de elde edilen yapı için açık/şifreli veri çiftleri denklemde yerine yazılırsa algoritmanın gizli parametresi olan anahtar değerleri açığa çıkarılmış olur. Anahtar değerine sahip olan bir kişi istediği herhangi bir veriyi şifreleyebilir veya şifresini çözebilir.

Saldırı sonucunda görülmüştür ki; şifreleme algoritması içerisinde kullanılan yapıların kriptolojik olarak güçlü karakteristiklere sahip olması gerekmektedir. Ancak ne kadar güçlü yapılar kullanılırsa kullanılsın asıl önemli olan bu yapıların kriptolojik tasarım sürecinde nasıl kullanıldığıdır.

5.11 Hu Şifreleme Algoritmasının Güvenlik Analizi

Hu ve arkadaşları [139] Chen kaotik sistemini temel alan bir sözde rasgele sayı üreteci önermişlerdir. Algoritmanın en önemli yeniliği ise Chen sisteminin çıkışları üzerinde düzenlemeler yaparak çıkışların düzgün (uniform) bir dağılım göstermesini sağlamışlardır. Üretilen kaotik sayıları kullanarak bir görüntü şifreleme algoritması tasarlamışlardır.

5.11.1 Algoritmanın Tarifi

Önerilen sözde rasgele üreteci Chen kaotik sistemini temel almaktadır. Chen kaotik sisteminin dinamikleri Denklem (5.59)'da verilmiştir. Denklem (5.59)'da kontrol parametreleri a=35, b=3 ve c=28 olarak seçilmiştir. Sistemin başlangıç koşulları ise $(x_0, y_0, z_0) = (-3, 2, 20)$ olarak belirlenmiştir. Verilen başlangıç koşulları ve kontrol parametreleri için sistem çıkışları Şekil 5.2'de verilmiştir. Şekil 5.2'den görüldüğü gibi çıkış değerleri düzgün bir dağılıma sahip değildir.

$$\begin{cases} \dot{x} = a(y - x) \\ \dot{y} = (c - a)x - xz + cy \\ \dot{z} = xy - bz \end{cases} \tag{5.59}$$

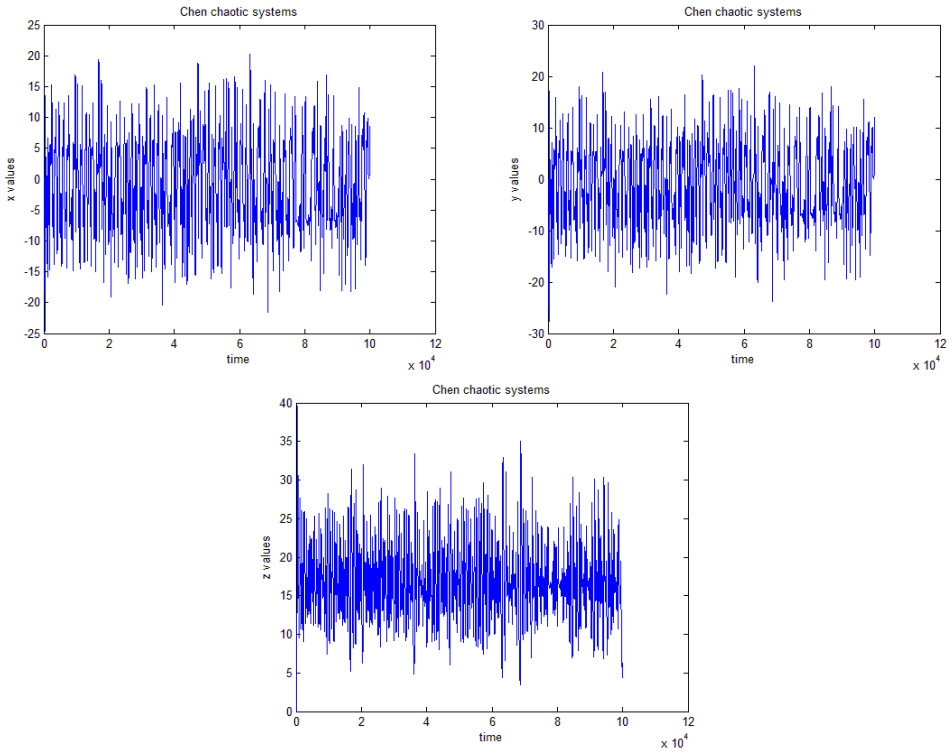
Çıkış değerlerinin düzgün bir dağılım göstermesi için Denklem (5.60) kullanılmıştır. Denklem (5.60) uygulandıktan sonra x değerlerinin dağılımı Şekil 5.3'de gösterilmiştir. Algoritmada düzgün dağılım gösteren sayı değerleri üretildikten sonra bu değerler kullanılarak şifrelenecek görüntünün piksel değerlerinin maskelenmesi sağlanmıştır.

$$\begin{cases} v(3i) = 3000 * (x(i) + 45) \\ v(3i+1) = 3000 * (y(i) + 35) \quad i = 0,1,2,\dots \\ v(3i+2) = 3000 * (z(i) + 45) \end{cases} \tag{5.60}$$
$$K(j) = v(j) mod 256 \quad j = 0,1,2,\dots$$

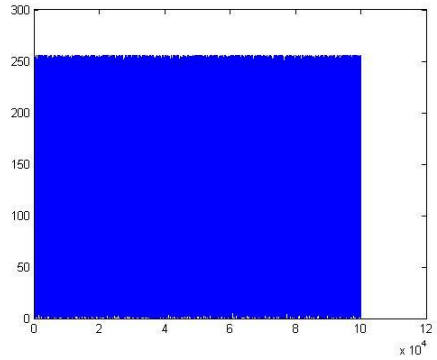
5.11.2 Algoritmanın Kriptanalizi

Bir algoritmanın güvenliği değerlendirilirken ilk olarak anahtar uzayının genişliği değerlendirilmelidir. Günümüz modern şifreleme algoritmaları için 128-bit uzunluğunda bir gizli anahtar etraflı aramaya karşı dirençlidir. Önerilen algoritmanın

anahtar uzayı $10^{78} \approx 2^{256}$ olduğu ifade edilmiştir. Bu durumda etraflı arama mantıksızdır.



Şekil 5.2 Chen kaotik sisteminin yörüngeleri



Şekil 5.3 Denklem (5.60)'ın uygulanması sonucunda x değerlerinin dağılımı

Yapılan saldırının mantığı anahtar uzayının indirgenmesi prensibine dayanmaktadır. Çizelge 5.8'de Chen kaotik sisteminin $(x(i)+45)$, $(y(i)+35)$ and $(z(i)+45)$ çıkışlarının maksimum ve minimum değerleri gösterilmiştir. Denklem (5.60)'daki mod alma işlemi sonucunda 256 farklı olasılık bulunmaktadır. Ancak Çizelge 5.8'den görülebileceği gibi her bir değer için sırasıyla 44, 53 ve 46 farklı olasılık vardır. Bu da anahtar uzayını indirgenmektedir. Üretilen herhangi bir rasgele sayı için maksimum 53

deneme ile çıkışın ne olduğu bulunabilir. Sonuç olarak önerilen saldırının karmaşıklığı $O(53 * n) = O(n)$'dir [160].

Çizelge 5.8 Chen sistemi için değerlerin değişim aralığı

	Minimum Değer	Maksimum Değer	Aralıktaki Değer Sayısı
$x(i)$	-25.5914	19.8718	∞
$y(i)$	-29.7154	24.2947	∞
$z(i)$	0	46.1850	∞
$(x(i) + 45)\%256$	20	64	44
$(y(i) + 35)\%256$	6	59	53
$(z(i) + 45)\%256$	45	91	46

5.12 Hermassi Şifreleme Algoritmasının Güvenlik Analizi

Hermassi ve arkadaşları [140] sıkıştırma ve şifrelemenin birleştirilmesi için kaotik olarak değiştirilmiş Huffman ağaçlarını kullanan bir yöntem önermişlerdir. Önerilen yöntem Huffman ağacının sağ ve sol dallarını kaotik olarak belirlenen anahtar kontrollünde değiştirerek çoklu Huffman tablolarını temel almakta sıkıştırma ve şifrelemeyi eş zamanlı olarak gerçekleştirmektedir.

5.12.1 Algoritmanın Tarifi

N sembolden oluşan L uzunluğundaki herhangi bir M mesajı için şifreleme ve sıkıştırma işlemini sağlayan algoritma kabaca aşağıdaki adımlardan oluşmaktadır.

Adım 1. Verilen mesaj için Huffman ağacı oluşturulur.

Adım 2. Kaotik sistem kullanılarak sözde rasgele bir sayı üretilir.

Adım 3. Şifreleme ve sıkıştırma işlemi geçekleştirilirken kaos tabanlı sözde rasgele sayının gösterdiği Huffman ağacı düğümünün yaprakları yer

değiştirilerek yeni bir ağaç oluşturulur ve bu ağaç kullanılarak mesajın bir karakteri kodlanır.

Adım 4. Mesajın tamamı şifrelenineceye kadar ikinci adımdan işleme devam edilir.

5.12.2 Algoritmanın Kriptanalizi

Önerilen algoritmada şifrelenecek ve sıkıştırılacak metinin her bir karakterini kodlamak için kullanılan değiştirilmiş Huffman ağacı oluşturulurken sadece kaos tabanlı sözde rasgele sayının işaret ettiği düğümün yaprakları yer değiştirmektedir. Bu değişimin sonucunda oluşan yeni ağaçta kaynak sembollerin olasılık değerleri değişmemekte sadece aynı uzunlukta farklı bir kod sözcüğü atanmaktadır. Bu saldırının [141] temel dayanak noktası kaotik olarak değiştirilen Huffman ağaçlarında her sembolün istatistiksel olarak olasılık ve kod uzunluklarının değişmemesine dayanmaktadır.

S sembol içeren L uzunluğundaki bir M mesajı için hepsi aynı karakterden oluşmuş L karakter uzunluğunda S tane açık ve şifreli metin çifti varsa M mesajının şifreli hali çözülebilir. Örneğin şifreleme ve sıkıştırma algoritmasında orijinal veri olarak Denklem (5.61)'de verilen mesaj kullanılsın.

