T.C.
HALİÇ ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
MATEMATİK ANABİLİM DALI
UYGULAMALI MATEMATİK TEZLİ YÜKSEK LİSANS PROGRAMI

KUANTUM KRİPTOGRAFİSİ: TEORİK KAVRAMLAR İLE PRATİK UYGULAMA ARASINDAKİ İLİŞKİ

YÜKSEK LİSANS TEZİ

Hazırlayan
Fatih Ali KOÇ

Tez Danışmanı
Dr. Öğr. Üyesi Nebi ÖNDER

İSTANBUL
Şubat 2024

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜ'NE

Matematik Anabilim Dalı Yüksek Lisans Programı Öğrencisi Fatih Ali KOÇ tarafından hazırlanan "Kuantum kriptografisi: Teorik kavramlar ile pratik uygulama arasındaki ilişki" konulu çalışması jürimizce Yüksek Lisans Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi: .....

Jüri Üyesinin Ünvanı, Adı, Soyadı ve Kurumu: İmzası

Jüri Üyesi : Dr. Öğr. Üyesi Nebi ÖNDER
Haliç Üniversitesi

Jüri Üyesi : Dr. Öğr. Üyesi Abdullah Serdar KAZANCIOĞLU
İstanbul Beykent Üniversitesi

Jüri Üyesi Dr. Öğr. Üyesi Hasan Halit TALİ
Haliç Üniversitesi

Bu tez yukarıdaki jüri üyeleri tarafından uygun görülmüş ve Enstitü Yönetim Kurulu'nun kararıyla kabul edilmiştir.

Prof. Dr. Nihat İNANÇ
Müdür

KUANTUM KRİPTOLOJİSİ

ORİJİNALLİK RAPORU

%2	%2	%0	%2
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	Submitted to University of Maryland, University College Öğrenci Ödevi	%1
2	Submitted to The Scientific & Technological Research Council of Turkey (TUBITAK) Öğrenci Ödevi	<%1
3	en.wikipedia.org İnternet Kaynağı	<%1
4	9lib.net İnternet Kaynağı	<%1
5	openaccess.ogu.edu.tr:8080 İnternet Kaynağı	<%1
6	eprints.whiterose.ac.uk İnternet Kaynağı	<%1
7	tel.archives-ouvertes.fr İnternet Kaynağı	<%1
8	www5.tbmm.gov.tr İnternet Kaynağı	<%1

26/01/2024

TEZ ETİK BEYANI

Yüksek Lisans Tezi olarak sunduğum “Kuantum Kriptografisi: Teorik Kavramlar İle Pratik Uygulama Arasındaki İlişki” başlıklı bu çalışmayı baştan sona kadar danışmanım Dr. Öğr. Üyesi Nebi ÖNDER’ın sorumluluğunda tamamladığımı, verileri/örnekleri kendim topladığımı, analizleri ilgili laboratuvarlarda yaptığımı/yaptırdığımı, başka kaynaklardan aldığım bilgileri metinde ve kaynakçada eksiksiz olarak gösterdiğimi, çalışma sürecinde bilimsel araştırma ve etik kurallara uygun olarak davrandığımı ve aksinin ortaya çıkması durumunda her türlü yasal sonucu kabul ettiğimi beyan ederim.

Fatih Ali KOÇ

ÖNSÖZ

Bu çalışmanın gerçekleşmesinde büyük desteği olan, çalışmamın her aşamasında sabırla gece ve gündüz demeden yardımcı olan, beraber çalışmaktan gurur duyduğum, çok kıymetli danışman hocam Dr. öğr. Üyesi Nebi ÖNDER'e, sonsuz teşekkür ederim.

Ayrıca bu çalışmamda her zaman beni motive eden, maddi manevi desteğini hiçbir zaman eksik etmeyen, yıkıldığım zaman ayakta durmamı sağlayan kardeşlerim Şaban KOÇ, Recep KOÇ ve Yasin KOÇ'a teşekkür ederim.

Son olarak beni hiçbir zaman yalnız bırakmayan, aldığım kararlarda beni koşulsuz destekleyen ve cesaretlendiren eşim Fatma KOÇ'a, aynı üniversitede beraber okuduğumuz oğlum Muhammed Ali KOÇ'a ve babam Bayram Ali KOÇ'a sonsuz şükranlarımı sunar ve teşekkür ederim.

Ocak 2024 Fatih Ali KOÇ

İÇİNDEKİLER

Sayfa No

KISALTMALAR

ABD : United States Of America
AES : Advanced Encryption Standard
BBM92 : Proposed in 1992 by Bennett, Brassard and Mermin
BB84 : Proposed in 1984 by Bennett and Brassard
DES : Data Encryption Standard
DC : District Of Columbia
Dr : Doctor
EDP : Electronic Data Processing
EPR : Einstein-Poddsky-Rosen
E91 : Proposed by Artur Ekert in 1991
GLLP : Global Laboratory Leadership
JN25 : Japanese Navy its operational code
NIST : National Institute Of Standards And Technology
NY : New York
PDC : Trigger parametric down transform
PQC : Post Quantum Cryptografi
QKD : Quantum Key Distribution
SIS : Secret Intelligence Service
SPD : Single Photon Detector
SOE : Stade Owned enterprise
VIC : Vigenere

ŞEKİL LİSTESİ

Sayfa No

ÖZET

KUANTUM KRİPTOGRAFİSİ: TEORİK KAVRAMLAR İLE PRATİK UYGULAMA ARASINDAKİ İLİŞKİ

Bu proje, tarihsel köklerinin araştırılmasıyla başlayıp çağdaş uygulamalara doğru ilerleyerek kriptografinin evrimini araştırmayı amaçlamaktadır. Kuantum kriptografisinin ortaya çıkışına ve kuantum bilişim çağında bilginin güvenliği üzerindeki dönüştürücü etkisine özel önem verilmektedir. Çalışma, teorik kavramları pratik uygulamayla birleştirmeyi, kuantum dirençli kriptografik algoritmaların geliştirilmesine ve bunların gelecekteki siber güvenlik üzerindeki etkilerine dair içgörüler sunmayı amaçlamıştır.

Anahtar Kelimeler : *Kriotografi, Kuantum Mekaniği*

ABSTRACT

QUANTUM CRYPTOGRAPHY: RELTİONSHİP BETWEEN THEORETİCAL CONCEPTS WİTH PRACTİCAL IMPLEMENTATİON

This project aims to investigate evolution of cryptography, commencing with an exploration of its historical roots and progressing towards contemporary applications. Special emphasis is placed on the advent of quantum cryptography and its transformative impact on securing information in the era of quantum computing. The study aims to bridge theoretical concepts with practical implementation, offering insights into the development of quantum-resistant cryptographic algorithms and their implications for future cybersecurity.

Keywords : *Cryptography, Quantum Mechanics*

1. GİRİŞ

Günümüzde, teknolojik gelişmelerin temelinde bilginin kesintisiz iletimi yatmaktadır. Dijital iletişimin yaygınlaşmasıyla birlikte, sağlam şifreleme tekniklerine duyulan ihtiyaç giderek daha hayati hale gelmiştir. Bu çalışma, kriptografinintarihsel ve evrimsel gelişimine odaklanarak, günümüzde de oldukça yaygınlaşan bir alt kolu olan Kuantum Kriptografisinin derinlemesine analizini hedeflemektedir. Araştırma, teorik kavramları pratik uygulamalarla kıyaslayarak, kriptografik teori ile gerçek dünya uygulamaları arasında devam eden ilişkilerini incelemeyi amaçlamaktadır.

Çalışma, kriptografinin tarihsel temellerinin geriye dönük incelenmesiyle başlamakta ve farklı çağlarda bilginin güvenliğinde kullanılan yöntemlerin ortaya çıkarılmasıyla devam etmektedir. Bu tarihsel perspektif, kriptografik protokollerdeki kuantum ilerlemelerinin getirdiği devrim niteliğindeki değişimlerin anlaşılmasını da kolaylaştıracaktır.

Kuantum bilgi işlemenin temel ilkeleri projenin temelini oluşturmaktadır. Kuantum mekaniği, klasik meknikten ve fiziği klasik kurallarından farklı olan özellikleriyle kuantum şifreleme sistemlerini dah karmaşık hale getirmektedir.

Klasik kriptografik tekniklerin ayrıntılı bir şekilde incelenmesi, yenilikçi yaklaşımlara olan ihtiyacın altını çizmektedir. Geleneksel kriptografik yöntemler etkili olsa da, kuantum bilgisayarların varlığının hakim olduğu bir çağda benzeri görülmemiş zorluklarla karşı karşıyadır.

Araştırmanın temel konusu Kuantum Kriptografisidir. Bu konudan 3. Ve 4. bölümlerde detaylı bir şekilde bahsetmek amaçlanmıştır. Kuantum mekaniğinin ilkelerini kullanan kuantum kriptografisi, öncelikle Kuantum Anahtar Dağıtımı (QKD) protokolleri aracılığıyla iletişim kanallarının güvenliğini sağlamada bir paradigma değişikliği sunmaktadır.

Hem klasik hem de kuantum kriptografik sistemlerdeki potansiyel güvenlik açıklarının ve karşı önlemlerin analizi esastır. Son bölümde kriptanaliz ile yeni ortaya çıkan kuantum kriptanaliz alanının kesişimi araştırılmıştır.

2. KRİPTOGRAFİNİN TARİHÇESİ

Gizli bilgileri korumak için şifreler ve kodlar kullanma uygulaması olan kriptografinin binlerce yıla yayılan zengin bir geçmişi vardır. Geleneksel olarak klasik kriptografi olarak bilinen yöntemler, daha önceki yıllarda kullanılan yöntemler, genellikle kalem ve kağıt veya temel mekanik yardımları içeren manuel işlemlere dayanıyordu. Bununla birlikte, 20. yüzyılın başlarındaki önemli ilerlemeler, Enigma rotor makinesi gibi karmaşık mekanik ve elektromekanik cihazların yaratılmasıyla kolaylaştırılan daha karmaşık ve etkili şifreleme tekniklerine doğru bir kaymaya işaret etmiştir. Daha sonra bilgisayarların ve elektronik cihazların piyasaya sürülmesi, karmaşık şifreleme şemalarının olanaklarını daha da genişletmiş ve bunların çoğunu geleneksel kalem ve kâğıt yöntemleriyle uygulama için kullanışsız hale getirmiştir (History of Cryptography, t.y.).

Kodları ve şifreleri deşifre etmeye ve çözmeye odaklanan disiplin olan kriptoanaliz, kriptografi alanıyla birlikte gelişmiştir. Tarihsel olaylar bazen, şifreli iletişimin şifresinin çözülmesinde frekans analizinin kullanılması gibi erken buluşlar nedeniyle değiştirilmiştir. Dikkate değer örnekler arasında, Amerika Birleşik Devletleri'ni Birinci Dünya Savaşı'na sürükleyen Zimmermann Telgrafının etkisi ve Nazi Almanyası'nın şifrelerinin açığa çıkması ve potansiyel olarak Müttefikler için II. Dünya Savaşı'nı iki yıl uzatması sayılabilir (History of Cryptography, t.y.).

Geleneksel olarak güvenli kriptografi, 1960'lara kadar öncelikle hükümetlerin alanı olmuştur. Bununla birlikte, iki önemli gelişme kriptografiyi kamusal alana itmiştir: açık anahtarlı kriptografinin tanıtılması ve genel şifreleme standardının (DES) oluşturulması (History of Cryptography, n.d.)

Kriptografinin bilinen ilk kullanımı, milattan önce 1900 civarında duvara standart olmayan hiyerogliflerin kazındığı Eski Mısır Krallığı'na ait bir mezarda görülebilir. Bununla birlikte, bunların gerçek gizli iletişim girişimlerinden ziyade

okuryazar seyirciler için gizem, entrik ve hatta eğlence girişimleri olduğuna inanılmaktadır (2001).

Biraz daha sonra, bir zanaatkarın muhtemelen ticaret açısından değerli olan seramik sır tarifini kodlayan Mezopotamya kil tabletleri bulunmuştur. Milattan önce 1500 yıllarına tarihlenen bu tabletlerden birinin amacının bilgiyi korumak olduğu açıktır. Buna ek olarak İbrani entelektüeller, muhtemelen MÖ 600-500 yıllarında Atbash şifresi de dahil olmak üzere temel tek alfabeli ikame şifrelerini kullanmaya başlamışlardır (2001).

Kama Sutra, şifreli yazıları yorumlama ve kelimeleri kendine özgü bir şekilde oluşturma becerisini ifade eden ve milattan önce 400'den milattan sonra 200'e kadar Hindistan'daki aşıklar arasında bir iletişim biçimi olarak hizmet eden "Mlecchita vikalpa" kavramını tanıtmıştır. Bu muhtemelen basit bir ikame şifresini içeriyordu. Şifreli yazının kullanımı, bazı Mısır demotik Yunan Büyülü Papirüslerinde de açıkça görülmektedir (2001).

Antik Yunanlıların şifre bilgisine sahip olduğuna inanılıyor, ancak Sparta ordusu tarafından tırpan transpozisyon şifresinin kullanımının ardındaki amaç belirsizliğini koruyor. Bu yöntemin şifreleme, kimlik doğrulama veya konuşmadaki olumsuz alametleri önlemek için mi kullanıldığı belirsizdir (2.1 - a Short History of Cryptography, n.d.).

Herodot, ahşap tabletlerdeki balmumunun altına gizlenmiş gizli mesajları veya kölelerin başlarındaki saç büyümesiyle gizlenen dövmeleri belgeledi. Steganografi olarak sınıflandırılan bu örnekler, mesajın şifresi çözüldükten sonra doğrudan okunabilmesi nedeniyle kriptografiden farklıdır. Polybius, bugün "Polybius Meydanı" olarak bilinen alternatif bir Yunan yöntemini tanıttı. Romalılar, Sezar şifresinin ve onun çeşitlerinin yaratılmasıyla şifreleme konusunda temel düzeyde bir anlayış sergilemişlerdir (2.1 - a Short History of Cryptography, n.d.)

İkinci Dünya Savaşı'ndan önce kriptanalizdeki en önemli ilerleme, monoalfabetik ikame şifrelerinin şifresini çözmek için frekans analizi yönteminin tanıtılmasıydı. Bu atılım, MS 800 civarında tekniği geliştiren Arap matematikçi Al-Kindi'ye atfedilir. Al-Kindi, "Risalah fi Istikhraj al-Mu'amma" (Kriptografik

Mesajların Şifresini Çözmek için El Yazması) başlıklı kitabında yalnızca frekans analizinin en eski tanımlarını yaptı ama aynı zamanda çok alfabetik şifreler, şifre kategorizasyonu, Arapça fonetik ve sözdizimi için ilk kriptanaliz yöntemlerini tanıttı. Ayrıca kodlama tekniklerini, Arapça karakterleri ve harf kombinasyonlarını istatistiksel olarak analiz etmeyi ve belirli kodlamaların kriptanalizini araştırdı. Bir başka dikkate değer katkı, frekans analizi için örneklem büyüklüğü hususları üzerine yaptığı çalışmayla alanı önemli ölçüde geliştiren İbn Adlan'dan (1187-1268) gelmiştir (2.1 - a Short History of Cryptography, n.d.).

Ahmed el-Kalkaşandi, milattan sonra 1355-1418 yılları arasında yazdığı 14 ciltlik "Subh al-a'sha" adlı eserinde kriptolojiye bir bölüm ayırmıştır. Her ne kadar kriptografi üzerine kitapları maalesef kaybolmuş olan İbn el-Durayhim'e (milattan sonra 1312-1361) atfedilmiş olsa da, makale hem aktarma hem de ikameyi içeren bir şifre kataloğu sunuyordu. Özellikle, ilk kez düz metindeki her harfe uygulanan, daha sonra homofonik ikame olarak bilinen, birden fazla ikame kullanan bir şifreyi tanıttı. İbnü'd-Durayhim ayrıca kriptanalizi açıklaması ve bir kelimede bir arada bulunamayan harf kümelerini ve harf sıklıklarını detaylandıran tabloları içeren pratik bir örnek sunmasıyla da tanınmaktadır (The Project Gutenberg eBook of the Kama Sutra of Vatsyayana, by Richard Francis Burton, Bhagavanlal Indrajit, and Shivaram Parashuram Bhide., n.d.).

Mantua Dükü, 1400'lerin başında homofonik ikame şifresini kullandı ve bu, uygulamasının bilinen en eski örneğini işaret ediyordu. Bu şifrede, her harf için birden fazla sembol kullanılır; bu, harflerin sıklığına göre değişen bir stratejidir. Homofonik şifre, hem tek alfabeli hem de çok alfabetik özelliklerin bir araya gelmesi nedeniyle, kullanıldığı dönemi aşan bir karmaşıklık düzeyi sergilemektedir (The Project Gutenberg eBook of the Kama Sutra of Vatsyayana, by Richard Francis Burton, Bhagavanlal Indrajit, and Shivaram Parashuram Bhide., n.d.).

Çok alfabeli şifrenin ortaya çıkmasından önce neredeyse tüm şifreler, frekans analizinin kriptanalitik tekniğine karşı savunmasızdı ve bu duyarlılık, icat edildikten sonra bile devam etmiştir. Yaklaşık 1467 yılında, sıklıkla "Batı kriptolojisinin babası" olarak selamlanan Leon Battista Alberti, çok alfabeli şifrenin en anlaşılır açıklamasını

sundu. Vigenère şifresinin çok önemli bir bileşeni olan tabula recta, Johannes Trithemius tarafından "Poligraphia" adlı çalışmasında tanıtıldı. Trithemius ayrıca "Steganographia"nın da yazarıdır. Adını Fransız kriptograf Blaise de Vigenère'den alan Vigenère şifresi, işlevsel bir çok alfabetik şemayı temsil etmektedir (The Project Gutenberg eBook of the Kama Sutra of Vatsyayana, by Richard Francis Burton, Bhagavanlal Indrajit, and Shivaram Parashuram Bhide., n.d.).

Avrupa'da, çoğunlukla gizlice yürütülen şifrelemenin artan önemi, siyasi rekabetler ve dini dönüşümlerden kaynaklanıyordu. Papalık Devletleri ve Roma Katolik Kilisesi de dahil olmak üzere çeşitli İtalyan devletleri, Avrupa'da Rönesans sırasında ve sonrasında kriptografi tekniklerinin hızla yayılmasında önemli bir rol oynadı. Bu artışa rağmen, bu yöntemlerin çoğu, Alberti'nin öncü çok alfabeli ilerlemesine dair bir anlayış veya farkındalık göstermedi. Alberti'nin katkılarından sonra bile "gelişmiş şifrelerin" iddia edilen karmaşıklığı her zaman gerçeklikle örtüşmüyordu, çünkü bunlar sık sık güvenlik açıklarıyla karşılaşıyordu. Bu aşırı güven duygusunun, kapsamlı bilgi eksikliği göz önüne alındığında, kişinin kendi sisteminin güvenlik açığını doğru bir şekilde değerlendirmenin zor olduğu kriptografi tarihinde derin kökleri olabilir; bu belirsizlik bugün bile bir dereceye kadar devam etmektedir (Kahn, 1996).

Kraliçe I. Elizabeth'in hükümdarlığı sırasında, İskoç Kraliçesi Mary, kriptografi, kriptanaliz ve gizli ajanlar ve haberciler tarafından ihanet unsurlarını içeren bir plan olan Babington komplosu nedeniyle ölümüyle karşılaştı. Dr. Dee'nin Ruhlar Kitabı'nın bir bölümünde Robert Hooke, John Dee'nin Kraliçe I. Elizabeth ile olan iletişimini gizlemek için Trithemian steganografisini kullandığını öne sürdü (Kahn, 1996).

Antoine Rossignol, Fransa Kralı XIV. Louis'nin baş kriptografı olarak görev yaptı. O, ailesiyle birlikte, başlangıcından 1890'a kadar çözülemeyen bir şifreleme sistemi olan Büyük Şifre'yi tasarladı ve Fransız askeri kriptanalisti Étienne Bazeries, şifreyi başarıyla çözdü. Demir Maskeli Adam olarak bilinen kötü şöhretli ve gizemli mahkumun tam kimliği açıklanmasa da, Étienne Bazeries'in 1900 yılından hemen önce

gerçekleştirdiği bir görev olan o döneme ait şifreli bir telgrafın şifresinin çözülmesiyle bazı bilgiler elde edilmiştir (Betz, 2022).

İslam'ın Altın Çağı'nın Moğollar tarafından sona ermesinin ardından, Avrupa dışındaki şifreleme durumu nispeten gelişmemiş durumda kaldı. Japonya'da yaklaşık 1510 yılına kadar kriptografinin benimsenmediği ve ülkenin Batılı güçlere açıldığı 1860'lara kadar gelişmiş yöntemlerin ortaya çıkmadığı görülmektedir (Betz, 2022).

Kriptografinin zengin ve karmaşık bir geçmişi olmasına rağmen, 19. yüzyıla kadar hem şifreleme hem de kriptanalize, yani kriptografik sistemlerdeki güvenlik açıklarını belirleme bilimine özel yaklaşımların ötesine geçemedi. İkincisinin örnekleri arasında Charles Babbage'nin, daha sonra Prusyalı Friedrich Kasiski tarafından tekrar gözden geçirilip yayınlanan, Kırım Savaşı döneminde çok alfabeli şifrelerin matematiksel kriptanalizi üzerine çalışması yer almaktadır. Bu dönemde kriptografinin anlaşılması, Auguste Kerckhoffs'un 19. yüzyılın ikinci yarısındaki kriptografik yazılarında açıkça görüldüğü gibi, esas olarak zor kazanılmış buluşsal yöntemlere dayanıyordu. 1840'lı yıllarda Edgar Allan Poe, şifreleri çözmek için sistematik yöntemler kullandı ve Philadelphia'daki bir gazeteye bir ilan verdikten sonra kendisine ulaşan başvuruları çözerek kamuoyunun dikkatini çekti. Onun içgörüleri daha sonra Birinci Dünya Savaşı sırasında İngiliz kriptanalistler için etkili olmuştur (Dale, 2023).

Kriptografi, hem doğru hem de yanlış kullanımıyla, 20. yüzyılın başlarında Mata Hari'nin idam edilmesi ve Dreyfus'un mahkum edilmesi ve hapsedilmesi gibi tarihi olaylarda rol oynadı. Kriptograflar aynı zamanda Dreyfus olayının ardındaki manipülasyonların ortaya çıkarılmasında da etkili oldular. Birinci Dünya Savaşı'nda, Deniz Kuvvetleri Komutanlığı'ndaki 40 numaralı oda, Alman deniz kanunlarını başarıyla ihlal ederek, deniz çatışmalarına ve Alman sortilerinin durdurulmasına önemli ölçüde katkıda bulunmuştur (Dale, 2023).

1917'de Gilbert Vernam, kağıt bant üzerinde önceden hazırlanmış bir anahtar kullanan bir teleprinter şifresi önerdi; bu, elektromekanik şifre makinelerinin geliştirilmesine ve kırılmaz tek şifre olan tek kullanımlık pedin yaratılmasına yol açmuştur (Salomon, 2006).

1920'lerde Polonyalı deniz subayları kodların ve şifrelerin geliştirilmesinde Japon ordusuyla işbirliği yaptı. Matematiksel yöntemler, II. Dünya Savaşı'ndan önceki dönemde, özellikle William F. Friedman'ın istatistiksel teknikleri kriptanalize ve şifre geliştirmeye uygulamasıyla ve Marian Rejewski'nin 1932'de Alman Ordusunun Enigma sistemine girmesiyle daha da çoğalmıştır (Salomon, 2006).

İkinci Dünya Savaşı sırasında mekanik ve elektromekanik şifreleme makineleri yaygın bir şekilde benimsendi. Bu tür makinelerin pratik olmadığı durumlarda manuel sistemlerden ve kod kitaplarından faydalanılmaya devam edildi. Hem şifrelerin tasarımında hem de kriptanaliz tekniklerinde önemli ilerlemeler kaydedildi ve bunların tümü katı bir gizlilik içinde yürütüldü. Britanya'da 50 yıllık resmi gizlilik döneminin sona ermesi, ABD arşivlerinin açılması ve çeşitli anı ve makalelerin yayınlanmasıyla bu döneme ait bilgilerin gizliliğinin kaldırılması yavaş yavaş başlamıştır (Kutash, 2023).

İkinci Dünya Savaşı sırasında Almanlar, elektromekanik rotorlu bir makine olan Enigma'nın çeşitli versiyonlarını yoğun bir şekilde kullandı. Aralık 1932'de çığır açan bir gelişmeyle, Polonya Şifre Bürosunda çalışan matematikçi Marian Rejewski, Alman Ordusu Enigma'sının ayrıntılı yapısını çözdü. Matematiğe ve Fransız askeri istihbaratından elde edilen sınırlı belgelere dayanan bu buluş, kriptanalizde bin yıldan fazla süredir kaydedilen en önemli ilerleme olarak kabul edilmiştir (Kutash, 2023).