M=EDCBBAFAADEEFEDDADADCDEFFCAECACADDACFAECCAAFFAFAE (5.61)

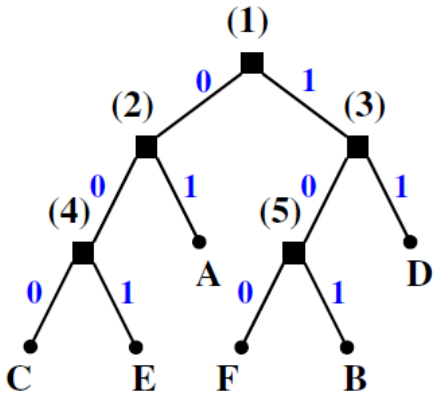
Çizelge 5.9 M mesajı için frekans, olasılık değeri ve kod sözcükleri

Sembol	Frekans	Olasılık	Kod
A	14	14/50=0.28	00
B	2	2/50=0.28	101
C	8	8/50=0.16	010
D	10	10/50=0.2	11
E	8	8/50=0.16	011
F	8	8/50=0.16	100

Seçilen mesaj için kullanılan sembollerin frekans değerleri, olasılıkları ve verilen kod sözcükleri Çizelge 5.9'da verilmiştir. Oluşturulan temel Huffman ağacı Şekil 5.4'de

gösterilmiştir. Mesajının ilk 11 karakteri için oluşturulmuş şifreli metni kırabilmek için 11 karakter uzunluğunda hepsi aynı karakterlerden oluşan 6 adet açık ve şifreli metin çifti gerekmektedir. Çizelge 5.10'da mesajların açık ve şifreli biçimleri verilmiştir.

Şifreleme süreci boyunca biliyoruz ki hiçbir sembolün kod uzunluğu değişmeyecektir. Buna göre A sembolü hep 2 karakter uzunluğundaki kod sözcükleriyle kodlanmıştır. Bu yüzden 11 adet A sembolünden oluşan M_1 mesajının şifrelenmiş biçimi 2x11=22 karakter uzunluğunda bir koda sahiptir. Benzer şekilde B, C, D, E, F sembolleri de hep 3, 3, 2, 3, 3 karakter uzunluğundaki kod sözcüklerinden oluşmaktadır. Dolayısıyla M_2, M_3, M_4, M_5 ve M_6 metinlerinin şifrelenmiş biçimleri de 33, 33, 22, 33 ve 33 karakter uzunluğunda bir koda sahiptir.



Şekil 5.4 M mesajı için oluşturulan temel Huffman ağacı

Çizelge 5.10 Saldırı için seçilen açık ve şifreli verilerin yapısı

Açık Metin	Şifreli Metin
M=EDCBBAFAADE	C=00010011111110101111111100101
M_1=AAAAAAAAAAA	C_1=0101000101010111111111
M_2=BBBBBBBBBBB	C_2=10111111111111011111100100100100010
M_3=CCCCCCCCCCC	C_3=00100101100100100100110110010011100
M_4=DDDDDDDDDDD	C_4=11111010101010100000000000
M_5=EEEEEEEEEEE	C_5=00000001000000000000100101100101
M_6=FFFFFFFFFFF	C_6=10011011011011111011011011011011

Çizelge 5.11'de her bir metindeki karakterlerin sıra numaralarına göre verilen kod sözcüklerinin değerleri gösterilmiştir. Kod sözcüklerinin altındaki (+) ve (-) işaretleri ise kendinden bir önceki sahip olduğu kod sözcüğü değerine göre kodun değişip değişmediğini göstermektedir. Örneğin M_2 mesajının ikinci karakteri için değiştirilmiş Huffman ağacıyla oluşturulmuş kod sözcüğü 111'dir. Kod sözcüğünün altındaki (+) işareti ise kendisinden bir önceki sahip olduğu kod sözcüğüne göre farklı bir kod sözcüğü üretildiğini yani atası olan düğümün yapraklarının yer değiştiğini göstermektedir. Her bir i. adımda hangi düğümün değiştiğini bulmak için tablodaki i. sütun incelenir.

Çizelge 5.11 Saldırı için analiz çizelgesi

	Karakter Sıra No											
Metin	**Başlangıç**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**
M_1	01	01 (-)	01 (-)	00 (+)	01 (+)	01 (-)	01 (-)	01 (-)	11 (+)	11 (-)	11 (-)	11 (-)
M_2	101	101 (-)	111 (+)	111 (-)	111 (-)	110 (+)	111 (+)	110 (+)	010 (+)	010 (-)	010 (-)	010 (-)
M_3	000	001 (+)	001 (-)	011 (+)	001 (+)	001 (-)	001 (-)	001 (-)	101 (+)	100 (+)	101 (+)	100 (+)
M_4	11	11 (-)	10 (+)	10 (-)	10 (-)	10 (-)	10 (-)	10 (-)	00 (+)	00 (-)	00 (-)	00 (-)
M_5	001	000 (+)	000 (-)	010 (+)	000 (+)	000 (-)	000 (-)	000 (-)	100 (+)	101 (+)	100 (+)	101 (+)
M_6	100	100 (-)	110 (+)	110 (-)	110 (-)	111 (+)	110 (+)	111 (+)	011 (+)	011 (-)	011 (-)	011 (-)
Kaotik Sayı		*4*	*3*	*2*	*2*	*5*	*5*	*5*	*1*	*5*	*5*	*5*

Örneğin mesajın birinci karakteri için 1. sütun incelenirse M_3 ve M_5 mesajlarının (+) ile etiketlendiği görülür. Çünkü M_3 ve M_5 mesajlarının birinci karakterleri için üretilen kod sözcükleri bir önceki koda göre değişmiştir. Bu 3 ve 5 numaralı semboller olan C ve E sembollerinin atası olan (4) numaralı düğümün yapraklarının yer değiştirdiği anlamına

gelir. Sonuç olarak kaotik sistem kullanılarak üretilmiş rasgele sayı değerinin 4 olduğu elde edilir. Benzer şekilde mesajın ikinci karakteri için 2. sütun incelenirse M_2, M_4 ve M_6 mesajlarının (+) ile etiketlendiği görülür. Bu 2, 4 ve 6 numaralı semboller olan B, D ve F sembollerinin atası olan (3) numaralı düğümün yapraklarının yer değiştirdiği anlamına gelir. Bu şekilde devam edilerek kaos tabanlı sözde rasgele sayı dizisi elde edildikten sonra başlangıçtaki Huffman ağacı kullanılarak C mesajının orijinali elde edilebilir.

BÖLÜM 6

HESAPLAMA DUYARLILIĞININ ŞİFRELEME SİSTEMİNE ETKİLERİ

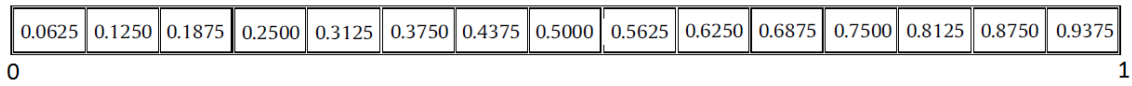
Kaotik sistemleri protokol tasarım aşamasında kullanmak teorik olarak mümkün olmasına rağmen pratik uygulamalar göz önüne alındığında birçok zayıf öneri ile karşılaşılmaktadır. Bu bölümde; kriptolojik protokollerin tasarımında rasgele benzeri bir süreç olarak tanımlanan kaotik sistemlerin kullanılması durumunda hesaplama duyarlılığına bağlı olarak kaotik sistemlerin gösterdiği davranışın şifreleme sistemi üzerine olan etkisi analiz edilmiştir. Deneysel sonuçlar ile lojistik haritayı temel alan tasarımların ulaşabileceği maksimum güvenlik düzeyinin standart bir rasgele fonksiyondan daha düşük olduğu gösterilmiştir.

6.1 Hesaplama Duyarlılığı

Verileri işlemek, kontrol etmek ve depolamak için tasarlanmış bir makine olarak tanımlanan bilgisayarlar için en önemli teorik problemlerden biri verinin bilgisayarlarda nasıl temsil edileceğidir. Tamsayı, reel sayı ve karakter dizileri gibi veri tipleri doğası gereği sonsuz uzunlukta olabilir. Ancak bilgisayarlar sonlu hesaplama kapasitesine sahip oldukları için hesaplama duyarlılığına bağlı olarak bir sayısal kötüleşme meydana gelecektir [142-145]. Bu sayısal kötüleşme ile farklı veri değerleri sanki aynı değeri temsil ediyormuş gibi algılanacaktır. Bu problemi teorik olarak gösterebilmek için bilgisayar bilimlerinde temel ispat yöntemlerinden biri olan güvercin yuvası kaidesi kullanılabilir [146].

Tanım 6.1: Güvercin yuvası kaidesi: Bir ortamda n tane güvercin ve t tane yuva bulunuyor ve $n > t$ ise en az bir yuvada $\left\lceil \frac{n}{t} \right\rceil$ kadar güvercin bulunur.

Örneğin; [0,1] aralığında sonsuz sayıda reel sayı bulunmaktadır. 4-bit hesaplama duyarlılığına sahip bir bilgisayar üzerinde bu sayıları gösterdiğimizi varsayalım. Bu durumda [0,1] aralığı 2^4-1=15 farklı aralığa bölünecektir. Her bir aralığın alt ve üst sınırları Şekil 6.1'de gösterilmiştir. Şekil 6.1'den kolayca görülebileceği gibi; örneğin 0.0625 ile 0.1250 değerleri arasındaki bütün reel sayılar 0.0625 değeri ile temsil edilecek ve hesaplamalarda bir sayısal kötüleşmeye meydana gelecektir.



Şekil 6.1 4-bit hesaplama duyarlılığı için hesaplama aralıkları

6.2 Hesaplama Duyarlılığının Kaotik Davranışa Etkisi

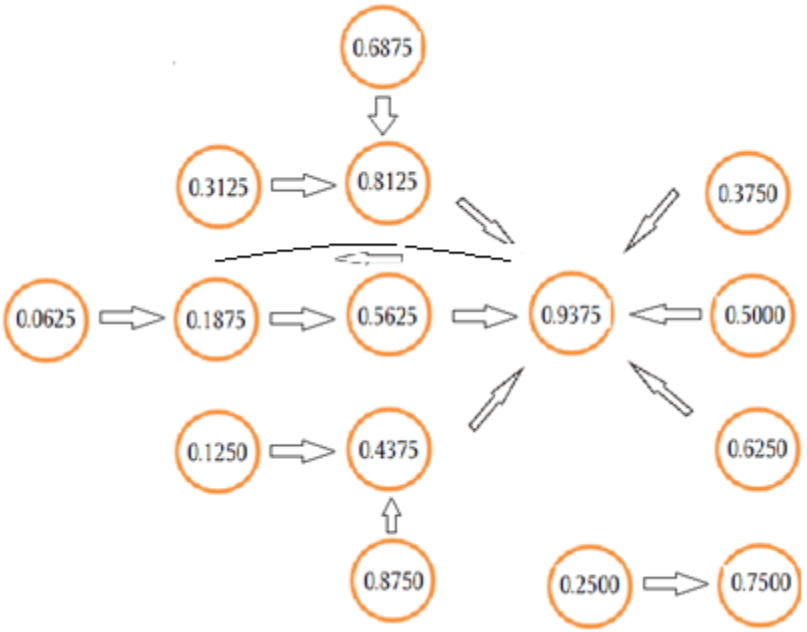
Hesaplama duyarlılığına bağlı olarak ortaya çıkan problem; kaotik sistemler sayısal bilgisayarlar üzerinde gerçekleştirildiğinde bozucu bir etkiye sebep olmaktadır. Kaotik sistemlerin faz uzayı reel sayıların sonlu bir kümesi üzerinde tanımlı olduğundan hesaplamalarda meydana gelecek bir kötüleşme kaotik sistemin göstereceği rasgele benzeri davranışı etkileyecektir [142-144]. Bu durumu örnek üzerinde göstermek için kriptolojik tasarımlarda yaygın bir şekilde kullanılan lojistik haritanın 4-bit hesaplama duyarlılığına sahip bir bilgisayar üzerinde gerçekleştirilmesi durumunda elde edilen yörüngelerin değişimi Şekil 6.2'de gösterilmiştir. 4-bit hesaplama duyarlılığı için 2^4-1=15 farklı hesaplama aralığı belirlenmiştir. Teorik olarak 15 farklı başlangıç değeri için 15 farklı yörüngenin elde edilmesi beklenirken sadece 2 farklı yörüngenin elde edildiği gözlemlenmiştir.