Rejewski, Şifre Bürosu'ndaki meslektaşları Jerzy Różycki ve Henryk Zygalski ile birlikte makinenin evrimi ve şifreleme prosedürlerine ayak uydurarak Enigma'nın şifresini çözmeye devam etti. Almanlar değişiklikleri uygulamaya koyarken ve savaş yaklaşırken, Polonya Şifreleme Bürosu, Genelkurmay'ın emri üzerine, Temmuz 1939'da Enigma şifre çözmenin sırlarını Fransız ve İngiliz istihbarat temsilcileriyle paylaşmıştır (Kutash, 2023).

Almanya'nın Polonya'yı işgalinin ardından Şifre Bürosu'nun kilit personeli Fransa'ya tahliye edildi ve Bletchley Park'ta İngiliz kriptologlarla işbirliği yaptı. Gordon Welchman, Max Newman ve Alan Turing gibi önemli isimlerin de aralarında bulunduğu İngilizler, Enigma'nın şifresini çözmede önemli ilerlemeler kaydetmiştir (Kutash, 2023).

İkinci Dünya Savaşı'nda Alman şifre kırıcılar, özellikle 3 No'lu Donanma Şifresini kırarak Atlantik konvoylarını takip edip batırma konusunda da başarı elde etti. British Room 40 şifre kırıcılarının önceki dünya savaşındaki başarısı şaşırtıcıydı, ancak Ultra istihbaratı sonunda Haziran 1943'te amiralliği kodlarını değiştirmeye ikna etmiştir (Anderson, 2018).

Savaşın sonunda, 19 Nisan 1945'te İngiliz yetkililere, mağlup düşmanın adil bir şekilde dövülmediğini iddia etmesini önlemek için Alman Enigma şifresinin kırıldığını açıklamamaları talimatı verilmiştir (Anderson, 2018).

Alman ordusu, Fish şifreleri olarak bilinen teleprinter akış şifrelerini kullandı ve Bletchley Park, Max Newman ve diğerleriyle birlikte, kriptanalizlerine yardımcı olmak için Heath Robinson'u ve dünyanın ilk programlanabilir dijital elektronik bilgisayarı Colossus'u tasarladı. Alman Dışişleri Bakanlığı, İkinci Dünya Savaşı'nda

tek kullanımlık bloknotu kullandı ve bu iletişimin bir kısmı, kısmen Güney Amerika'daki bir Alman kuryesi tarafından yeterli özen gösterilmeden atılan anahtar malzemenin kurtarılması nedeniyle deşifre edilmiştir (Anderson, 2018).

Savaşın sonlarında Enigma'nın yerine daha güvenli bir alternatif olarak geliştirilen Schlüsselgerät 41 sınırlı kullanım görmüştür (Anderson, 2018).

1940 yılında, ABD Ordusu'nun SIS (Sinyal İstihbarat Servisi), Pearl Harbor saldırısından önce, elektromekanik bir adım değiştirme makinesi olan Purple olarak bilinen en yüksek güvenlikli Japon diplomatik şifre sisteminin şifresini başarıyla çözdü. Mor makine, Japon Dışişleri Bakanlığı tarafından kullanılan daha önceki "Kırmızı" makinenin ve Donanma ataşeleri tarafından kullanılan ve ABD Donanması'ndan Agnes Driscoll tarafından kırılan ilgili M-1 makinesinin yerini aldı. Müttefikler tüm Japon makine şifrelerini farklı düzeylerde çözmeyi başardılar (Froomkin & Froomkin, 2021).

Japon Donanması ve Ordusu ağırlıklı olarak kod kitabı sistemlerine dayanıyordu ve daha sonra ayrı bir sayısal katkı maddesi ekledi. ABD Donanması kriptografları, 1940'tan sonra İngiliz ve Hollandalı mevkidaşlarının işbirliğiyle, birçok Japon Donanması kriptografik sistemine başarıyla sızdı. Bu sistemlerden biri olan JN-

25'teki buluş, ABD'nin Midway Muharebesi'ndeki zaferinde çok önemli bir rol oynadı. İlginç bir şekilde bu gerçek, savaştan kısa bir süre sonra Chicago Tribune'de kamuya açıklandı, ancak Japonlar, JN-25 sistemini kullanmaya devam ederken bundan habersiz görünüyordu (Froomkin & Froomkin, 2021).

Kriptanalizden, özellikle de Mor makineden elde edilen istihbarat, Amerikalılar tarafından 'Büyü' olarak anılıyordu. İngilizler, kriptanalizden, özellikle de çeşitli Enigmalar tarafından korunan mesaj trafiğinden elde edilen istihbarat için 'Ultra' terimini benimsedi. Ultra için daha önce kullanılan bir İngiliz terimi, ihanete uğraması durumunda kaynak olarak potansiyel bir bireysel ajanı önermeye çalışan 'Boniface' idi (Froomkin & Froomkin, 2021).

İkinci Dünya Savaşı'nda, İngiliz TypeX ve Amerikan SIGABA dahil olmak üzere Müttefik şifreleme makineleri, Enigma'ya benzer ancak önemli iyileştirmeler içeren elektromekanik rotor tasarımları kullandı. Ne TypeX'in ne de SIGABA'nın savaş sırasında herhangi bir tarafça çözüldüğü bilinmiyor. Polonyalılar Lacida makinesini kullandı ancak güvenliği beklentilerin altında kaldı ve kullanımdan kaldırıldı. Sahadaki ABD birlikleri M-209'u ve daha az güvenli M-94 ailesi makinelerini kullandı. İngiliz SOE ajanları başlangıçta ezberlenen şiirlerin şifreleme/şifre çözme anahtarları olarak kullanıldığı 'şiir şifrelerini' kullandı. Savaşın ilerleyen dönemlerinde tek kullanımlık pedlere geçmeye başlamışlardır (Froomkin & Froomkin, 2021).

Rudolf Abel'in NY casus çetesiyle bağlantılı olarak en az 1957'ye kadar kullanıldığı bilinen VIC şifresi oldukça karmaşık bir el şifresiydi ve Sovyetler tarafından kullanıldığı bilinen en karmaşık şifre olduğu iddia edilmektedir (Froomkin & Froomkin, 2021).

Kod kırma operasyonlarında, hem Birleşik Krallık hem de ABD önemli sayıda kadını istihdam etti; bunların yaklaşık 7.000'i Bletchley Park'ta ve 11.000'i Washington DC çevresindeki ayrı ABD Ordusu ve Deniz Kuvvetleri operasyonlarındaydı. Japonya ve Nazi Almanya'sında kadınlar başlangıçta savaş işlerinin dışında tutuldu, ancak Birleşik Krallık ve ABD, Elizabeth Friedman ve Agnes Meyer Driscoll gibi önemli katkıda bulunanlar da dahil olmak üzere kadın kolejlerinin

en iyi mezunlarını aktif olarak işe aldı. Müttefikler ve Mihver Devletleri arasındaki kadınların yeteneklerinden yararlanma konusundaki stratejik farklılığın savaş üzerinde dikkate değer bir etkisi olduğu ileri sürülmektedir

Çağdaş zamanlarda şifreleme, hem şifreleme hem de şifre çözme işlemleri için belirli anahtarlara sahip algoritmalara dayanır. Bu anahtarlar, mesajları ve verileri genellikle "dijital anlamsızlık" olarak adlandırılan şifrelenmiş formlara dönüştürür ve ardından şifre çözme yoluyla bunları orijinal durumlarına geri yükler. Genel olarak kodun çözülmesinin karmaşıklığı, anahtarın uzunluğu arttıkça artar. Bunun nedeni, şifrelenmiş bir mesajı kaba kuvvetle kırmaya çalışmanın mümkün olan her anahtarı denemeyi gerektirmesidir. Örnek olarak, 8 bitlik bir anahtarın 256 (2^8) olası anahtarı bulunurken, 56 bitlik bir anahtarın 72 katrilyon (2^56) potansiyel anahtarı vardır. Bu tür anahtar uzunluklarına sahip şifreler modern teknolojiyle birlikte daha savunmasız hale gelirken, teknolojide devam eden gelişmeler şifreleme kalitesini de artırmaktadır (2.1 - a Short History of Cryptography, n.d.).

İkinci Dünya Savaşı'ndan bu yana, kriptografide önemli bir dönüm noktası, açık anahtar şifreleri olarak da bilinen asimetrik anahtar şifrelerinin kullanıma sunulması olmuştur. Bu algoritmalar aynı mesajı şifrelemek için matematiksel olarak ilişkili iki anahtar kullanır. Bu algoritmalardan bazıları, bir anahtarın yalnızca diğerinin bilgisine dayanarak belirlenmesinin son derece zor olması nedeniyle bir anahtarın yayınlanmasına bile izin vermektedir (2.1 - a Short History of Cryptography, n.d.).

1990'lı yıllarda İnternet'in ticari amaçlarla artan kullanımı, özellikle çevrimiçi işlemlerde şifrelemeye yönelik standart bir yaklaşımı gerektirdi. Gelişmiş Şifreleme Standardı'nın (AES) benimsenmesinden önce, İnternet üzerinden iletilen finansal veriler genellikle Veri Şifreleme Standardı (DES) kullanılarak şifreleniyordu. Güvenlik açısından Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından onaylanmasına rağmen DES, yüksek kaliteli şifrelemeye halkın erişimi konusundaki tartışmalar nedeniyle kullanılmaya devam etti. Sonunda, NIST tarafından düzenlenen başka bir halka açık yarışmanın ardından DES'in yerini AES aldı. 1990'ların sonlarından 2000'lerin başlarına kadar, şifreleme için genel anahtar algoritmaları daha

yaygın hale geldi ve açık anahtar ile simetrik anahtar şemalarının bir karışımı, e-ticaret operasyonlarında yaygın olarak kabul edilen yaklaşım haline geldi. Güvenli Yuva Katmanı (SSL) protokolünün kullanıma sunulması, mal satın almaktan çevrimiçi fatura ödemeye ve bankacılığa kadar güvenli çevrimiçi işlemlerin yolunu açtı. Evlerde kablosuz İnternet bağlantılarının yaygınlaşmasıyla birlikte, günlük durumlarda güvenliği sağlamak için şifrelemeye olan talep de artmıştır (2.1 - a Short History of Cryptography, n.d.).

1970'lerin ortalarında iki önemli gelişme kriptografi alanını dönüştürdü. İlk olarak, Veri Şifreleme Standardı'nın (DES) taslağı 17 Mart 1975'te ABD Federal Sicilinde yayınlandı. Ulusal Standartlar Bürosu'nun (şimdi NIST) daveti üzerine bir IBM araştırma grubu tarafından önerilen DES, güvenli şifreleme sağlamayı amaçlıyordu. işletmeler için elektronik iletişim. NSA tarafından değiştirildikten sonra, 1977'de Federal Bilgi İşleme Standardı Yayını olarak resmi olarak kabul edildi. DES, NSA gibi ulusal bir kurum tarafından onaylanan, halka açık ilk şifreyi oluşturdu. 2001 yılında resmi olarak Gelişmiş Şifreleme Standardı (AES) ile değiştirilmesine rağmen, DES ve Triple DES gibi daha güvenli varyantlar, çeşitli ulusal ve kurumsal standartlara entegre edilerek kullanılmaya devam etmektedir (The Project Gutenberg eBook of the Kama Sutra of Vatsyayana, by Richard Francis Burton, Bhagavanlal Indrajit, and Shivaram Parashuram Bhide., n.d.).

1976'daki ikinci büyük gelişme, Whitfield Diffie ve Martin Hellman'ın çığır açıcı makalesi "Kriptografide Yeni Yönler"in yayınlanmasıydı. Bu makale, Diffie-Hellman anahtar değişimi olarak bilinen, kriptografik anahtarların dağıtımına yönelik devrim niteliğinde bir yöntem tanıttı. Bundan önce tüm modern şifreleme algoritmaları, hem gönderen hem de alıcı için aynı gizli anahtarı gerektiren simetrik anahtar algoritmalarıydı. Simetrik anahtar sistemleri, taraflar arasında güvenli bir şekilde anahtar alışverişinde bulunma konusunda zorluklarla karşılaştı. Asimetrik anahtar algoritması olarak sınıflandırılan Diffie-Hellman anahtar değişimi, matematiksel olarak ilişkili anahtar çiftlerini kullanarak anahtar dağıtımını kolaylaştırdı. Bu yenilik, asimetrik anahtar algoritmaları adı verilen yeni bir şifreleme algoritması sınıfının hızla geliştirilmesine yol açmıştır (The Project Gutenberg eBook

of the Kama Sutra of Vatsyayana, by Richard Francis Burton, Bhagavanlal Indrajit, and Shivaram Parashuram Bhide., n.d.).

Asimetrik anahtar şifrelemede, şifreleme ve şifre çözme için matematiksel olarak ilişkili bir çift anahtar kullanılır. Özel olarak belirlenen anahtarlardan birinin gizli tutulması gerekirken, halka açık olarak bilinen diğeri geniş çapta erişilebilir olabilir. Bu, anahtar alışverişi için güvenli bir kanal ihtiyacını ortadan kaldırdı ve anahtar dağıtımını daha yönetilebilir hale getirdi. Asimetrik anahtar algoritmaları, büyük asal sayıların çarpımı gibi tek yönlü işlevlere dayanır ve bu da sürecin tersine çevrilmesini zorlaştırır. Asimetrik algoritmalar simetrik algoritmalara göre hesaplama açısından pahalı olsa da gelişmiş güvenlik sunmaktadırlar (Kahn, 1996).

Kriptografide yaygın olarak kullanılan diğer bir teknik olan karma, bir "hash değeri" veya "dijital parmak izi" üretmek için algoritmalar kullanarak bilgilerin kodlanmasını içerir. Bu işlem, "mesaj özeti" veya "sağlama toplamı" olarak bilinen sabit uzunlukta bir çıktı oluşturur. Hashing, iletilen bilgilerdeki değişiklikleri hızlı bir şekilde tanımlamak için kullanışlıdır. Belgeler için dijital bir imza sağlayarak bütünlüklerinin doğrulanmasına olanak tanır. Hashing aynı zamanda şifrelerin hash edildiği ve bir veritabanında saklandığı şifre güvenliğinde de kullanılır. Şifrelemeden farklı olarak karma, geri dönüşü olmayan çıktılar üreten tek yönlü bir işlemdir. Hash fonksiyonlarının kullanımı, veri bütünlüğünün sağlanması ve dijital imzaların doğrulanması açısından çok önemlidir (Kahn, 1996).

3. KUANTUM KRİPTOGRAFİ

Kuantum kriptografisi, kriptografik amaçlar için kuantum mekaniğinin ilkelerinden yararlanan bir alandır. Öne çıkan bir uygulama, anahtar değişim sorununa teorik olarak güvenli bir çözüm sağlayan kuantum anahtar dağıtımıdır. Kuantum kriptografisinin temel avantajı, imkansız olduğu düşünülen kriptografik görevleri yalnızca klasik iletişimi kullanarak gerçekleştirebilme yeteneğinde yatmaktadır. Böyle bir imkansızlık, kuantum durumunda kodlanmış verileri kopyalamaktır; çünkü bu verileri okumaya çalışmak, klonlama yapılmaması teoremi ve dalga fonksiyonunun çökmesi nedeniyle kuantum durumunu değiştirir. Bu özellik, kuantum anahtar dağıtımındaki gizli dinlemeyi tespit etmek için kullanılabilmektedir (Gisin et al., 2002).

Kriptografi, veri güvenliğinin sağlanmasında çok önemli bir unsurdur ancak kriptografik anahtarların güvenliğinin uzun ömürlülüğü süresiz olarak garanti edilmez. Kuantum kriptografi, klasik kriptografiye göre daha uzun şifreleme süreleri sunarak potansiyel bir çözüm sunmaktadır. Geleneksel kriptografik yöntemler yaklaşık 30 yıldan fazla güvenlik sağlayamayabilirken, sağlık gibi bazı sektörler daha uzun koruma süreleri talep ediyor. Örneğin elektronik tıbbi kayıt sistemlerinin yaygın olarak benimsendiği sağlık sektöründe gizliliğin uzun süre korunmasının gerekliliği ortadadır. Kuantum anahtar dağıtımı, elektronik kayıtları yüzyıla kadar koruyabilecek bir teknoloji olarak ortaya çıkıyor. Tarihsel olarak hassas verileri 60 yılı aşkın süredir gizli tutmaya alışkın olan hükümetler ve askeri kuruluşlar da kuantum kriptografisinden yararlanabilirler ("Kriptoyu Sansürlemek Cevap Değil Schneier," 2001).

Dahası, güvenliği korurken gürültülü kanallar aracılığıyla uzun mesafelerde kuantum anahtar dağıtımının kullanılmasının fizibilitesini destekleyen kanıtlar vardır. Bu, gürültülü kanal boyunca bölümler halinde stratejik olarak yerleştirilmiş kuantum bilgisayarlara benzer kuantum tekrarlayıcılar kullanılarak elde edilir. Kuantum

tekrarlayıcılar, kuantum iletişimindeki hataların verimli bir şekilde çözülmesinde çok önemli bir rol oynamaktadır. Kuantum tekrarlayıcılar, kanal bölümlerini bağlamadan önce saflaştırarak güvenli bir iletişim hattı oluşturur. Optimumun altındaki kuantum tekrarlayıcılar bile gürültülü kanallar aracılığıyla uzun mesafelerde önemli düzeyde güvenlik sunabilmektedir (Lo & Chau, 1999).

3.1. Kuantum Bilgi İşleme

Kuantum bilgi bilimi olarak da bilinen kuantum bilgi işleme, kuantum fiziği ile bilgi biliminin alanlarını bir araya getirir. Bu disiplinlerarası alan, fizikteki kuantum etkilerine dayanan, hem iletişim ve hesaplamalı modellerle ilgili teorik yönleri hem de kuantum fiziğinin deneysel yönlerini kapsayan bilgi bilimini araştırıyor. Kapsam, kuantum bilgisiyle ilişkili olasılıkları ve sınırlamaları anlamaya kadar uzanır. Kuantum bilgi işleme, fizik, bilgi teorisi, mühendislik, bilgisayar bilimi, matematik ve kimya gibi çeşitli disiplinlerden yararlanır (Watrous, 2009).

Klasik bilgi teorisindeki temel birim olan klasik bit, fiziksel görünümüne bakılmaksızın 0 veya 1'i temsil eden ikili bir rakamdır. Klasik sistemlerde 1 genellikle yüksek voltajla, 0 ise düşük voltajla temsil edilir (Watrous, 2009).

Öte yandan kuantum biti veya kübit, kuantum bilgisinin temel birimi olarak hizmet eder. Bu bilgi, esas olarak iki boyutlu bir Hilbert uzayı olan iki seviyeli bir kuantum mekanik sistemi içindeki bir durum vektörü tarafından tanımlanır. Her ne kadar klasik bitlerle bazı benzerlikler taşısa da kübit doğası gereği farklıdır. Bit'e benzer şekilde, kübit de 0 veya 1 değerlerini alabilir. Bununla birlikte, önemli fark, kübitin aynı anda hem 0 hem de 1 süperpozisyonunda var olabilme yeteneğinde yatmaktadır ve bu da benzersiz bir kuantum özelliği sağlamaktadır (Watrous, 2009).

Kuantum bilgi işleme kapsamındaki alt alanlar şunları kapsar (Watrous, 2009):

- Kuantum hesaplama: Bu alan, kuantum bilgisayarların yapısını ve fizibilitesini ve aynı zamanda onların hesaplama gücünden yararlanan arama algoritmalarının geliştirilmesini araştırıyor.Kuantum hesaplama: Çeşitli

kuantum algoritmalarının hesaplama karmaşıklığının araştırılması bu alt alanın odak noktasıdır.

- Kuantum hatası düzeltme: Kuantum hesaplama alanında, bu alt alan, kuantum bilgisini uyumsuzluğun ve diğer kuantum gürültüsü biçimlerinin neden olduğu hatalardan korumaya adanmıştır.
- Kuantum dolaşıklığı: Bu alan, bilgi teorik açıdan dolaşıklığın incelenmesini ele alır.
- Kuantum kriptografisi ve kuantum iletişimi: Bu alanlar, kuantum durumlarının bir konumdan diğerine güvenli bir şekilde aktarılmasını içerir. Kuantum kriptografisinin ticarileşmeye uygun bir olgunluk düzeyine ulaşan ilk kuantum bilgi uygulaması olması dikkat çekicidir. Bu çalışmanın vurgusu kuantum kriptografisidir.

3.2. Kriptografi

Çağdaş çağda, çevrimiçi işlemler, e-postalar ve görüntülü sohbetler gibi çeşitli alanlarda güvenli iletişimin önemi artarken, uzaktan iletişim günlük faaliyetlerimizde çok önemli bir rol oynamaktadır (Shannon, 1949).

Gizli mesajların kodlanması ve kodunun çözülmesine yönelik uygulama ve araştırma olan kriptografi, güvenli iletişimi sağlamanın temel taşı olarak hizmet eder. Kriptografinin iki ana dalı simetrik anahtar kriptografisi (veya gizli anahtar kriptografisi) ve asimetrik anahtar kriptografisidir (veya genel anahtar kriptografisi) (Bruss, 1998).

Bir bilgi parçası veya parametre olarak hizmet veren bir anahtar, bir şifreleme algoritmasının işleyişini yönetir. Şifrelemede, bir anahtar, şifre çözme sırasında düz metinden şifreli metne veya tam tersi şekilde belirli bir dönüşümü belirler. Anahtarlar, dijital imza şemalarında ve mesaj kimlik doğrulama kodlarında kullanılanlar da dahil olmak üzere çeşitli şifreleme algoritmalarının ayrılmaz bir parçasıdır (Bruss, 1998).

Gizli anahtar şifrelemesinde anahtarların güvenli bir şekilde dağıtılmasıyla ilgili zorluklar göz önüne alındığında, açık anahtar şifreleme algoritmaları, geleneksel

şifreleme sistemlerindeki pratik uygulamalarda yaygın olarak benimsenmiştir (Bruss, 1998).

Bu şifreleme yöntemlerinin güvenliği, iki önemli asal sayının çarpımının çarpanlara ayrılması gibi bir matematik probleminin varsayılan karmaşıklığına dayanır. Hiçbir genel anahtar şifreleme planının, sınırsız hesaplama gücüne sahip kulak misafiri olanlara karşı güvenliği garanti edemeyeceğini vurgulamak önemlidir (Bennett ve Brassard, 1984).

Öne çıkan kuantum hesaplama algoritmaları arasında Shor'un algoritması öne çıkmaktadır. Bu algoritma, O((log N)^3) zaman ve O(log N) uzayında bir N sayısını çarpanlarına ayırabiliyor ve bu da onu dikkate değer kılıyor. Bunun önemi, yeterince büyük bir kuantum bilgisayarın potansiyel olarak açık anahtar şifrelemesini kırabileceği imasından kaynaklanmaktadır. Örneğin RSA, iki büyük asal sayının çarpımından elde edilen bir genel anahtar N kullanır. RSA şifrelemesini kırmanın geleneksel yöntemleri, daha büyük N ile giderek daha fazla zaman alan bir süreç olan N'yi çarpanlara ayırmayı içerir. Klasik algoritmalar, N büyüdükçe herhangi bir k için O((log N)k) süresini hesaba katma verimliliğinden yoksundur. Buna karşılık, Shor'un algoritması bunu polinom zamanında gerçekleştirebilir ve bu da onu diğer çeşitli açık anahtarlı şifreleme sistemlerinin potansiyel olarak tehlikeye atılmasına kadar uzanan güçlü bir araç haline getirmektedir (Bennett ve Brassard, 1984).

Kriptografi alanında, tek kullanımlık ped, düz metnin benzersiz ve rastgele oluşturulmuş bir anahtar veya "pad" ile birleştirildiği bir şifreleme algoritmasını temsil eder. Bu ped düz metin kadar uzundur ve yalnızca tek bir şifreleme işlemi için kullanılır. Düz metin ve altlığın kombinasyonu modüler ekleme yoluyla elde edilmektedir (Bennett ve Brassard, 1984).

Tek kullanımlık ped kavramı 1917'de Vernam tarafından tanıtıldı. 1949'da Shannon, tek kullanımlık pedlerin bilgi-teorik güvenlik sağladığını kanıtlayarak ortaya koydu. Bu, potansiyel dinleyicilerin kullanabileceği hesaplama gücü ne olursa olsun, anahtar gerçekten rastgeleyse, asla tekrarlanmıyorsa ve gizli tutuluyorsa, tek kullanımlık tuş takımının mükemmel bir gizlilik sağladığı anlamına gelir. Tek

kullanımlık defterin mükemmel gizlilik sağladığı bilinen tek şifreleme sistemi olması dikkat çekicidir (Bennett ve Brassard, 1984).