6.3 Sözde Rasgele Fonksiyonların Temel Özellikleri

Modern kriptoloji biliminin asıl amacı iletişim güvenliği sağlamak için kullanılacak protokolün tasarlanması ve analiz edilmesiyle ilgilidir. Sözde rasgele fonksiyonlar protokol tasarımında merkezi bir role sahiptir. Sözde rasgele fonksiyonların giriş çıkış ilişkisi rasgele bir fonksiyondan hesapsal olarak ayırt edilemeyen bir fonksiyon olması

istenmektedir. Tasarım sürecinde sözde rasgele fonksiyonların kullanılması kriptanalistin şifreleme sistemi üzerinde istatistiki çıkarımlar yapmasını önleyecek ve kriptolojik uygulamalar için temel gereksinimler olan karıştırma ve yayılma özellikleri sağlanacaktır [147-152].

Rasgele fonksiyon n elemanlı sonlu bir kümeden m elemanlı sonlu bir kümeye tanımlı bir fonksiyon olarak tanımlanmaktadır. $f: X \to X$; n elemanlı X kümesi üzerinde tanımlı bir fonksiyon olsun. f fonksiyonu F_n ile gösterilen fonksiyonlar kümesi içerisinden eşit olasılıklı olarak seçilmiştir. Örnek uzayı n^n farklı rasgele fonksiyon içerdiği için F_n fonksiyonlar kümesinden f fonksiyonunun seçilme olasılığı $\frac{1}{n^n}$ olarak hesaplanmaktadır.



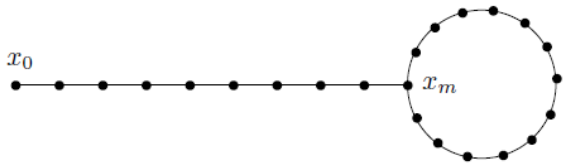
Şekil 6.2 4-bit hesaplama duyarlılığı için lojistik haritanın yörüngeleri

$x_0 \in X$ gibi bir başlangıç noktasından başlamak üzere f fonksiyonu iteratif olarak hesaplanırsa Denklem (6.1)'de gösterilen dizi elde edilmektedir.

$$\{x_0, f(x_0), f^2(x_0), \dots\} \tag{6.1}$$

$0 \leq k \leq n$ olmak üzere X kümesi üzerinde tanımlı f fonksiyonunun k. İterasyonu $f^k(x_0) = f(f^{k-1}(x_0))$ ile hesaplanmaktadır. Burada $f^0(x_0) = x_0$ dır. $k \geq 0$ için $f^k(x_0) = y$ ise y değeri; f fonksiyonunda x_0 değerinin k. görüntüsü olarak

adlandırılmaktadır. $k < 0$ için ise $f^k(x_0)$ ifadesinin bir değeri yoktur. Ters görüntüsü olmayan bu noktalar terminal düğümler olarak adlandırılmaktadır.



Şekil 6.3 Bir fonksiyon için fonksiyonel grafiği

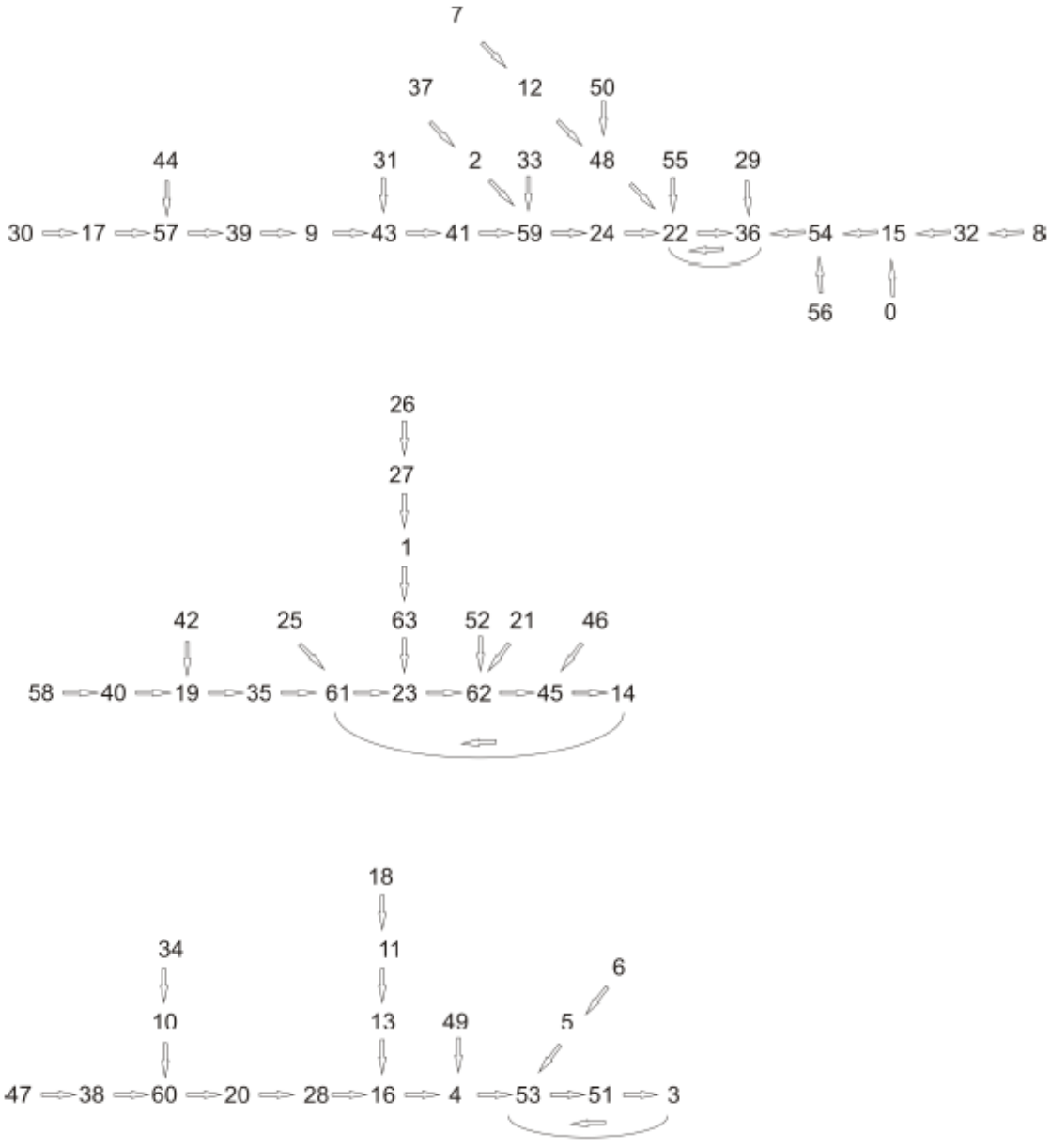
Bir $f: X \to X$ fonksiyonunun fonksiyonel grafiği tüm $x \in X$ için X'in elemanları düğümleri ve $(x, f(x))$ sıralı ikilileri de kenarları göstermek üzere yönlü bir çizgedir. Şekil 6.3'de iterasyonların tipik bir davranışı gösterilmiştir. $f^m(x_0),\ 0 \leq m \leq n-1$ noktaların bir iterasyona girdiğini göstermektedir. $f^m(x_0) = f^k(f^m(x_0))$ ise k pozitif tamsayı olmak üzere en küçük çevrim uzunluğunu göstermektedir. $f^m(x_0)$ kuyruk uzunluğu olarak adlandırılır. Kuyruk uzunluğu ile çevrim uzunluğu toplamı p-uzunluk değerinin vermektedir.

Çizelge 6.1 $n = 2^6$ için rasgele bir fonksiyon

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

Çizelge 6.1'de $n = 2^6$ için rasgele bir fonksiyon verilmiştir. Çizelge 6.1'de verilen fonksiyon için fonksiyon çzgesi Şekil 6.4'de verilmiştir. Şekilden görülebileceği gibi birleşen sayısı 3 ve çevrime giren düğüm sayısı 10'dur. k-ön görüntüye sahip düğüm sayısı Çizelge 6.2'de verilmiştir. Örneğin $x_0 = 43$ noktası için kuyruk uzunluğu 3, çevrim uzunluğu 2 ve sonuç olarak toplam p-uzunluk 5 olarak bulunur.

Rasgele haritalamanın istatistiksel özellikleri literatürde yaygın şekilde çalışılmıştır. Aşağıda rasgele haritalamanın yaygın kullanılan bazı karakteristikleri verilmiştir. Detaylı bilgi için Kaynaklar [147-152] incelenebilir.



Şekil 6.4 Çizelge 6.1'de verilen rasgele fonksiyonun grafı

- Bileşen sayısı: $\frac{\ln(n)}{2}$
- Terminal düğüm sayısı: $e^{-1}n \cong 0.3679n$
- Görüntüsü olan düğüm sayısı: $\sqrt{\frac{\pi n}{8}} \cong 0.6267\sqrt{n}$

- Ortalama çevrim uzunluğu: $\sqrt{\frac{\pi n}{8}} \cong 0.6267\sqrt{n}$
- Ortalama kuyruk uzunluğu: $\sqrt{\frac{\pi n}{8}} \cong 0.6267\sqrt{n}$
- Ortalama p-uzunluğu: $\sqrt{\frac{\pi n}{2}} \cong 1.2533\sqrt{n}$
- Ortalama birleşen boyutu: $\frac{2n}{3}$
- Maksimum çevrim uzunluğu: 0.78248 $\sqrt{n}$
- Maksimum kuyruk uzunluğu: 1.73746 $\sqrt{n}$

Çizelge 6.2 k-ön görüntüye sahip düğümlerin sayısı

k	0	1	2	3	4
Düğüm sayısı	24	23	12	4	1

6.4 Performans Karşılaştırmaları

Bölüm 6.2'de 4-bit hesaplama duyarlılığına sahip bir makine üzerinde lojistik harita rasgele fonksiyon olarak kullanıldığında toplam iki farklı yörüngenin elde edildiği ve maksimum uzunluklu yörüngenin p-uzunluğunun 5 olduğu gösterilmiştir. Bölüm 6.3'de verilen formüllere göre beklenen ortalama bileşen sayısının (yörünge sayısının) ve p-uzunluğu değerlerinin hesaplanan değerler ile benzer çıktığı görülmektedir. Ancak Çizelge 6.3'de kaotik sistem olarak lojistik harita seçilmesi ve hesaplama duyarlılığı olarak farklı n-bit hesaplama hassasiyeti seçilmesi durumunda elde edilebilecek yörüngelerin sayısı ve p-uzunluğu ölçümlerinin beklenen değerleri ile ortalama değerleri karşılaştırmalı olarak verilmiştir. Çizelge 6.3'de görülebileceği gibi lojistik haritanın rasgelelik özelliklerinin standart bir rasgele fonksiyondan daha kötü olduğu deneysel olarak gösterilmiştir.

6.5 İstatistiki Rasgelelik Testlerinin Problemleri

Kaos tabanlı kriptolojik tasarımların analizinde karşılaşılan en önemli problem istatistiksel testlerde başarılı sonuçların elde edilmesinin birçok tasarımcı tarafından

kriptolojik sistemin güvenlik analizi için yeterli olduğunun düşünülmesidir. Bu tip bir algıyı ortadan kaldırmak için bu bölümde lojistik harita kullanılarak elde edilen çıkışların istatistiksel testler kullanılarak analiz işlemi gerçekleştirilmiştir.

Çizelge 6.3 Hesaplama duyarlılığının lojistik haritanın davranışına olan etkisi

2^neleman (n hesaplama hassasiyeti)		2^8	2^{10}	2^{16}	2^{23}
Ortalama p-uzunluğu	Beklendik Değer	20	40	320	2896
	Hesaplanan Değer	27	32	251	444
	Maksimum p-uzunluğu	30	33	264	487
Bileşen sayısı	Beklendik Değer	4	5	8	11
	Hesaplanan Değer	4	4	6	7

Lojistik harita Denklem (6.2)'de verilen haritalama kullanılarak 0 ve 1 dizisine dönüştürülmüştür. Elde edilen sözde rasgele sayıların istatistiksel özellikleri NIST tarafından [164] geliştirilen istatistiksel test paketi kullanılarak analiz edilmiştir. Test sonuçları Çizelge 6.4'de verilmiştir. Çizelge 6.4'de test paketi ile uyum göstermesi açısından istatistiksel testlerin orijinal isimleri kullanılmıştır. Kaynak [165]'de bu testlerin yapısına ilişkin Türkçe bir çalışma yapılmıştır. Kaynak [165]'e göre testlerin Türkçe karşılıkları ve kısa açıklamaları aşağıda verilmiştir.

$$B_i = f(x_i) = \begin{cases} 0, & x_i < c \\ 1, & x_i \geq c \end{cases} \tag{6.2}$$

- Frekans Testi: Bit dizisindeki 1 ve 0 dengesini inceler.
- Blok Frekans Testi: m bitlik bir blok içerisindeki 1'lerin oranının gözlemlenmesi ilkesine dayanır.
- Akış Testi: Bit dizisindeki akışların toplam sayısıyla ilgilidir.
- En Uzun Birler Akış Testi: Dizideki 0 ve 1 bloklarının uzunluklarını inceler. M-bitlik bloklarda bulunan en uzun birler grubu üzerinde yoğunlaşır.

- İkili Matris Rank Testi: Her biri bir satırı belirtecek şekilde sabit uzunlukta bir blokları kullanarak bir matris oluşturulur ve matrisin rankı hesaplanarak bloklar arası lineer bağımlılık incelenir.
- Ayrık Fourier Dönüşüm Testi: Mevcut bit dizisinin ayrık fourier dönüşümü alınır ve periyodikliği incelenir.
- Örtüşmeyen Şablon Eşleştirme Testi: m bitlik bloğun dizi içerisinde tekrarını inceler. Tekrar edildiği takdirde tekrar edilen bloktan itibaren yeni m bitlik blok oluşturulur.
- Örtüşen Şablon Eşleştirme Testi: m bitlik bloğun dizi içerisinde tekrarını inceler. Tekrar edildiği takdirde blok 1 bit ötelenerek yenisi oluşturulur.
- Maurer's Universal İstatistiksel Testi: Dizininin veri kaybı olmadan ne kadar sıkıştırılabildiğini inceler.
- Doğrusal Karmaşıklık Testi: Bit dizisinin geri besleme(feedback register) uzunluğuna bakarak karmaşıklığını inceler.
- Lempel-Ziv Sıkıştırma Test : Lempel-Ziv algoritması kullanarak test edilen dizinin en çok ne kadar sıkıştırılabileceğinin belirlenmesidir.
- Seri Testi: Tekrar eden m bitlik 2m tane bloğun tekrar sayısının dağılımı inceler.
- Yaklaşık Entropi Testi: İki ardışıl uzunlukta (m ve m+1) tekrarlayan bloğun frekansını, rasgele bir dizinin beklenen frekans değeri ile karşılaştırmaktır.
- Kümülatif Toplam Testi: Bu test, bir dizide ayarlanmış (-1, +1) dijitlerin kümülatif toplamı olarak tanımlanan, rastgele yürüyüş (random walk) maksimal gezinimlerin araştırılmasına dayanır. Testin amacı, test edilen dizide bulunan kısmi altdizilerin kümülatif toplamlarının, rastgele olduğu bilinen bir dizinin beklenen değerine göre çok büyük veya çok küçük olup olmadığının belirlenmesidir. Bu kümülatif toplam, rastgele bir yürüyüş olarak kabul edilebilir.
- Rasgele Yürüyüş Testi: Bu test, kümülatif toplam rasgele yürüyüşündeki tam olarak K ziyaretlik çevrimin sayısına odaklanır.

- Rasgele Yürüyüş Değişken Testi: Bu testte, bir kümülatif toplam rasgele yürüyüşünde, özel bir durumun ziyaret edilme sayısı ölçülür. Testin amacı, bir rasgele yürüyüşte özel durumların beklenen ziyaret sayısındaki sapmalarının gözlenmesidir

İstatistiki rasgelelik testleri genellikle hipotez testleri olarak bilinirler. Testlerin hipotezi kabul veya ret etmesine göre test sonuçları başarılı veya başarısız olarak sonuçlandırılır. NIST testlerinde $\alpha = 0.01$ hipotezi ortaya koyulur. Her bir istatistiki test için hesaplana p-değerlerinin α değerinden büyük olması istenir. Çizelge 6.4'de verilen test sonuçlarından görülebileceği gibi lojistik harita kullanılarak üretilen sözde rasgele sayı dizisi tüm istatistiki testleri başarılı olarak geçmiştir. Ancak bir önceki bölümde elde edilen deneysel sonuçlar lojistik haritanın rasgelelik özelliklerinin beklenenden kötü olduğunu göstermiştir. Bu yüzden istatistiki rasgelelik testleri kriptolojik tasarımların güvenlik analizinde tek başına bir değerlendirme kriteri olarak kullanılamayacağı gösterilmiştir.

6.6 Özet

Kaos ve kriptoloji bilimleri benzer özellikler göstermesinden dolayı aralarında güçlü bir bağlantı vardır. Ancak iki disiplin arasındaki benzerliklerin yanı sıra farklılıklarda detaylı olarak irdelenmelidir. İki disiplin arasındaki en dikkat çekici ayrımlardan biri kaotik sistemlerin faz uzayının reel sayılar üzerinde tanımlı olmasına rağmen kriptolojik sistemlerin tam sayıların bir kümesini temel alarak tasarlanmasıdır. Dolayısıyla kaotik sistemler kriptolojik uygulamalarda kullanılacaksa bir ayrıklaştırma işlemine gereksinim duyulmaktadır. Ayrıklaştırma işlemi sonucunda bir sayısal kötüleşme meydana geleceği şifreleme algoritmalarında yaygın şekilde kullanılan lojistik harita üzerinde deneysel olarak gösterilmiştir. Sonuç olarak kaotik sistemler yeni kriptolojik sistemlerin tasarımında kullanılacaksa sayısal kötüleşmenin etkileri iyi incelenmelidir. Bu çalışmada hesaplama duyarlılığına bağlı olarak sayısal kötüleşmeden dolayı ortaya çıkan ve kaotik sistemin davranışında meydana gelen bozulmalar incelenmiştir. Bu sonuç kaosun kriptolojik uygulamalar için gerçekten uygun olup olmadığı sorusunun yeniden tartışılması gerektiğini ön plana çıkarmıştır.

Çizelge 6.4 İstatistiki test sonuçları

Test Adı	**p-değeri**
Frekans (Frequency) Testi	0.021999
Blok-freakans (Block-frequency) Testi	0.016717
İleri Yönlü Kümülatif Toplam (Cumulative-sums/forward) Testi	0.042808
Geri Yönlü Kümülatif Toplam (Cumulative-sums/reverse) Testi	0.455937
Akış (Runs) Testi	0.419021
En Uzun Birler Akış (Longest-runs of ones) Testi	0.616305
İkili Matris Rank (Rank) Testi	0.534146
Ayrık Fourier Dönüşüm (FFT) Testi	0.455937
Örtüşen Şablon Eşleştirme (Overlapping-templates) Testi	0.137282
Örtüşmeyen Şablon Eşleştirme (Non-periodic-templates) Testi	0.224821
Maurer's Universal İstatistiksel (Universal) Testi	0.739918
Yaklaşık Entropi (Approximate entropy) Testi	0.554420
Rasgele Yürüyüş (Random-excursions)Testi	0.585209
Rasgele Yürüyüş Değişken (Random-excursions Variant) Testi	0.422034
Seri 1 (Serial 1) Testi	0.025193
Seri 2 (Serial 2) Testi	0.334538
Doğrusal Karmaşıklık (Linear-complexity) Testi	0.935716

BÖLÜM 7

SONUÇ VE ÖNERİLER

Kaotik doğrusal olmayan dinamik sistemler rasgele gürültü benzeri bir karakteristiğe sahiptir. Kaotik sistemlerin bu özelliği iletişim teorisi, kriptoloji ve bilgisayar benzetimleri gibi çok geniş bir alanda uygulama alanı bulmaktadır. Ancak kaos ve uygulama alanları arasındaki ilişkininin yanlış anlaşılması sonucunda birçok zayıf öneri ortaya çıkmıştır.

Kaos tabanlı şifreleme algoritmalarının temeli iki disiplin arasındaki paralelliklere dayanmaktadır. Kaotik sistemler başlangıç koşulları ve kontrol parametrelerindeki değişimlere hassas bağımlıdır. Bu bağımlılık ve kaotik sistemlerin doğrusal olmayan dinamiklerini kullanarak; şifreli metnin elde edilmesinde anahtar ve açık metne olan aşırı bağımlığı sağlanmış olur. Ayrıca kaotik iterasyonlar ile açık metin ile şifreli metin arasındaki istatistiki bağımlılık ortadan kaldırılmış olur. Sonuç olarak kaotik dinamikler kullanılarak bir kriptolojik sistem için temel gereksinimler olan karıştırma ve yayılma özellikleri sağlanabilir.