Shannon'un güvenliğine dair kanıtlarına rağmen, tek kullanımlık ped önemli pratik zorluklarla karşı karşıya (Aspelmeyer ve ark., 2003):

- Tamamen rastgele bir anahtar gerektirir.
- Anahtarın güvenli bir şekilde oluşturulması ve değişimi en az mesajın kendisi kadar uzun olmalıdır.

Bu uygulama engelleri, tek kullanımlık ped sistemlerini kullanışsız hale getirmiş ve bilgi güvenliğinde bir araç olarak yaygın biçimde benimsenmelerini engelleyecek kadar önemli olmuştur (Aspelmeyer ve ark., 2003).

Kuantum fiziği, tek kullanımlık ped ile ilgili yukarıda belirtilen sorunlara bir çözüm sağlar. İlk olarak, kuantum mekaniğinin doğasında olan süperpozisyon ve belirsizlik ilkeleri, gerçek rastgeleliğin oluşmasını sağlar. İkinci olarak, kuantum kriptografisi, anahtarların iki uzak taraf tarafından güvenli bir şekilde oluşturulmasını kolaylaştırır (Aspelmeyer ve ark., 2003).

3.3. Kuantum Kriptografi

Kuantum anahtar dağıtımı (QKD) olarak da bilinen kuantum kriptografisi, güvenli iletişimi sağlamak için kuantum fiziğinin temel ilkelerinden yararlanır. Genellikle Alice ve Bob olarak adlandırılan iki yetkili kullanıcının, paylaşılan gizli bir rastgele bit dizisi oluşturmasına olanak tanır. Bu dize, mesaj şifreleme (örneğin tek kullanımlık tuş takımı) ve kimlik doğrulama dahil olmak üzere kriptografik amaçlar için bir anahtar görevi görür. Genellikle doğrulanmamış hesaplama varsayımlarına dayanan geleneksel kriptografinin aksine, QKD, kuantum mekaniğinin temel yasalarına dayanan koşulsuz güvenlik sunmaktadır (Bennett ve Brassard, 1984). Kuantum Anahtar Dağıtımı (QKD) şemalarının öncelikle iki kategorisi vardır. Bunlardan ilki, BB84 ile örneklenen hazırla ve ölç şemasıdır; burada Alice, her kübiti iki tamamlayıcı bazın dört durumundan birinde iletir; B92, burada Alice her kübiti iki

dik olmayan durumdan birinde gönderir ve Alice'in her kübiti üç tamamlayıcı bazın altı durumundan birinde gönderdiği altı durumdur (Bruss, 1998).

İkinci tür, Ekert91 tarafından temsil edilen dolanıklık tabanlı QKD'dir; burada dolaşmış kübit çiftleri Alice ve Bob'a dağıtılır ve onlar daha sonra kübit ölçümleri yoluyla anahtar bitleri türetir; ve her bir tarafın EPR çiftinin yarısını iki tamamlayıcı temelden birinde ölçtüğü BBM92. Ekert91'de Alice ve Bob, Eve'in bilgilerini Bell'in eşitsizlik testi aracılığıyla değerlendirirken, BBM92'de, BB84'e benzer şekilde Alice ve Bob, Eve'in son anahtarla ilgili bilgilerini ortadan kaldırmak için gizlilik artırmayı kullanmaktadır (Ekert, 1991).

Kuantum Anahtar Dağıtımı (QKD) hem kuantum kanalına hem de klasik kanala dayanır. Klasik kanalın kimliğinin doğrulandığı varsayılırken kuantum kanalı güvensizliğe duyarlı olabilir. Neyse ki klasik kriptografide Wegman-Carter kimlik doğrulama şeması gibi koşulsuz güvenliğe sahip kimlik doğrulama şemaları mevcuttur. Ayrıca, bu şemalar etkilidir ve N bitlik bir mesajın kimliğini doğrulamak için paylaşılan anahtarın yalnızca logaritmik bitlerini gerektirir. Alice ve Bob arasında az sayıda önceden paylaşılan güvenli bit gerekli olduğundan, QKD'nin amacı anahtarı dağıtmak yerine büyütmektir. Geleneksel bilgi teorisinde anahtar büyütmenin imkânsız bir görev olarak kabul edildiğini belirtmek önemlidir. Bu nedenle QKD,

klasik olarak imkânsız kabul edilen bir soruna temel bir çözüm sağlamaktadır (Ekert, 1991).

En bilinen Kuantum Anahtar Dağıtımı (QKD) protokolü olan BB84'ün süreci şu şekilde gelişmektedir. Alice'in polarizasyon kodlamasını kullandığını varsayarız (Ma, 2004).

BB84 Kuantum Anahtar Dağıtımı (QKD) protokolünde prosedür şu şekilde gerçekleşir (Ma, 2004):

- Alice dikey, yatay, 45 derece ve 135 derece polarizasyonları temsil eden dört durumdan birini rastgele seçer. Bunlar Z tabanı (dikdörtgen) ve X tabanı
- (köşegen) olarak adlandırılır. Daha sonra kübiti güvenli olmayan bir kuantum kanalı aracılığıyla Bob'a iletir

- Bob, kübiti aldıktan sonra durumları ölçmek için rastgele Z veya X tabanını seçer. Ölçüm sonuçlarını gizli tutar.
- Alice ve Bob, seçtikleri bazları karşılaştırmak için halka açık bir klasik kanaldan yararlanıyor. Yalnızca her iki tarafın da aynı temeli kullandığı ölçüm sonuçlarını korurlar; bu adıma genellikle temel mutabakatı denir. Temel seçimleri rastgele ise tespit sonuçlarının yarısı atılacaktır.
- Alice ve Bob, son güvenli anahtarı elde etmek için hata düzeltme ve gizlilik artırma işlemlerini gerçekleştirir. Sonraki tartışmada, genellikle güvenlik kanıtının birincil odağı olan bu adımın gerçekleştirilmesi üzerinde durulacaktır.

Eve, Alice tarafından gönderilen durumları değiştirerek veya ölçerek kuantum kanalına müdahale etme potansiyeline sahiptir. Topluca işlem sonrası olarak adlandırılan son iki adım, genellikle kimliği doğrulanmış bir klasik kanal gerektirir. Bu bağlamda Eve'in işlem sonrası klasik iletişime ilişkin tüm bilgilere ulaşabilmesi ancak bu bilgileri değiştirememesi anlamına gelmektedir (Mayers, 2001).

3.4. Kriptanaliz ve Kuantum Kriptanaliz

Kriptanaliz, genellikle gizli anahtarın tanımlanmasını da içeren, gerekli gizli bilgilere erişim olmaksızın şifrelenmiş bilgilerin şifresini çözmeyi amaçlayan tekniklerin araştırılmasıdır. Daha basit bir ifadeyle, kodları kırma veya bilgilerin şifresini çözme faaliyetlerini kapsar, ancak bu terimler aynı zamanda belirli teknik anlamlar da taşır. Kuantum analogları alanında odak noktası, Kuantum Anahtar Dağıtımı (QKD) sistemlerindeki potansiyel güvenlik açıklarının belirlenmesi ve çeşitli saldırı stratejilerinin geliştirilmesidir. Saldırıların araştırılması ikili bir amaca hizmet eder: Birincisi, güvenliği pratik olarak değerlendirir, ikincisi ise kuantum mekaniğinin temel yönlerini derinlemesine incelemektedir (Fuchs ve ark., 1997).

İki dedektör içeren pratik QKD sistemlerinde dikkate değer bir husus, tespit verimliliğindeki boşluktur. Bu sorun QKD gibi uygulamalı teknolojilerin ötesine uzanıyor ve Bell eşitsizliklerinin test edilmesi gibi temel fiziği de etkiliyor. Ek olarak,

iki dedektörün yapısında aynı özelliklerin elde edilmesi pratikte zorlayıcıdır (Fuchs ve ark., 1997).

Kuantum hesaplamayla ilgili bazı tartışmalar, büyük bir kuantum makinesinin yalnızca varlığının, 1992 yapımı Spor Ayakkabıları filminde tasvir edilen senaryoya benzer şekilde, tüm şifrelemeyi tehlikeye atabileceğini öne sürüyor. Bazıları, başarılı kuantum hesaplamanın, dünyanın sırlarını otomatik olarak ortaya çıkarmak için tüm şifreleme sistemlerindeki temel bir zayıflıktan yararlanabileceğini ima ediyor. Ancak durum böyle değil. Gerçekte, bir saldırganın anahtar bazında kriptanaliz için bir kuantum bilgisayarı kullanması gerekir. O zaman bile, saldırgan yalnızca başarılı bir şekilde yakalayıp sakladığı mesajların şifresini çözebilir. Kuantum kriptanaliz tehdidini sınırlayan üç pratik zorluk vardır (Fuchs ve ark., 1997).

İlk olarak, saldırganın analiz için şifrelenmiş verileri elde etmesi gerekir; bu da hedefe karşı gözetleme yetenekleri gerektirir. Kuantum kriptanaliz tehdidi tipik olarak önemli gözetim ve depolama yeteneklerine sahip ulus devletlerin yanı sıra internet üzerinde önemli etkiye sahip özel aktörlerden kaynaklanmaktadır. Birincil risk, mesajları uzun süre saklayacak kaynaklara ve motivasyona sahip olan kurumlarda yatmaktadır (Fuchs ve ark., 1997).

İkinci zorluk ise zamandır. Kriptanaliz, kuantum bilgisayarda bile zaman alan bir süreçtir. Örneğin, Ulusal Akademiler sağlam bir RSA anahtarının kırılmasının 28 saat süreceğini tahmin ederken, 2019'da yayınlanan bir Google makalesi 8 saat gerektiren bir yöntem önerdi. Standart bir 2.048 bitlik anahtarın bile kırılmasının 3,5 saat süreceği tahmin edilmektedir (Quantum Cryptanalysis: Hype and Reality, n.d.).

Üçüncü zorluk kaynak yönetimini içerir. Askeri doktrin, kaynakların karneye bağlanmasına ilişkin kararların alınması için hedeflemeyi, görevlendirme emirlerini ve çatışmayı ortadan kaldırmayı kapsayan metodik bir süreç öngörmektedir. Hedefleme, mesajları seçmeyi, önceliklendirmeyi ve bunları uygun bir yanıtla eşleştirmeyi içerir. Hedefler belirlendikten sonra askeri komuta, saldırı yöntemini belirlemek için görev emirleri verir (Quantum Cryptanalysis: Hype and Reality, n.d.).

Bu sürecin önemini göstermek için, hedefin telefonu ile Twitter gibi bir yayın hizmeti arasındaki kablosuz mesajları yakalayan bir kuruluşu düşünün. Her kablosuz

mesaj, anında yayınlanmak üzere bir tweet, planlanmış bir tweet, doğrudan mesaj veya diğer mesajlar için bir durum kontrolü yoklaması içerebilir. Bazı mesajlar daha değerli olsa da hepsinin şifresini çözmek aynı çabayı gerektirir. Bu zorluk, iyi tasarlanmış bir şifreleme sistemiyle, şifreyi çözmeden önce mesajları birbirinden ayırmanın açık bir yolunun bulunmamasından kaynaklanmaktadır. Akıllı düşmanlar, bir sistemi değersiz şifrelenmiş mesajlarla doldurarak başka bir devletin şifre çözme kapasitesini aşabilir. Anahtar uzunluklarının arttırılması saldırganlara ek süre zorunluluğu getirmektedir. Örneğin, Ulusal Akademilerin tahminlerine göre 8.000 bitlik bir RSA anahtarının kullanılması, yaklaşık 1,5 hafta kadar 229 saatlik bir çalışma gerektirecektir (Quantum Cryptanalysis: Hype and Reality, n.d.).

4. KUANTUM KRIPTOGRAFI: ÖN HAZIRLIK

Kuantum Anahtar Dağıtımı (QKD), iletişim kanallarını güvenli hale getirmek için kuantum mekaniği ilkelerinden yararlanan kuantum kriptografisinin bir dalıdır. QKD'nin temel amacı, geleneksel olarak Alice (gönderen) ve Bob (alıcı) olarak adlandırılan iki tarafın, genellikle Eve olarak belirtilen potansiyel bir dinleyicinin varlığında güvenli olmayan bir iletişim kanalı üzerinden gizli bir şifreleme anahtarı oluşturmasını sağlamaktır (Pugh ve ark., 2017).

QKD'nin güvenliği, klonlama yapmama teoremi ve belirsizlik ilkesi gibi kuantum mekaniğinin temel ilkelerine dayanır. Klonlamama teoremi, rastgele bilinmeyen bir kuantum durumunun tam olarak kopyalanamayacağını belirtir ve bu, gizlice dinlemeyi tespit etmek için bir araç sağlar. Belirsizlik ilkesi, belirli özellik çiftlerinin eşzamanlı olarak ölçülmesinin kesinliğine doğal sınırlamalar getirerek kuantum iletişiminin güvenliğini artırır.