Ancak iki disiplin arasındaki benzerliklerin yanı sıra farklılıklarda dikkat çekmektedir. Bu farklılıkların genellikle teoriden pratik uygulamalara geçildiğinde ortaya çıkması sadece teorik temellere dayandırılan birçok algoritmanın zayıf, yavaş veya güvensiz olarak nitelendirilmesine sebep olmaktadır.

Teori ve pratik arasındaki farkların ortak sebepleri incelendiğinde aşağıdaki problemlerin ön plana çıktığı görülmektedir. Bu problemler:

- Şifreleme algoritmalarının tasarımında protokollerin olmaması veya protokollerin belirsizlikler içermesi

- Kriptolojik tasarım süreçlerine dikkat edilmeden oluşturulmuş protokollerin ne kadar güvenli olduğunun kanıtlanmaması
- Kriptanaliz çalışmalarının olmaması veya eksikliği
- Farklı tanım kümelerine sahip olan kaos ve kriptoloji yapılarını bir arada kullanmak için uygulanan dönüşüm işlemleri sonucunda hesaplama duyarlılığına bağlı olarak bir sayısal kötüleşmenin meydana gelmesi ve bu kötüleşmenin tasarlanan sistem üzerindeki etkilerinin analiz edilmemesi

olarak sıralanabilir.

7.1 Tez Çıktılarının Literatüre Katkıları

Tez çalışmasında yukarıda belirtilen problemleri gidermek için çeşitli önerilerde bulunulmuştur. Çıktı olarak aşağıda sıralanan katkılar literatüre kazandırılmıştır.

- Kriptolojik tasarım süreci özetlenerek protokollerin önemine değinilmiştir. İster klasik isterse kaos tabanlı tasarımların mutlaka bir protokol ile ifade edilmesi gerektiği vurgulanmıştır.
- Temel kriptanaliz yöntemleri özetlenmiş; kaos tabanlı kriptolojik tasarımlara uygulanabilecek genel bir saldırı senaryosu verilmiştir.
- Saldırı senaryosunun uygulaması 11 farklı kaos tabanlı şifreleme algoritması üzerinde gösterilmiştir. Saldırıların birçoğunun benzer hataları tekrarladığı görülmüştür. Bu hatalar aşağıda özetlenmiştir.
    - Analiz edilen şifreleme algoritmalarının çeşitli cebirsel bağımlılıklar içerdiği görülmüştür.
    - Saldırıların birçoğu; algoritmalarda kaotik sistemler ile birlikte kullanılan mod işlemi veya sürekli değerlerin ayrık değerlere dönüştürülmesi işlemi gibi yapıların değişme, birleşme özelliği gibi temel özelliklerini kullanarak tasarlanmıştır.

- Algoritma tasarımında açık metin veya şifreli metin değerlerinin özel seçilmesi durumunda sistemin nasıl etkileneceğine iyi analiz edilmemiştir.
- Algoritmalarda EKG verileri, DNA işlemleri veya “Game of Life” benzeri optimizasyon süreçleri gibi çeşitli yapılar kullanılarak sistemin karmaşıklığının artırılması düşünülmüş ancak bu yapıların kriptolojik olarak birçok açıklığa sebep olduğu saldırılarda gösterilmiştir. Bu sonuçlar ile kriptolojik son işlemin önemi ortaya çıkmıştır.
- Anahtar uzayı şifreleme sistemindeki parametre sayısıyla ilişkilendirilerek kaba kuvvet saldırılarına karşı algoritmaların çok geniş bir anahtar uzayına sahip olması istenmiştir. Ancak parametreler arasındaki bağımlılık ve çeşitli düzenlemeler ile anahtar uzaylarının kolayca indirgenebileceği gösterilmiştir.

- Kaotik sistemlerin sayısal bilgisayarlar üzerinde gerçekleştirilmesi ile hesaplama duyarlılığına bağlı olarak yuvarlama, kesme işlemlerinden dolayı bir sayısal kötüleşmenin meydana geleceği gösterilmiştir. Sayısal kötüleşme sonucunda kaotik sistem rasgele benzeri bir davranış yerine periyodik bir davranış göstereceği ve temel kriptolojik gereksinimlerin sağlanmayacağı gösterilmiştir.
- Birçok şifreleme algoritmasında rasgelelik kaynağı olarak kullanılan lojistik harita standart rasgelelik testlerini geçmesine rağmen rasgelelik özelliklerinin standart bir rasgele fonksiyondan daha kötü olduğu deneysel olarak gösterilmiştir.
- Kriptolojik olarak güçlü özelliklere sahip olmayan yapıların bile istatistiki rasgelelik testlerini geçebilmektedir. Tasarımcıların kriptolojik rasgelelik ile olasılıksal rasgeleliği birbirinden net bir şekilde ayırması gerekmektedir. Bu yüzden istatistiksel rasgelelik testlerinin kriptolojik yapıların güvenlik analizinde tek başına bir değerlendirme kriteri olarak kullanılamayacağı gösterilmiştir.

7.2 Öneriler

İlerideki çalışmalarda kaos teorisi kriptolojik tasarımlarda kullanılacak ise tasarımlar kriptolojik bir protokole dayandırılmalı, kriptanaliz işlemi detaylı olarak yapılmalı ve mutlaka sayısal kötüleşmenin etkileri göz önünde bulundurulmalıdır. Kaotik kriptoloji konusunda çalışacak araştırmacıların aşağıda konu başlıklarını değerlendirmesinin literatüre yeni kazanımlar sağlayacağı düşünülmektedir.

- Kriptoloji ve kriptanaliz arasındaki ilişki göz önünde bulundurulursa literatürün gelişimi için yeni kriptanaliz çalışmaları yapılmalı ve bütün tasarımlara uygulanabilecek genel saldırı yöntemleri araştırılmalıdır.
- Kaotik sistemlerin sayısal bilgisayarlar üzerinde gerçekleştirilmesi ile meydana gelen sayısal kötüleşme sadece kriptoloji biliminde değil kaosun uygulaması bulunan birçok alanda temel bir problemdir. Bu problemi gidermek için kaotik sistemleri daha iyi tanımlayabilecek yeni veri gösterim biçimleri araştırılmalıdır.
- Kaos ve kriptoloji bilimleri arasındaki ilişkiyi sadece yeni tasarımların gerçekleştirilmesinde kullanmak yerine dinamik sistemler teorisindeki çeşitli araçları kullanılarak klasik şifreleme algoritmalarının analizinde nelerin elde edilebileceği araştırılmalıdır.
- Kaotik zaman serilerinin kestirim ve analizi için kullanılan yöntemler ile kriptanaliz çalışmalarında nelerin elde edilebileceği araştırılmalıdır.

KAYNAKLAR

[1] Canbek, G. ve Sağıroğlu Ş., (2007). "Bilgisayar Sistemlerine Yapışan Saldırılar ve Türleri: Bir İnceleme", Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23:1-12.

[2] Vizyon 2023 Teknoloji Öngörüsü Projesi Bilgi ve İletişim Teknolojileri Paneli Sonuç Raporu (2004).

[3] Koç, Ç., (2009). Cryptographic Engineering, Springer-Verlag.

[4] Katz, J.ve Lindell, Y., (2008). Introduction to modern cryptography : principles and protocols, Chapman & Hall.

[5] Paar, C. ve Pelzl, J., (2010). Understanding Cryptography A Textbook for Student and Practitioners, Springer.

[6] Stinson, D., (2007). Cryptography Theory and Practice Third Edition, Chapman & Hall.

[7] Bellare, M., (2008). Ders Notları. http://cseweb.ucsd.edu/~mihir/cse207 16 Eylül 2013.

[8] Alligood, K.T., Sauer, T.D. ve Yorke, J.A., (1997). Chaos, Springer-Verlag.

[9] Strogatz, S.H., (1994). Nonlinear Dynamics and Chaos, Perseus Books Publishing.

[10] Parker, T.S. ve Chua, L.O., (1989). Practical Numerical Algorithms for Chaotic Systems, Springer-Verlag.

[11] Baker, G.L. ve Gollub, J.P., (1990). Chaotic Dynamics, Cambridge University Press, Cambridge.

[12] Hilborn, R.C., (2003). Chaos and Nonlinear Dynamics, Oxford University Press.

[13] Özer, A. B. ve Akın, E., (2005). "Tools for Detecting Chaos", Sakarya Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 9/1.

[14] Antoine, J., (2009). Algorithmic cryptanalysis, Chapman & Hall.

[15] Bard, G., (2008). Algebraic Cryptanalysis, Springer-Verlag.

[16] Stamp, M. ve Low, R., (2007). Applied cryptanalysis : breaking ciphers in the real world, John Wiley & Sons, Inc.

[17] Arroyo, D., (2009). Framawork for the analysis and design of encryption strategies based on discrete time chaotic dynamical system, Instituto de Fı´sica Aplicada.

[18] Çokal, C., (2008). Security of Chaotic Cryptosystems, Işık Üniversitesi Fen Bilimleri Enstitüsü.

[19] Chi, L., (2005). Study and implementation of probabilistic block ciphet algorithm, City University of Hong Kong.

[20] Shujun, L., (2003). Analyses and New Designs of Digital Chaotic Ciphers, Jiaotong University.

[21] Sprott, J., (2010) Elegant Chaos Algebraically Simple Chaotic Flows, World Scientific.

[22] Baptista, M. S., (1998). "Cryptography with chaos", Physics Letters A, 240:50-54.

[23] Alvarez, G., Amigo, J. M., Arroyo, D. ve Li, S., (2011). "Lessons Learnt from the Cryptanalysis of Chaos-Based Ciphers", In: L. Kocarev, S. Lian (Eds.), Chaos Based Cryptography Theory Algorithms and Applications Springer-Verlag, 257-295.

[24] Solak, E., (2011). "Cryptanalysis of Chaotic Ciphers", In: L. Kocarev, S. Lian (Eds.), Chaos Based Cryptography Theory Algorithms and Applications Springer-Verlag, 227-256.

[25] Shannon, CE., (1949). "Communication theory of secrecy system", Bell Syst Tech J, 28:656–715.

[26] Amigo, J. M., Kocarev, L. ve Szczapanski, J., (2007). "Theory and practice of chaotic cryptography", Physics Letters A, 366:211-216.

[27] Alvarez, G. ve Li, S., (2006). "Some basic cryptographic requirements for chaos-based cryptosystems", International Journal Bifurcation and Chaos, 16/8:2129–2153.

[28] Jakimoski, G. ve Kocarev, L., (2001). "Chaos and cryptography: block encryption ciphers", IEEE Trans Circ Syst—I 48/2:163–169.

[29] Tang, G., Liao, X. ve Chen, Y., (2005). "A novel method for designing S-boxes based on chaotic maps", Chaos Solitons Fract 23:413-419.

[30] Tang, G. ve Liao, X., (2005). "A method for designing dynamical S-boxes based on discretized chaotic map", Chaos Solitons Fractals, 23/5:1901–1909.

[31] Chen, G., Chen, Y. ve Liao, X., (2007). "An extended method for obtaining S-boxes based on 3-dimensional chaotic baker maps", Chaos, Solitons & Fractals, 31:571–579.

[32] Chen, G., (2008). "A novel heuristic method for obtaining S-boxes". Chaos, Solitons & Fractals 36:1028–1036.

[33] Wang, Y., Wong, K., Liao, X. ve Xiang, T., (2009). “A block cipher with dynamic S-boxes based on tent map”, Commun Nonlinear Sci Numer Simulat, 14:3089–3099.

[34] Yin, R., Yuan, J., Wang, J., Shan, X. ve Wang, X., (2009). “Designing key-dependent chaotic S-box with larger key space”, Chaos, Solitons and Fractals, 42:2582–2589.

[35] Özkaynak, F. ve Özer, A. B., (2010). “A method for designing strong S-Boxes based on chaotic Lorenz system”, Physics Letters A, 374:3733–3738.

[36] Jakimoski, G. ve Kocarev, L., (2001). “Logistic map as a block encryption algorithm”, Physics Letters A, 289:199–206.

[37] Wong, K., (2002). “A fast chaotic cryptographic scheme with dynamic look-up table”, Physics Letters A, 298:238–242.

[38] Wong, K., Ho, S. ve Yung, C., (2003). “A chaotic cryptography scheme for generating short ciphertext”, Physics Letters A, 310:67–73.

[39] Wei, J., Xiaofeng, L., Wong, K.ve Xiang, T., (2006). “A new chaotic cryptosystem”, Chaos, Solitons and Fractals 30:1143–1152.

[40] Shujun, L., Chen, G., Wong, K., Xuanqin, M. ve Yuanlong, C., (2004). “Baptista-type chaotic cryptosystems: problems and countermeasures”, Physics Letters A, 332:368–375.

[41] Shiguo, L., Jinsheng, S. ve Zhiquan, W., (2005). “A block cipher based on a suitable use of the chaotic standard map”, Chaos Solitons and Fractals 26:117–129.

[42] Masuda, N., Jakimoski, G., Aihara, K. ve Kocarev, L., (2006). “Chaotic Block Ciphers: From Theory to Practical Algorithms”, IEEE Trans Circ Syst—I, 53/6:1341-1352.

[43] Xiang, T., Wong, K. ve Xiaofeng, L., (2008). “An improved chaotic cryptosystem with external key”, Communications in Nonlinear Science and Numerical Simulation, 13:1879–1887.

[44] Arifin, M. ve Noorani, M., (2008). “Modified Baptista type chaotic cryptosystem via matrix secret key”, Physics Letters A, 372:5427–5430.

[45] Shiguo, L., (2009). “A block cipher based on chaotic neural Networks”, Neurocomputing, 72:1296–1301.

[46] Wang, X. ve Qing, Y., (2009). “A block encryption algorithm based on dynamic sequences of multiple chaotic systems”, Communications in Nonlinear Science and Numerical Simulation, 14:574–581.

[47] Yang, H., Xiaofeng, L., Wong, K., Zhang, W.ve Wei, P., (2009). “A new block cipher based on chaotic map and group theory”, Chaos, Solitons and Fractals, 40:50–59.

[48] Yang, H., Xiaofeng, L., Wong, K., Zhang, W. ve Wei, P., (2009). “A new cryptosystem based on chaotic map and operations algebraic”, Chaos, Solitons and Fractals, 40:2520–2531.

[49] Yang, D., Xiaofeng, L., Wang, Y., Yang, H. ve Wei, P., (2009). “A novel chaotic block cryptosystem based on iterating map with output-feedback”, Chaos, Solitons and Fractals, 41:505–510.

[50] Stojanovski, T. ve Kocarev, L., (2001). “Chaos-Based Random Number Generators—Part I: Analysis”, IEEE Trans Circ Syst—I, 48/3:1-12.

[50] Li, P., Li, Z., Halang, W. ve Chen, G., (2006). “A multiple pseudorandom-bit generator based on a spatiotemporal chaotic map”, Physics Letters A, 349:467–473.

[51] Lian, S., Sun, J., Wang, J. ve Wang, Z., (2007). “A chaotic stream cipher and the usage in video protection”, Chaos, Solitons and Fractals, 34:851–859.

[52] Li, P., Li, Z., Halang, W. ve Chen, G., (2007). “A stream cipher based on a spatiotemporal chaotic system”, Chaos, Solitons and Fractals, 32:1867–1876.

[53] Hu, Y., Liao, X., Wong, K. ve Zhou, Q., (2009). “A true random number generator based on Mouse movement and chaotic cryptography”, Chaos, Solitons and Fractals, 40:2286–2293.

[54] Sun, F. ve Liu, S., (2009). “Cryptographic pseudo-random sequence from the spatial chaotic map”, Chaos, Solitons and Fractals, 41:2216–2219.

[55] Kanso, A. ve Smaoui, N., (2009). “Logistic chaotic maps for binary numbers generations”, Chaos, Solitons and Fractals, 40:2557–2568.

[56] Zhao, L., Liao, X., Xiao, D., Xiang, T., Zhou, Q. ve Duan, S., (2009). “True random number generation from mobile telephone photo based on chaotic cryptography”, Chaos, Solitons and Fractals, 42:1692–1699.

[57] Liu, N., (2011). “Pseudo-randomness and complexity of binary sequences generated by the chaotic system”, Communications in Nonlinear Science and Numerical Simulation, 16/2:761-768.

[58] Kanso, A., (2011). “Self-shrinking chaotic stream ciphers”, Communications in Nonlinear Science and Numerical Simulation, 16/2:822-836.

[59] Wong K., (2003). “A combined chaotic cryptographic and hashing scheme”, Physics Letters A, 307:292–298.

[60] Xiao, D., Liao, X.ve Deng, S., (2005). “One-way Hash function construction based on the chaotic map with changeable-parameter”, Chaos, Solitons and Fractals, 24:65–71.

[61] Zhang, J., Wang, X. ve Zhang, W., (2007). “Chaotic keyed hash function based on feedforward–feedback nonlinear digital fitler”, Physics Letters A, 362:439–448.

[62] Xiao, D., Liao, X. ve Deng, S., (2008). “Parallel keyed hash function construction based on chaotic maps”, Physics Letters A, 372:4682–4688.

[63] Deng, S., Xiao, D., Li, Y. ve Peng, W., (2009). “A novel combined cryptographic and hash algorithm based on chaotic control character”, Commun Nonlinear Sci Numer Simulat, 14:3889–3900.

[64] Ren, H., Wang, Y., Xie, Q. ve Yang, H., (2009). “A novel method for one-way hash function construction based on spatiotemporal chaos”, Chaos, Solitons and Fractals, 42:2014–2022.

[65] Amin, M., Faragallah, O. ve El-Latif, A., (2009). “Chaos-based hash function (CBHF) for cryptographic applications”, Chaos, Solitons and Fractals, 42:767–772.

[66] Akhshani, A., Behnia, S., Akhavan, A., Jafarizadeh, M., Hassan, H. ve Hassan, Z., (2009). “Hash function based on hierarchy of 2D piecewise nonlinear chaotic maps”, Chaos, Solitons and Fractals, 42:2405–2412.

[67] Akhavan, A., Samsudin, A. ve Akhshani, A., (2009). “Hash function based on piecewise nonlinear chaotic map”, Chaos, Solitons and Fractals, 42:1046–1053.

[68] Xiao, D., Liao, X. ve Wang, Y., (2009). “Improving the security of a parallel keyed hash function based on chaotic maps”, Physics Letters A, 373:4346–4353.

[69] Yang, H., Wong, K., Liao, X., Wang, Y. ve Yang, D., (2009). “One-way hash function construction based on chaotic map network”, Chaos, Solitons and Fractals, 41:2566–2574.

[70] Xiao, D., Liao, X. ve Wang, Y., (2009). “Parallel keyed hash function construction based on chaotic neural network”, Neurocomputing, 72:2288–2296.

[71] Zhang, L., Liao, X. ve Wang, X., (2005). “An image encryption approach based on chaotic maps”, Chaos, Solitons and Fractals, 24:759–765.

[72] Guan, Z., Huang, F. ve Guan, W., (2005). “Chaos-based image encryption algorithm”, Physics Letters A, 346:153–157.

[73] Gao, H., Zhang, Y., Liang, S. ve Li, D., (2006). “A new chaotic algorithm for image encryption”, Chaos, Solitons and Fractals, 29:393–399.

[74] Xiang, T., Liao, X., Tang, G., Chen, Y. ve Wong, K., (2006). “A novel block cryptosystem based on iterating a chaotic map”, Physics Letters A, 349:109–115.

[75] Yu, W. ve Cao, J., (2006). “Cryptography based on delayed chaotic neural Networks”, Physics Letters A, 356:333–338.

[76] Xiang, T., Wong, K. ve Liao, X., (2007). “A novel symmetrical cryptosystem based on discretized two-dimensional chaotic map”, Physics Letters A, 364:252–258.

[77] Behnia, S., Akhshani, A., Ahadpour, S., Mahmodi, H. ve Akhavand, A., (2007). “A fast chaotic encryption scheme based on piecewise nonlinear chaotic maps”, Physics Letters A, 366:391–396.

[78] Kwok, H. ve Tang, W., (2007). “A fast image encryption system based on chaotic maps with finite precision representation”, Chaos, Solitons and Fractals, 32: 1518–1529.

[79] Wong, K., Kwok, B. ve Law, W., (2008). “A fast image encryption scheme based on chaotic standard map”, Physics Letters A, 372:2645–2652.

[80] Gao, T. ve Chen, Z., (2008). “A new image encryption algorithm based on hyper-chaos”, Physics Letters A, 372:394–400.

[81] Behnia, S., Akhshani, A., Ahadpour, S., Mahmodi, H. ve Akhavand, A., (2008). “A novel algorithm for image encryption based on mixture of chaotic maps”, Chaos, Solitons and Fractals, 35:408–419.

[82] Sun, F., Liu, S., Li, Z. ve Lu, Z., (2008). “A novel image encryption scheme based on spatial chaos map”, Chaos, Solitons and Fractals, 38:631–640.

[83] Gao, T. ve Chen, Z., (2008). “Image encryption based on a new total shuffling algorithm”, Chaos, Solitons and Fractals, 38:213–220.

[84] Wanga, Y., Wong, W., Liao, X., Xiang, T. ve Chen, G., (2009). “A chaos-based image encryption algorithm with variable control parameters”, Chaos, Solitons and Fractals, 41:1773–1783.

[85] Yang, H., Liao, X., Wong, K., Zhang, W. ve Wei, P., (2009). “A new block cipher based on chaotic map and group theory”, Chaos, Solitons and Fractals, 40:50–59.

[86] Patidar, V., Pareek, N. ve Sud, K., (2009). “A new substitution–diffusion based image cipher using chaotic standard and logistic maps”, Commun Nonlinear Sci Numer Simulat, 14:3056–3075.