Tipik QKD protokolü, Alice ve Bob arasında kuantum bitlerinin veya kübitlerin iletimini içerir. Bu kübitler, fotonların polarizasyon durumları gibi çeşitli kuantum özellikleri kullanılarak kodlanabilmektedir. Anahtar oluşturma sürecinin güvenliği kuantum mekaniğinin ilkeleriyle sağlanıyor ve bu da onu teorik olarak bazı klasik kriptografik saldırılara karşı bağışık hale getirmektedir (Popkin, 2017).

Yaygın QKD protokolleri arasında her biri kuantum bilgilerini güvenli bir şekilde paylaşmak için farklı stratejiler kullanan BB84, E91 ve BBM92 bulunur. Hata düzeltme ve gizliliğin artırılmasını içeren işlem sonrası adımlar, Alice ve Bob arasındaki paylaşılan anahtarı daha da hassaslaştırır (Dynes ve ark., 2009).

Teorik güvenlik avantajlarına rağmen QKD'nin pratik uygulamaları cihaz kusurları, kanal kayıpları ve çevre koşullarıyla ilgili zorluklarla karşı karşıyadır. Araştırmacılar ve mühendisler, bu zorlukların üstesinden gelmek ve gerçek dünyauygulamalarında güvenli kuantum iletişiminin önünü açmak için sürekli olarak

sağlam QKD sistemleri geliştirmeye çalışıyor. Kuantum teknolojileri ilerledikçe QKD, kuantum ve klasik

saldırılara dayanıklı güvenli iletişim kanallarının arayışında önemli bir bileşen olmaya devam etmektedir (Ji ve ark., 2017).

4.1. Kuantum Anahtar Dağıtımı: Teori ve Pratik Uygulamalar Arasındaki Farklar

Kuantum Anahtar Dağıtımında (QKD) birkaç önemli rakamı tanıtalım: Gönderen Alice, bir kriptografik anahtarın iletimini başlatırken, alıcı Bob kuantum durumlarını yakalar ve Alice tarafından gönderilen anahtarı çıkarır. Bu roller yaygın olarak kullanılan kurallar olmasına rağmen kesin olarak tanımlanmamıştır. Dolaşma temelli QKD gibi spesifik protokollerde Alice ve Bob'un rolleri değiştirilebilir (Rosenberg ve ark., 2009).

Üçüncü önemli karakter, gizli bir rol üstlenen, genellikle Eve olarak bilinen, kulak misafiri olan kişidir. Eve, Alice ile Bob arasında kurulan anahtar hakkında bilgi edinmek için QKD sürecine sızmaya çalışır. QKD'deki ihtiyatlı bir varsayım, Eve'in hem kuantum hem de klasik kanallar üzerinde tam kontrole sahip olduğu, QKD bileşenleri hakkında derinlemesine bir anlayışa sahip olduğu ve önemli miktarda hesaplama gücüne sahip olduğu yönündedir. Bu, bir kuantum bilgisayarına sahip olmayı içerebilir. Eve'in saldırıları yalnızca kuantum mekaniği ve diğer fizik yasalarıyla sınırlıdır. QKD'deki Kutsal Kase koşulsuz güvenliktir ve güvenliğin Eve'in hesaplama yetenekleri üzerinde herhangi bir kısıtlama olmaksızın kanıtlandığı anlamına gelir. Koşulsuz güvenlik kanıtlarında genel olarak Eve'in güçlü bir kuantum bilgisayarına ve kanalların tam kontrolüne sahip olduğu varsayılmaktadır (Rosenberg ve ark., 2009).

Buna karşılık, RSA gibi yaygın olarak kullanılan birçok geleneksel klasik şifreleme protokolü, Eve'in sınırlı hesaplama gücüne sahip olduğunu varsayarak güvenliği sağlar. Teknolojinin ve algoritmaların dinamik doğası göz önüne alındığında bu varsayım, gelecekte güvenliği garanti etmez. Örneğin Eve şifrelenmiş bir mesajı saklayabilir ve gelecekte gelişmiş hesaplama gücü veya geliştirilmiş algoritmalarla

şifresini çözebilir. Gerçek hayattaki uygulamalara hitap eden koşulsuz güvenlik, bu tür sınırlamaların ötesine geçer (Rosenberg ve ark., 2009).

Farklı Kuantum Anahtar Dağıtımı (QKD) protokollerini veya kurulumlarını değerlendirmek için QKD performansının değerlendirilmesi, iki kritik hususun karakterize edilmesini içerir: anahtar hızı ve maksimum güvenli mesafe. Alice'in kuantum bilgisini zayıf lazer darbeleri halinde kodladığını (veya farklı bir yöntem kullanılıyorsa zaman alanlarını manuel olarak darbelere böldüğünü) varsayarsak, anahtar hızı, bir darbeden elde edilen son güvenli anahtar bitlerinin ortalama sayısı olarak tanımlanır. Anahtar oranının darbe tekrarlama oranıyla çarpılması, anahtar oluşturma hızını sağlar. Kayıp ve gürültüden etkilenen pratik QKD sistemleri, güvenli mesafe konusunda bir sınırlama sergiler. Belirli bir mesafenin ötesinde, belirli bir işlem sonrası prosedürle birleştirilmiş bir QKD kurulumu pozitif bir güvenli anahtar elde edemez. Maksimum güvenli mesafe, belirli bir QKD kurulumu ve pozitif anahtar hızı sağlayabilen son işleme şeması için en uzak iletim mesafesidir (Rosenberg ve ark., 2009).

Bahsedilen anahtar hızının ve maksimum güvenlik mesafesinin her zaman garantili güvenliğe dayandığını unutmamak önemlidir. Çoğu durumda bu, en az ulaşılabilir performansı temsil eden alt sınır olarak kabul edilir. QKD kurulumları ve protokolleri için performansın üst sınırını keşfetmek de ilgi çekici bir konudur (Gasbarri ve ark., 2021).

Gerçek hayattaki uygulamalar genellikle belirli performans ölçümlerini gerektirir. Örneğin, son teknoloji ürünü dijital konuşma kodlaması genellikle 4-10 kbit/sn civarında bir bit hızı gerektirir. Tipik bir şehir çapındaki alan ağının yarıçapı 5-25 km olan bir alanı kapsaması gerekir. Daha sonra sonuç bölümünde tartışacağımız gibi, QKD'deki mevcut teknolojinin bu performans gereksinimlerini karşılayabileceği aşikâr olacaktır (Gasbarri ve ark., 2021)

Kuantum Anahtar Dağıtımının (QKD) güvenliğinin sağlanması, cihaz kusurlarının ele alınmasını içerir. Örneğin, tek bir foton kaynağındaki kusurlar, foton sayısını bölme saldırıları gibi güvenlik açıkları yaratabilir. Tespit tarafında, bir kulak misafiri (Eve) tarafından gerçekleştirilen potansiyel saldırılar, sinyal darbelerinin

zamanlama bilgilerinin manipüle edilmesi gibi tespit sürecindeki kusurlardan yararlanabilir. Bu tür bir saldırının mevcut teknolojiyle somut bir örneği zaman kaydırmalı saldırıdır. Sonuç olarak, pratik bir QKD sisteminin güvenliğini sağlamak için, QKD bileşenlerinin kapsamlı bir şekilde incelenmesi gereklidir ve bu da gerçekçi bir modelin oluşturulmasına yol açar. Bu model daha sonra mevcut güvenlik kanıtlarına bağlanarak güvenliği kanıtlamak için yapılan varsayımların ve QKD deneylerinin yürütülmesine yönelik gereksinimlerin anlaşılmasına olanak tanır (Gottesman ve ark., 2004).

Pratik uygulamalarda, iki temel hususa odaklanılarak yüksek Kuantum Anahtar Dağıtımı (QKD) performansı elde edilmesi çok önemlidir: anahtar oluşturma hızı (saniyedeki bit cinsinden ölçülür) ve iletim mesafesi. Bu kriterler sırasıyla anahtar oranı ve maksimum güvenli mesafe ile temsil edilir. Teorik çabalar, kusurlu cihazların varlığında QKD'nin güvenlik kanıtına kapsamlı bir şekilde adanmıştır. Ancak bu güvenlik analizlerinin doğrudan uygulanması çoğu zaman QKD performansına önemli sınırlamalar getirir (Gottesman ve ark., 2004).

Buna karşılık, QKD deneyi iletim mesafeleri, ilk deneylerde birkaç metreden şu anda 150 km'yi aşmaya kadar belirgin bir şekilde ilerlemiştir. GLLP gibi standart güvenlik analizlerinin uygulanması, mevcut deneysel kurulumların yalnızca sınırlı iletim mesafelerini tolere edebildiğini ortaya koymaktadır. Birincil zorluk, deneyin güvenliğini sağlamak ve QKD teorisi ile uygulama arasında önemli bir boşluk yaratmaktır. Bu tez, yalnızca güvenliği garanti etmekle kalmayıp aynı zamanda pratik QKD'nin performansını da artırarak bu boşluğu doldurmayı amaçlamaktadır. Bazı durumlarda daha iyi QKD performansı elde etmenin güvenlikten ödün vermeyi gerektirebileceğini unutmamak önemlidir (Gottesman ve ark., 2004).

4.2. Kuantum Anahtar Dağıtımı: Genel Bir Bakış

Gelecekteki keşifler için ilgi çekici bir yol, mevcut araştırmaların pratik Kuantum Anahtar Dağıtımı (QKD) sistemlerinin performansını daha da artırmak için genişletilmesini içerir. Sürekli Değişken QKD, kısa ve orta iletim mesafelerinde daha yüksek anahtar hızı elde etmenin bir yolu olarak öneriliyor ve bu alanda ilgi çekici bir

konu olan güvenliğine ilişkin açık bir soru ortaya koyuyor. Sürekli Değişken QKD'ye özel modelleme ve simülasyonlar bu araştırmaya derinlik katmaktadır (Kurtsiefer ve ark., 2002).

Gerçek dünya senaryolarında, kuantum sinyallerinin kanaldaki düzenli klasik sinyallerle bir arada bulunması gibi ek bozuklukların dikkate alınması gerekir. Nihai hedef, kullanıcı dostu, İnternet ile sorunsuz bir şekilde entegre olan ve pratik uygulamalara uyarlanabilen bir QKD sistemi geliştirmektir (Kurtsiefer ve ark., 2002).

Sonlu anahtar uzunluğuna sahip QKD senaryolarında istatistiksel dalgalanmaların hesaba katılması hayati önem taşıyor ve son çalışmalar bu konuyu ele almıştır. Keşif için ilginç bir yol, Koashi'nin tamamlayıcı fikrinin, sonuçlarını önceki sonuçlarla karşılaştırarak sonlu anahtar QKD'ye uygulanmasıdır (Weier ve ark., 2006).

Kuantum kriptografi alanının ötesinde düşündürücü bir soru ortaya çıkıyor: QKD'de geliştirilen teknikler kuantum hesaplamada kullanılabilir mi? Örneğin, QKD'deki modellerin ve işlem sonrası şemaların doğrusal optik gerçekleştirmeler yoluyla kuantum hesaplamaya katkıda bulunup bulunamayacağını keşfetmek, araştırma için ilgi çekici bir yol sunmaktadır (Weier ve ark., 2006).

Son olarak, kuantum bilgi işleme alanı, kuantum mekaniğinin temelleriyle karmaşık bir şekilde bağlantılıdır. Von Neumann entropisi gibi kuantum bilgisi kuantum dolaşıklığının anlaşılmasına yardımcı olsa da açık bir soru var: Kuantum mekaniğindeki diğer ilkeler kuantum bilgi işlemedeki ilerlemelerden nasıl yararlanabilir? Bu bütünsel keşif, kuantum mekaniğinin temel yönlerinin daha derin anlaşılmasına katkıda bulunacaktır (Weier ve ark., 2006).

5. KUANTUM KRİPTANALİZİ

Bilgiyi korumanın son derece önemli olduğu dinamik kriptografi alanında, kuantum mekaniği ve kriptografik metodolojilerin birleşimiyle çığır açan bir paradigma ortaya çıktı: kuantum kriptanaliz. Kuantum bilgisayarların ortaya çıkışı, klasik şifreleme tekniklerinin belirlediği sınırları zorluyor ve yeniden şekillendiriyor. Klasik kriptografik sistemleri kırmak için kuantum hesaplamanın kullanılması olan kuantum kriptanaliz, dijital güvenlik alanında hem önemli potansiyel hem de derin zorluklar sunmaktadır.