[87] Behnia, S., Akhshani, A., Ahadpour, S., Akhavand, A. ve Mahmodi, H., (2009). “Applications of tripled chaotic maps in cryptography”, Chaos, Solitons and Fractals, 40:505–519.

[88] Mazloom, S. ve Moghadam, A., (2009). “Color image encryption based on Coupled Nonlinear Chaotic Map”, Chaos, Solitons and Fractals, 42:1745–1754.

[89] Lian, S., (2009). “Efficient image or video encryption based on spatiotemporal chaos system”, Chaos, Solitons and Fractals, 40:2509–2519.

[90] Huang, C. ve Nien, H., (2009). “Multi chaotic systems based pixel shuffle for image encryption”, Opt. Commun., 282/11:2123–2127.

[91] Amin, M., Faragallah, O. ve El-Latif, A., (2010). “A chaotic block cipher algorithm for image cryptosystems”, Commun Nonlinear Sci Numer Simulat, 15:3484-3497.

[92] Yang, H., Wong, K., Liao, X., Zhang, W. ve Wei, P., (2010). “A fast image encryption and authentication scheme based on chaotic maps”, Commun Nonlinear Sci Numer Simulat, 15:3507-3517.

[93] Xing-yuan, W., Feng, C. ve Tian, W., (2010). “A new compound mode of confusion and diffusion for block encryption of image based on chaos”, Commun Nonlinear Sci Numer Simulat, 15:2479–2485.

[94] Yoon, J. ve Kim, H., (2010). “An image encryption scheme with a pseudorandom permutation based on chaotic maps”, Commun Nonlinear Sci Numer Simulat, 15:3998–4006.

[95] Tang, Y., Wanga, Z. ve Fang, J., (2010). “Image encryption using chaotic coupled map lattices with time-varying delays”, Commun Nonlinear Sci Numer Simulat, 15:2456–2468.

[96] Patidar, V., Pareek, N., Purohit, G. ve Sud, K., (2010). “Modified substitution–diffusion image cipher using chaotic Standard and logistic maps”, Commun Nonlinear Sci Numer Simulat, 15:2755–2765.

[97] Wanga, Y., Wong, K., Liao, X. ve Chen, G., (2011). “A new chaos-based fast image encryption algorithm”, Applied Soft Computing, 11:514-522.

[98] Kumar, A. ve Ghose, M., (2011). “Extended substitution–diffusion based image cipher using chaotic standard map”, Commun Nonlinear Sci Numer Simulat, 16:372-382.

[99] Álvarez, G., Montoya, F., Romera, M. ve Pastor, G., (2003). “Cryptanalysis of an ergodic chaotic cipher”, Physics Letters A, 311:172–179.

[100] Álvarez, G. Montoya, F., Romera, M. ve Pastor, G., (2004). “Cryptanalysis of dynamic look-up table based chaotic cryptosystems”, Physics Letters A, 326:211–218.

[101] Wang, Y., Xiaofeng, L., Xiang, T., Wong, K. ve Yang, D., (2007). “Cryptanalysis and improvement on a block cryptosystem based on iteration a chaotic map”, Physics Letters A, 363:277–281.

[102] Chengqing, L., Shujun, L., Alvarez, G., Chen, G. ve Lo, K., (2008). “Cryptanalysis of a chaotic block cipher with external key and its improved version”, Chaos, Solitons and Fractals, 37:299–307.

[103] Rhouma, R., Solak, E., Arroyo, D., Shujun, Li., Alvarez, G. ve Belghith, S., (2009). “Comment on “Modified Baptista type chaotic cryptosystem via matrix secret key”, Physics Letters A, 373:3398–3400.

[104] Rhouma, R. ve Belghith, S., (2009). “Cryptanalysis of a spatiotemporal chaotic cryptosystem”, Chaos, Solitons and Fractals, 41:1718–1722.

[105] Arroyo, D., Alvarez, G., Amigó, J. ve Li, S., (2011). “Cryptanalysis of a family of self-synchronizing chaotic stream ciphers”, Communications in Nonlinear Science and Numerical Simulation, 16/2:805-813.

[106] Guo, W., Wang, X., Hea, D. ve Cao, Y., (2009). “Cryptanalysis on a parallel keyed hash function based on chaotic maps”, Physics Letters A, 373:3201–3206.

[107] Deng, S., Li, Y. ve Xiao, D., (2010). “Analysis and improvement of a chaos-based Hash function construction”, Commun Nonlinear Sci Numer Simulat, 15:1338–1347.

[108] Xiao, D., Peng, W., Liao, X.ve Xiang, T., (2010). “Collision analysis of one kind of chaos-based hash function”, Physics Letters A, 374:1228–1231.

[109] Solak, E. ve Çokal, C., (2008). “Cryptanalysis of a cryptosystem based on discretized two-dimensional chaotic maps”, Physics Letters A, 372:6922–6924.

[110] Rhouma, R. ve Belghith, S., (2008). “Cryptanalysis of a new image encryption algorithm based on hyper-chaos”, Physics Letters A, 372:5973–5978.

[111] Rhouma, R. ve Belghith, S., (2008). “Cryptanalysis of a spatiotemporal chaotic image/video cryptosystem”, Physics Letters A, 372:5790–5794.

[112] Solak, E. ve Çokal, C., (2009). “Algebraic break of a cryptosystem based on discretized two-dimensional chaotic maps”, Physics Letters A, 373:1352–1356.

[113] Xiao, D., Liao, X. ve Wei, P., (2009). “Analysis and improvement of a chaos-based image encryption algorithm”, Chaos, Solitons and Fractals, 40:2191–2199.

[114] Çokal, C. ve Solak, E., (2009). “Cryptanalysis of a chaos-based image encryption algorithm”, Physics Letters A, 373:1357–1360.

[115] Arroyo, D., Li, C., Li, S., Alvarez, G. ve Halang, W., (2009). “Cryptanalysis of an image encryption scheme based on a new total shuffling algorithm”, Chaos, Solitons and Fractals, 41:2613–2616.

[116] Alvarez, G. ve Li, S., (2009). “Cryptanalyzing a nonlinear chaotic algorithm (NCA) for image encryption”, Commun Nonlinear Sci Numer Simulat, 14:3743–3749.

[117] Solak, E., Rhouma, R. ve Belghith, S., (2010). “Cryptanalysis of a multi-chaotic systems based image cryptosystem”, Optics Communications, 283:232–236.

[118] Rhouma, R., Solak, E. ve Belghith, S., (2010). “Cryptanalysis of a new substitution–diffusion based image cipher”, Commun Nonlinear Sci Numer Simulat, 15:1887–1892.

[119] Li, C., Li, S. ve Lo, K., (2011). “Breaking a modified substitution–diffusion image cipher based on chaotic standard and logistic maps”, Commun Nonlinear Sci Numer Simulat, 16:837-843.

[120] Marsaglia, G., (1996). The Marsaglia random number CDROM including the DIEHARD battery of tests of randomness.

[121] Caelli, W., Dawson, E., Nielsen, L. ve Gustafson H., (1992). CRYPT–X statistical package manual, measuring the strength of stream and block ciphers.

[122] Rukhin, A., Soto, J., Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M., Vangel, M., Banks, D., Heckert, A., Dray, J. ve Vo. S., (2001). A statistical test suite for random and pseudorandom number generators for cryptographic applications.

[123] Zhu, C., (2012). “A novel image encryption scheme based on improved hyperchaotic sequences”, Optics Communications 285/1, 29-37.

[124] Özkaynak, F., Özer, A. B. ve Yavuz S., (2012). “Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences”, Optics Communications, 285:4946–4948.

[125] Li, C., Liu, Y. ve Xie, T., (2013). “Breaking a novel image encryption scheme based on improved hyperchaotic sequences”, Nonlinear Dynamics, 73:2083-2089.

[126] Chen, C., Lin, C., Chiang, C. ve Lin, S., (2012). “Personalized information encryption using ECG signals with chaotic functions”, Information Sciences, 193:125–140.

[127] Arroyo, D., Alvarez, G., Li, S., Li, C. ve Nunez, J., (2008). “Cryptanalysis of a discrete-time synchronous chaotic encryption system”, Physics Letters A, 372:1034–1039.

[128] Zhang, Q., Guo, L. ve Wei, X., (2010). “Image encryption using DNA addition combining with chaotic maps”, Mathematical and Computer Modelling 52:2028-2035.

[129] Wangn, X., Teng, L. ve Qin, X., (2012). “A novel colour image encryption algorithm based on chaos”, Signal Processing 92:1101–1108.

[130] Arroyo, D., Rhouma, R., Alvarez, G., Li, S. ve Fernandez, V., (2008). “On the security of a new image encryption scheme based on chaotic map lattices”, Chaos, 18:124-136.

[131] Li, C., Li, S., Lo, K.-T.ve Kyamakya, K., (2010). “A differential cryptanalysis of Yen-Chen-Wu multimedia cryptography system”. Journal of Systems and Software 83/8:1443–1452.

[132] Liu, L., Zhang, Q. ve Wei, X., (2012). “A RGB image encryption algorithm based on DNA encoding and chaos map”, Computers & Electrical Engineering, 38/5:1240-1248.

[133] Bigdeli, N., Farid, Y. ve Afshar, K., (2012). “A robust hybrid method for image encryption based on Hopfield neural network”, Computers and Electrical Engineering, 38:356–369.

[134] Özkaynak, F., Özer, A. B.ve Yavuz S., (2012). “Cryptanalysis of Bigdeli algorithm using Çokal and Solak attack”, International Journal of Information Security Science, 1/3:79-81.

[135] Ahmad, M., Alam, B. ve Farooq, O., (2012). “Chaos Based Mixed Keystream Generation for Voice Data Encryption”, International Journal on Cryptography and Information Security (IJCIS), 2/1:20-28.

[136] Özkaynak, F., Özer, A. B. ve Yavuz S., (2012). “Cryptanalysis of Chaos Based Mixed Keystream Generation for Voice Data Encryption”, 3th World Conference on Information Technology, Barcelona, Spain.

[137] François, M., Grosges, T., Barchiesi, D. ve Erra, R., (2012). “A new image encryption scheme based on a chaotic function”, Signal Processing: Image Communication, 27:249–259.

[138] Machicao, J., Marco, A. G. ve Bruno, O. M., (2012). “Chaotic encryption method based on life-like cellular automata”, Expert Systems with Applications, 39/16:12626–12635.

[139] Hu, H., Liu, L. ve Ding, N., (2012). “Pseudorandom sequence generator based on Chen chaotic system”, Computer Physics Communications 184:765–768.

[140] Hermassi, H., Rhouma, R. ve Belghith, S., (2010). “Joint compression and encryption using chaotically mutated Huffman trees”, Communications in Nonlinear Science and Numerical Simulation, 15:2987-2999.

[141] Özkaynak, F., Özer, A. B. ve Yavuz S., (2012). “Analysis of Chaotic Methods for Compression and Encryption Processes in Data Communication”, 20th IEEE Signal Processing and Communications Applications Conference, Muğla, Turkey.