Geleneksel kriptografi, hassas bilgilerin gizliliğini ve bütünlüğünü sağlamak için geleneksel olarak matematiğin karmaşıklığına ve hesaplama kısıtlamalarına dayanır. Bununla birlikte, klasik bilgisayarlara kıyasla katlanarak daha hızlı hesaplamalar yapmak için kuantum mekaniğinin özelliklerinden yararlanan kuantum bilgisayarların piyasaya sürülmesi, kriptografik araştırmalar için yeni yollar açtı.

Kuantum kriptanalizine yönelik bu keşif, kuantum hesaplamayı ve onun benzersiz hesaplama yeteneklerini yönlendiren temel ilkelere derinlemesine bir dalışı içerecektir. Kuantum kriptanaliz çalışması salt teorik merakın ötesine uzanır; mevcut şifreleme yöntemlerinin kısıtlamalarını ortadan kaldırmak ve veri güvenliğinin yeniden tanımlandığı bir geleceği şekillendirmek için bir anahtar görevi görmektedir.

Kriptanalizin temelinde, önceden bilgi olmadan gizli anahtarı veya belirli bir mesajı açığa çıkararak şifreleme şemalarını deşifre etmek gibi zorlu bir görev yatmaktadır. Bu zorluk genellikle algoritmaların istenen hedefi bulmak için geniş bir çözüm alanında gezinmesi gereken arama problemleri biçiminde özetlenir. Çeşitli türde arama problemleri mevcuttur ve hepsi önemli hesaplama kaynakları talep etme ortak özelliğini paylaşmaktadır.

Arama Sorunlarının Çeşitli Kategorileri (Sk, 2023).:

- Kaba Kuvvet Arama: Bu yöntem, doğru çözüm belirlenene kadar tüm potansiyel çözümlerin sistematik olarak denenmesini içerir. Daha zayıf şifreleme yöntemlerine karşı etkili olsa da, çözüm alanı anahtar uzunluğuyla birlikte katlanarak genişledikçe uygulanabilirliği azalır.
- Rastgele Arama: Çözüm uzayının kaba kuvvet yöntemlerine göre daha verimli bir şekilde keşfedilmesi için rastgelelik kullanan algoritmalar. Örnekler arasında genetik algoritmalar ve simüle edilmiş tavlama yer alır.
- Sezgisel Arama: Sezgisel algoritmalar, araştırmaya rehberlik etmek ve keşfedilen olasılıkları daraltmak için alana özgü bilgilerden yararlanır. Kapsamlı arama ile rastgelelik arasında bir denge kuruyorlar.

Kuantum hesaplama, kriptanaliz alanında dönüştürücü bir güç olarak ortaya çıkıyor ve geleneksel yaklaşımları yeniden şekillendirme potansiyeline sahip devrim niteliğinde bir paradigma sunuyor. Grover'ın algoritması başta olmak üzere kuantum arama algoritmaları, klasik yöntemlere göre arama sürecini hızlandırma konusunda kayda değer bir ilerleme sunmaktadır (Sk, 2023).

1996 yılında Lov Grover tarafından geliştirilen Grover'ın algoritması, rastgele arama algoritmalarının kuantum karşılığı olarak hizmet ediyor. Klasik kaba kuvvet aramasına göre ikinci dereceden bir hızlanmaya sahiptir ve bu da onu kuantum kriptanaliz için zorlu bir araç haline getirir. Grover'ın algoritması, N öğeden oluşan sıralanmamış bir veritabanındaki işaretli bir öğeyi tanımlama konusunda çok başarılıdır ve bu görevi yaklaşık √N işlemle gerçekleştirir (Sk, 2023).

Araştırmacılar, arama alanlarında verimli bir şekilde gezinmek için kuantum yürüyüşlerinden yararlanan kuantum yürüyüş arama algoritmaları da dahil olmak üzere daha karmaşık kuantum arama tekniklerini araştırıyor. Bu algoritmalar, klasik

rastgeleliği aşan yapılarla karmaşık arama problemlerini çözme konusunda umut vaat etmektedir (Sk, 2023).

Kuantum veri yapıları, verileri oldukça paralel bir şekilde depolamak ve almak için kuantum paralelliğinden yararlanan başka bir yenilikçi yolu temsil ediyor. Bu

yaklaşım, belirli senaryolarda arama operasyonlarını hızlandırma, kriptanalizi ve daha geniş hesaplama zorluklarını etkileme potansiyeline sahiptir (Sk, 2023).

Kuantum bilgisayarlar, süperpozisyon ve dolaşma ilkelerine göre çalışarak bilgiyi klasik yeteneklerin ötesinde işlemelerine olanak tanır. Öne çıkan bir kuantum kriptanaliz aracı olan Shor'un algoritması, büyük sayıların çarpanlara ayrılmasını katlanarak hızlandırarak RSA gibi yaygın olarak kullanılan asimetrik şifreleme yöntemlerine önemli bir tehdit oluşturmaktadır (Sk, 2023).

Başka bir kuantum kriptanaliz tekniği olan Grover algoritması, yapılandırılmamış arama görevlerini klasik algoritmalardan ikinci dereceden daha hızlı gerçekleştirir. Bu, etkili anahtar uzunluğunu azaltarak simetrik anahtar şifrelemeye yönelik potansiyel bir risk oluşturur ve potansiyel olarak kaba kuvvet saldırılarının uygulanabilirliğini artırır (Sk, 2023).

Kuantum Anahtar Dağıtımı (QKD), taraflar arasında güvenli iletişimi sağlamak için kuantum mekaniğinin ilkelerinden yararlanan, kuantum kriptografisi alanında devrim niteliğinde bir teknolojidir. Birincil hedefi, geleneksel olarak Alice (gönderen) ve Bob (alıcı) olarak adlandırılan iki taraf arasında, olası dinlemelere karşı güvenli bir şekilde gizli bir şifreleme anahtarı oluşturmaktır (Mo, 2010).

Kuantum Anahtar Dağıtımının bazı temel kavramları ve yönleri şunlardır (Winick ve ark. 2018):

- Kuantum Süperpozisyon ve Dolaşma: QKD, süperpozisyon ve dolaşma ilkelerine dayanır. Kuantum bitleri veya kübitler bilgiyi kodlamak için kullanılır ve aynı anda birden fazla durumda bulunabilen kuantum durumlarının yaratılmasına olanak tanır.
- Klonlama Olmama Teoremi: Klasik kriptografide bilginin kopyalanması basittir. Ancak kuantum mekaniğinde klonlamama teoremi, rastgele
- bilinmeyen bir kuantum durumunun tam olarak kopyalanamayacağını belirtir. Bu özellik QKD'de gizli dinlemeyi tespit etmek için kullanılır.

- Kuantum Durumlarının İletimi: Tipik olarak kuantum durumları, fotonlar gibi ışık parçacıkları kullanılarak iletilir. Bu parçacıkların polarizasyonu veya diğer kuantum özellikleri kübitleri temsil eder.
- Ölçüm ve Temel: Bob, kuantum durumlarını aldıktan sonra bunları seçilmiş bir temeli kullanarak ölçer. Temel seçimi QKD protokollerinin çok önemli bir yönüdür ve iletişim sırasında Alice ve Bob tarafından kararlaştırılır.
- Gizli Dinleme Tespiti: Kuantum mekaniğinin ilkeleri nedeniyle, bir kulak misafirinin (Eve) kuantum durumlarını engellemeye veya ölçmeye yönelik herhangi bir girişimi, kaçınılmaz olarak sistemi bozacaktır. Bu rahatsızlık Alice ve Bob tarafından algılanarak onları bir dinleyicinin varlığı konusunda uyarabilir.
- Anahtar Üretimi: Herhangi bir gizlice dinleme tespit edilmezse Alice ve Bob, paylaşılan bir gizli anahtar oluşturmak için kalan kuantum durumlarını kullanabilir. Bu anahtar daha sonra klasik şifreleme algoritmaları kullanılarak güvenli iletişim için kullanılabilir.
- Anahtar Hızı ve Maksimum Güvenli Mesafe: QKD'nin performansı genellikle anahtar oluşturma hızını temsil eden anahtar hızı ve güvenli anahtar üretimi için maksimum iletim mesafesini ifade eden maksimum güvenli mesafe cinsinden ölçülür.
- Cihaz Kusurları: QKD'nin pratik uygulamaları, kusurlu tek foton kaynakları veya dedektör zayıflıkları gibi cihaz kusurlarını dikkate almalıdır. Bu kusurların giderilmesi, QKD sistemlerinin güvenliğinin sağlanması açısından çok önemlidir.
- Sürekli Değişken QKD: Sürekli Değişken QKD olarak bilinen bir QKD varyasyonu, anahtar dağıtımı için kuantum durumlarının sürekli değişkenlerinin kullanımını araştırır ve potansiyel olarak kısa ve orta iletim mesafelerinde daha yüksek anahtar hızları sunar.
- Gerçek Dünyayla İlgili Hususlar: Gerçek dünya uygulamalarında QKD sistemleri, iletişim kanalında diğer sinyallerin varlığı gibi ek zorluklarla mücadele etmelidir. Amaç, pratik, müşteri dostu ve mevcut iletişim altyapısıyla uyumlu QKD sistemleri geliştirmektir.

QKD, geleneksel şifreleme yöntemlerinin savunmasız olabileceği kuantum bilişim çağında güvenli iletişim kanalları sağlama konusunda umut vaat ediyor. Devam eden araştırmalar, zorlukları ele almayı, performansı artırmayı ve QKD'nin pratik uygulaması için yeni yollar keşfetmeyi amaçlamaktadır (Mo, 2010).

5.1. Dedektör Verimsizliği Boşluğu ve Zamanlama Bilgisi

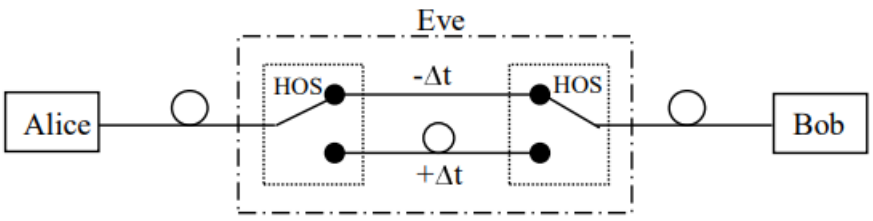
Kuantum Anahtar Dağıtımı (QKD) sistemlerindeki dedektörlerin verimlilik uyumsuzluğundan yararlanan yeni bir gizlice dinleme tekniği bu çalışma alanına tanıtılmıştır. Bu saldırıda Eve, Alice tarafından iletilen her kuantum durumunu yakalar, tam bir von Neumann ölçümü gerçekleştirir ve ardından ölçüm sonucuna dayalı olarak zaman kaydırmalı yeni bir sinyal üretir ve bunu Bob'a gönderir. Bu saldırıyı gerçekleştirmek için Eve'in Bob'unkine benzer gelişmiş bir tespit sistemine ve Alice'inkine benzer bir yeniden gönderme sistemine sahip olmasını gerektirmesi dikkat çekicidir. Eve'in "pratik" dinleme cihazını mevcut teknolojiyi kullanarak oluşturduğunu varsayarsak, düşük tespit verimliliği ve kurulumundaki kusurlardan kaynaklanan ek hatalar gibi sorunlarla karşılaşacaktır.

Eve, Alice'in kuantum durumunu ölçmek yerine, Alice'in kuantum durumu için rastgele bir zaman kayması kullanır ve bu durumun Bob'un dedektörüne t_0 veya t_1 zamanında ulaşmasını sağlar. Eğer Eve t_0 zamanını seçerse ve Bob bir sinyal tespit ederse, bit değerinin "0" olma olasılığı $\eta_0/(\eta_0 + \eta_1)$ olur. Burada η_0 ve η_1, sırasıyla SPDO ve SPD1'in t0 zamanındaki dedektör verimliliklerini temsil eder ve Alice, bir ön olasılıkla "0" ve "1" bitlerini eşit şekilde seçer. Eve'nın Bob'un bit değerini yanlış tahmin etme olasılığı $\eta_1/ (\eta_0 + \eta_1)$'dir. Sonuç olarak Eve'nın son anahtara ilişkin bilgisi bu olasılıkla belirlenmektedir.

$$\mathbf{I}\,(\boldsymbol{B}\colon\boldsymbol{E}) = \mathbf{1} - \boldsymbol{H}_{\mathbf{2}}\left(\frac{\boldsymbol{\eta}_{\mathbf{1}}}{\boldsymbol{\eta}_{\mathbf{0}} + \boldsymbol{\eta}_{\mathbf{1}}}\right)$$

Bu saldırıda Eve'in Alice'in durumunu ölçmediğine dikkat edin. Bu nedenle Eve fazladan hatalar getirmeyecektir. Simetri nedeniyle aynı analiz Eve'in t_1'i seçmesi durumuna da uygulanabilir.