[142] Persohn, K.J. ve Povinelli, R.J., (2012). “Analyzing logistic map pseudorandom number generators for periodicity induced by finite precision floating-point representation”, Chaos, Solitons & Fractals 45:238–245.

[143] Dachselt, F., Schwarz, W., (2001). Chaos and cryptography. IEEE Trans Circ Syst I: Fundam Theory Appl; 48(12):1498–509.

[144] Kocarev, L., (2001). “Chaos-based cryptography: a brief overview”. IEEE Circ Syst Mag; 1:6–21.

[145] Standard for floating-point arithmetic, Tech. Rep. 754-2008, IEEE (2008).

[146] Rosen K. H., (2007). Discrete mathematics and its applications, sixth edition McGraw-Hill.

[147] Arney, J. ve Bender, E. A. (1982). “Random mappings with constraints on coalescence and number of origins”. Pacific J. Math., 103:269–294.

[148] Harris, B., (1960). “Probability distributions related to random mappings”. The Annals of Mathematical Statistics, 31:1045–1062.

[149] Hellman, M. E., (1980). “A cryptanalytic time-memory trade-of”. IEEE Transactions on Information Theory, 26:401–406.

[150] Kolchin, V. F., (1986). Random Mappings. Springer ,-Verlag.

[151] Turan, M. S., Calik, C., Saran, N. B. ve Doğanaksoy, A., (2008). “New distinguishers based on random mappings against stream ciphers”, In SETA ’08: Proceedings of the 5th international conference on Sequences and Their Applications, 30–41.

[152] Turan, M. S., (2008). On Statistical Analysis of Synchronous Stream Ciphers. Middle East Technical University, Ankara, Turkey.

[153] Özkaynak, F., Özer, A. B. ve Yavuz S., (2012). “Differential Cryptanalysis of Block Ciphers Based on Randomly Selected Substitution Boxes”, 5th

International Conference on Information Security and Cryptology, Ankara, Turkey.

[154] Özer, A. B.ve Özkaynak, F., (2010). "A Cryptographic pseudo random bit sequence generator with chaos-based coding table", 1th International Symposium on Computing in Science & Engineering, Kuşadası, Turkey.

[155] Özkaynak, F., Özer, A. B. ve Yavuz S., (2012). "Modern Kriptolojik Sistemlerin Tasarlanmasında Kaotik Dinamiklerin Uygulamaları", 1. Ulusal Karmaşık Dinamik Sistemler ve Uygulamaları Çalıştayı, Ankara.

[156] Özkaynak, F., Özer, A. B. ve Yavuz S., (2012). "Doğanın Hesapsal Güzelliklerinden Öğrendiğimiz Görüntü Şifreleme Algoritmaları", Akıllı Sistemlerde Yenilikler ve Uygulamaları Sempozyumu, Trabzon.

[157] Kırkıl, K., Özer, A. B. ve Özkaynak, F., (2012). "Kaos Tabanlı Kriptolojik Özetleme Fonksiyonları", Akıllı Sistemlerde Yenilikler ve Uygulamaları Sempozyumu, Trabzon.

[158] Özkaynak, F., Özer, A. B. ve Yavuz S., (2011). "Kaos Tabanlı Yeni Bir Blok Şifreleme Algoritması", IV. Ağ ve Bilgi Güvenliği Sempozyumu, Ankara.

[159] Özkaynak, F. ve Özer, A. B., (2010). "Kaos Tabanlı S-Box Üreteçlerinin Güçlendirilmesi için Yeni Bir Algoritma", Elektrik - Elektronik ve Bilgisayar Mühendisliği Sempozyumu, Bursa.

[160] Özkaynak, F. ve Yavuz S., (2013). "Security problems of pseudorandom sequence generator based on Chen chaotic system", Computer Physics Communications, 184:2178–2181.

[161] Özkaynak, F., Özer, A. B. ve Yavuz S., (2013). "A Security Analysis of An Image Encryption Algorithm Based on Chaos and DNA Encoding", 21th IEEE Signal Processing and Communications Applications Conference, Cyprus.

[162] Özkaynak, F., Özer, A. B., Yavuz S., (2013). "Security analysis of an encryption algorithm based on cellular automata and chaos", 6th International Conference on Information Security and Cryptology, Ankara.

[163] Özkaynak, F. ve Yavuz S., (2013). "Designing chaotic S-boxes based on time-delay chaotic system", Nonlinear Dynamics, DOI: 10.1007/s11071-013-0987-4 (in press).

[164] Rukhin, A., Soto, J. Nechvatal, J., Smid, M., Barker, E., Leigh, S., Levenson, M. Vangel, M., Banks, D., Heckert, A., Dray, J., ve Vo, S. (2001). "A statistical test suite for random and pseudorandom number generators for cryptographic applications",http://csrc.nist.gov/groups/ST/toolkit/rng/documentation_software.html, 16 Eylül 2013.

[165] Avaroğlu, E., Özer, A. B., ve Turk, M. (2013). "Rasgele Sayıları Test Etme Yöntemleri" 8. Uluslararası İstatistik Kongresi.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı	: Fatih ÖZKAYNAK
Doğum Tarihi ve Yeri	: 11.12.1983 / ELAZIĞ
Yabancı Dili	: İngilizce
E-posta	: ozkaynaklar@gmail.com

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Y. Lisans	Bilgisayar Müh.	Fırat Üniversitesi	2007
Lisans	Bilgisayar Müh.	Fırat Üniversitesi	2005
Lise		Balakgazi Lisesi	2001

İŞ TECRÜBESİ

Yıl	Firma/Kurum	Görevi
2011-devam	Fırat Üniversitesi	Araştırma Görevlisi
2011	Fırat Üniversitesi	Öğretim Görevlisi
2009-2011	Tunceli Üniversitesi	Araştırma Görevlisi
2009	Bozok Üniversitesi	Uzman

2007-2009 Bank Asya A. Ş. Yazılım Mühendisi

YAYINLARI

Makale

1. Özkaynak, F., Yavuz S., (2013). Designing chaotic S-boxes based on time-delay chaotic system, Nonlinear Dynamics, DOI: 10.1007/s11071-013-0987-4 (in press).
2. Özkaynak, F., Yavuz S., (2013). Security problems of pseudorandom sequence generator based on Chen chaotic system, Computer Physics Communications 184, 2178–2181.
3. Özkaynak, F., Özer, A. B., Yavuz S., (2012). Cryptanalysis of a novel image encryption scheme based on improved hyperchaotic sequences, Optics Communications 285, 4946–4948.
4. Özkaynak, F., Özer, A. B., Yavuz S., (2012). Cryptanalysis of Bigdeli algorithm using Çokal and Solak attack, International Journal of Information Security Science, Vol:1 No:3, 79-81.
5. Özkaynak, F., Özer, A. B., (2010). A method for designing strong S-Boxes based on chaotic Lorenz system. Physics Letters A, 374, 3733–3738.
6. Özkaynak, F., Özer, A. B., (2006). Lojistik Harita ile Rasgele Sayı Üretilmesi ve İstatistiki Yöntemlerle Sınanması, İstanbul Kültür Üniversitesi, Fen ve Mühendislik Bilimleri Dergisi, Vol. 4, No 3, 129-133.

Bildiri

1. Özkaynak, F., Özer, A. B., Yavuz S., (2013). A Security Analysis of An Image Encryption Algorithm Based on Chaos and DNA Encoding, 21th IEEE Signal Processing and Communications Applications Conference, Cyprus.
2. Kamışlıoğlu, M., Külahcı, F., Özkaynak, F., (2013). Nonlinear reply of radon and deterministic chaos. The 6th Chaotic Modeling and Simulation International Conference, Istanbul, Turkey.
3. Özkaynak, F., Özer, A. B., Yavuz S., (2012). Analysis of Chaotic Methods for Compression and Encryption Processes in Data Communication, 20th IEEE Signal Processing and Communications Applications Conference, Muğla, Turkey.
4. Özkaynak, F., Özer, A. B., Yavuz S., (2012). Differential Cryptanalysis of Block Ciphers Based on Randomly Selected Substitution Boxes, 5th International Conference on Information Security and Cryptology, Ankara, Turkey.
5. Özkaynak, F., Özer, A. B., Yavuz S., (2012). Cryptanalysis of Chaos Based Mixed Keystream Generation for Voice Data Encryption, 3th World Conference on Information Technology, Barcelona, Spain.

6. Özer, A. B., Özkaynak, F., (2010). A Cryptographic pseudo random bit sequence generator with chaos-based coding table", 1th International Symposium on Computing in Science & Engineering, Kuşadası, Turkey.
7. Özkaynak, F., Özer, A. B., Yavuz S., (2013). Kriptolojik Uygulamalarda İstatistiki Rasgelelik Testlerinin Problemleri, Kripto Günleri, Bilgem/Tübitak.
8. Özkaynak, F., Özer, A. B., Yavuz S., (2012). Modern Kriptolojik Sistemlerin Tasarlanmasında Kaotik Dinamiklerin Uygulamaları, 1. Ulusal Karmaşık Dinamik Sistemler ve Uygulamaları Çalıştayı, Ankara.
9. Özkaynak, F., Özer, A. B., Yavuz S., (2012). Doğanın Hesapsal Güzelliklerinden Öğrendiğimiz Görüntü Şifreleme Algoritmaları, Akıllı Sistemlerde Yenilikler ve Uygulamaları Sempozyumu, Trabzon.
10. Kırkıl, K., Özer, A. B., Özkaynak, F., (2012). Kaos Tabanlı Kriptolojik Özetleme Fonksiyonları, Akıllı Sistemlerde Yenilikler ve Uygulamaları Sempozyumu, Trabzon.
11. Özkaynak, F., Özer, A. B., (2012). Yazılım Proje Yönetiminde Kullanılan Sezgisel Yöntemlerinin Geliştirilmesi için Kaos Tabanlı Çözümler, VI. Ulusal Yazılım Mühendisliği Sempozyumu, Ankara.
12. Özkaynak, F., Özer, A. B., Yavuz S., (2011). Kaos Tabanlı Yeni Bir Blok Şifreleme Algoritması, IV. Ağ ve Bilgi Güvenliği Sempozyumu, Ankara.
13. Özkaynak, F., Özer, A. B., (2010). Kaos Tabanlı S-Box Üreteçlerinin Güçlendirilmesi için Yeni Bir Algoritma, Elektrik - Elektronik ve Bilgisayar Mühendisliği Sempozyumu, Bursa.
14. Özkaynak, F., Öksüztepe E., (2010). Kaotik Zaman Serilerinin Analizi, Bilimde Modern Yöntemler Sempozyumu.

Proje

1. Doğrusal Olmayan Sistemlerde Lyapunov Üstellerini Hesaplayan Yazılımın Gerçekleştirilmesi (FÜBAP-Fırat Üniversitesi Bilimsel Araştırma Projeleri Birimi), 2005-2007 (Araştırmacı).