Eve, istenen zaman kaymasını elde etmek amacıyla Alice'in sinyalini uzun veya kısa bir optik yoldan yeniden yönlendirmek için yüksek hızlı optik anahtarlar kullanabilir. Saldırımızın bir diğer avantajı da Eve'in asla hata yapmamasıdır. Bu nedenle Alice ve Bob'un Eve'in varlığını tespit etmesi zordur (Zhao ve ark., 2008).



Şekil 1. Eve'in saldırısının şematik diyagramı.

Zaman kaydırma saldırısı konusundaki farkındalığımız göz önüne alındığında, bu tür gizlice dinlemeyi engellemek için güvenli Kuantum Anahtar Dağıtımı (QKD) stratejilerini uygulayabiliriz. İki ana yaklaşım vardır: sayaç ölçümlerini veya sistem iyileştirmelerini içeren donanım tabanlı bir çözüm ve dedektör verimliliği uyumsuzluğu hususlarıyla bir güvenlik analizini birleştiren yazılım tabanlı bir yaklaşımdır (Zhao ve ark., 2008).

Yakın zamanda önerilen tek bir Tek Foton Dedektörlü (SPD) QKD sisteminin doğası gereği bu saldırıya karşı bağışık olması dikkat çekicidir. Bu tasarımın faz kodlamalı BB84 versiyonunda, Bob'un faz modülasyonu Alice'in faz modülasyonuna yönelik setle aynı olan dört değerden oluşan bir setten rastgele seçilmektedir, Bob yalnızca gelen her darbe için ölçüm esasını rastgele seçmekle kalmaz, aynı zamanda hangi SPD'yi rastgele belirler. "0" bitini veya "1" bitini tespit etmek için kullanılır. Bob temel seçimini yayınlarken, dedektör seçimini ("0" veya "1" biti için) gizli tutar. Böyle bir konfigürasyonda Eve hangi dedektörün tıkladığına dair bilgiye sahip olsa bile Bob'un bit değerini çıkaramaz çünkü hangi dedektörün "0" bitine karşılık geldiğine dair bilgisi yoktur. Bob'un "0" veya "1" bitini tespit etmek için rastgele seçtiği dedektörler, verimlilik uyumsuzluğunu etkili bir şekilde telafi etmektedir (Zhao ve ark., 2008).

5.2. Dedektör Verimliliğine Sahip Bir QKD Sistemi İçin Güvenlik Kanıtı

Bu bağlamda, tek bir foton kaynağı, gürültüsüz bir kanal ve "0" ve "1" bitlerini tespit etmekten sorumlu, verimlilikleri η_0 ve η_1 olarak gösterilen iki dedektör içeren basit bir senaryonun güvenlik kanıtını özel olarak ele alacağız (Renner, 2005).

Bu basitleştirilmiş Kuantum Anahtar Dağıtımı (QKD) çerçevesinde, Eve'in müdahalesi bit veya faz hatalarına yol açmaz; bunun yerine yan bilgileri elde etmek için yalnızca yardımcı boyuta müdahale eder. Bölüm 2.4'te detaylandırıldığı gibi, Alice ve Bob'un iletim sonrası paylaştığı durum (Eve'in müdahalesi dikkate alındığında) ve temel uzlaşma şu şekilde tanımlanabilir (Renner, 2005):

$$(|00> + |11>)_{AB} \rightarrow (\sqrt{\eta_1}|00> + \sqrt{\eta_1}|11>)_{AB}$$

Eve'in müdahalesi herhangi bir bit hatasına neden olmuyor; bunun yerine, sinyallerin zamanlamasını ayarlayarak, yardımcı boyuta katılımını temsil eden ek bir T sistemini birleştirir. Karma tabanlı Dolaşıklık Damıtma Protokolü (EDP) [13] kullanılarak, Alice ve Bob'un son durumdan damıtabileceği Einstein-Podolsky-Rosen (EPR) çiftlerinin miktarı H2(η0/(η0 + η1)) tarafından belirlenir. , Denklemden elde edilen sonuçla uyumlu olarak. (9.1). η0 ≠ η1 olduğunda anahtar oranın, R = 1 olduğu ideal senaryoya kıyasla 1'den küçük olması dikkat çekicidir (Renner, 2005).

5.3. Dedektör Verimliliğine Sahip Bir QKD Sistemi İçin Güvenlik Kanıtı: Sonuçlar

Bu analiz, bir güvenlik kanıtının altında yatan varsayımların kritik öneminin altını çizer. Güvenlik açıklarını belirlemek zordur, ancak keşfedildikten sonra bunlara çözüm bulmak ve Kuantum Anahtar Dağıtımı (QKD) sistemlerinde koşulsuz güvenliği yeniden sağlamak için karşı önlemler geliştirilebilir. QKD sistemlerinin karmaşıklığı ve doğasında olan kusurlar, iyi huylu kusurlar ile güvenliğe ciddi tehdit oluşturan kusurlar arasında ayrım yapmak için kapsamlı araştırma yapılmasını gerektirir. Bu hususların araştırılması ve karşı önlemlerin geliştirilmesi, güvenlik kanıtlarının yanı sıra çok önemli bir rol oynamaktadır (Renner, 2005).

Herhangi bir güvenlik sistemi gibi QKD sistemleri de pratik senaryolarda kaçınılmaz olan uygulama boşluklarına sahip olabilir. Örneğin akıllı kartlar gibi geleneksel güvenlik sistemleri de uygulama zorluklarıyla karşı karşıyadır. QKD, geleneksel sistemleri tamamlayarak, güvenliği azaltmak yerine ekstra bir güvenlik katmanı ekleyebilir. Üstelik QKD, sinyaller kuantum olduğundan geleceğe hazır olma konusunda benzersiz bir avantaj sunuyor. İletim sonrası bir transkriptin bulunmaması, kulak misafiri olanların kuantum saldırıları başlatmasını zorlaştırıyor ve iletim sırasında gelişmiş kuantum teknolojisi gerektiriyor. Bunun aksine, Diffie-Hellman gibi geleneksel genel anahtar sistemleri, onlarca yıl boyunca saklanabilen transkriptler sağlayarak bunları donanım ve algoritmalarda gelecekteki potansiyel gelişmelere maruz bırakır. Bu nedenle, QKD'nin geleneksel şifreleme sistemleriyle birlikte entegre edilmesi, derinlemesine savunma stratejisine katkıda bulunarak riski azaltır ve potansiyel tehditlere karşı gelişmiş güvenlik sağlamaktadır (Renner, 2005).

6. TARTIŞMA VE SONUÇLAR

Bu çalışma, Kuantum Anahtar Dağıtımının (QKD) teorik ilkeleri ile pratik uygulaması arasındaki ayrımı daraltmayı amaçlamıştır Pratik QKD'deki önemli bir zorluk, şu anda mevcut teknolojiyle talep edilen bir görev olan güvenilir bir tek foton kaynağının elde edilmesinde yatmaktadır. Tuzak durumu yönteminin tanıtılmasının bu sınırlamanın giderilmesinde etkili olduğu kanıtlanmıştır. Özellikle, anahtar hızının kanal aktarımına doğrusal bağımlılığı, mükemmel bir tek foton kaynağı olmasa bile, zayıf tutarlı durum kaynaklarının ve tetikleyici parametrik aşağı dönüşüm (PDC) kaynaklarının QKD kurulumları için etkili alternatifler olarak değerlendirilmesini mümkün kılar.

Çalışma, yalnızca bir veya iki tuzak durumunun kullanılmasının, tuzak durumu yönteminin pratik uygulamalarında önemli faydalar sağlayabileceğini göstermektedir. Performansı teorik sınıra yaklaştıracak şekilde, işlem sonrası adıma iki yönlü klasik iletişim dahil edilerek daha fazla iyileştirme keşfedildi. Tuzak durumu yönteminin uygulanabilirliği, PDC kaynaklarının tetiklenmesi de dahil olmak üzere çeşitli foton kaynakları için de sürekli olarak olumlu sonuçlarla araştırıldı.

Çalışmanın kendi gerçekleştirmesi de dahil olmak üzere tuzak durum QKD'nin deneysel gösterileri, yöntemin gerçek dünya sistemlerinde uygulama kolaylığının altını çizmeye çalışmıştır. Sonuç olarak, bu bulgular pratik kuantum kriptografisinin gerçek hayattaki uygulamalara doğru önemli ilerlemeler kaydetmenin eşiğinde olduğunu göstermektedir.

Tuzak durumu Kuantum Anahtar Dağıtımı'nın (QKD) temeline dayanan bu çalışma, pratik QKD sistemlerinin performansını artırmak için ek yolları araştırıyor.

Dikkate değer bir öneri, hızlı ve gürültülü dedektörlerin kullanıldığı senaryoları iyileştirmek için uyarlanmış bir ikili dedektör şemasını içerir.

Tuzak durumu QKD alanının ötesinde, çalışma alternatif QKD protokollerini, özellikle de dolaşıklığa dayalı olanları araştırıyor. Yakın zamanda yapılan bir deneyisimüle eden bulgular, ilk olarak, ortada dolaşık bir Parametrik Aşağı Dönüştürme (PDC) kaynağı içeren bir QKD kurulumunun, tuzak durumlu QKD protokolüne kıyasla kanal kaybına karşı gelişmiş tolerans sergilediğini vurgulamaktadır. İkinci olarak, tuzak durumlarıyla birlikte tutarlı durum QKD'si, orta ve düşük kayıplı bölgelerde en yüksek anahtar oranına ulaşır.

QKD'de güvenliğin büyük önemini vurgulayan araştırma, kuantum kriptografisindeki çeşitli gizlice dinleme saldırı planlarını inceliyor. İlgili potansiyel çözümlerle birlikte teknolojik olarak uygulanabilir bir saldırı planı önerilmektedir. Saldırı BB84 tutarlı durum QKD uygulaması için tasarlanmış olsa da uygulanabilirliğinin diğer birçok protokole kadar uzanması dikkat çekicidir. Çalışma aynı zamanda bu özel saldırıya karşı karşı önlemleri de ele alıyor ve dedektör verimliliği uyumsuzluğunu içeren bir QKD sistemi için bir güvenlik kanıtı sağlamaktadır.

Gelecekte, pratik Kuantum Anahtar Dağıtımı (QKD) sistemlerinin anahtar hızı ve güvenli iletim mesafesindeki iyileştirmelere odaklanarak sürekli olarak geliştirilmesi, keşfedilmesi gereken ilgi çekici bir alan olacaktır. Kuantum sinyallerinin normal klasik sinyallerle kanalları paylaştığı potansiyel bozulmalar gibi gerçek dünyadaki zorluklar, İnternet ile sorunsuz bir şekilde entegre edilmiş, müşteri dostu bir QKD sisteminin geliştirilmesini gerektirir.

Kıtalararası iletim mesafelerine ulaşmak için yer uydusu QKD umut verici bir olasılık olarak ortaya çıkıyor. Dolaşmış bir foton kaynağı kullanılarak yer uydusu QKD'nin fizibilitesine ilişkin ön çalışmalar yapılmıştır. Daha gerçekçi bir temsile

imkan verecek şekilde, atmosferik bozuklukların yer uydu kanalı üzerindeki etkisini modellemek ve simüle etmek için daha fazla araştırmaya ihtiyaç vardır. Bu, tek fotonlu dedektörlerin verimliliği ve gürültü seviyeleri ve gerekli teleskop boyutu gibi QKD bileşenleri için gereksinimlerin belirlenmesini içerir. Yer uydusu QKD'si için özel olarak tasarlanmış sağlam QKD şemalarını keşfetmek ilgi çekici bir yol olmaya devam ediyor.

Daha yüksek QKD anahtar hızlarına ulaşmak için, özellikle kısa ve orta iletim mesafeleri için sürekli değişken QKD gibi alternatif QKD protokolleri önerilmektedir. Sürekli değişken QKD'nin güvenliğiyle ilgili açık bir soru var ve bu da onu araştırma için büyüleyici bir konu haline getiriyor. Bu alandaki modelleme ve simülasyonlar da büyük ilgi görmektedir.

Sonlu anahtar uzunluklarıyla QKD'deki istatistiksel dalgalanmaların dikkate alınması, bu hususu ele alan son çalışmalarla birlikte dikkat çekmektedir. Koashi'nin tamamlayıcı fikrini sonlu anahtar QKD'ye uygulamak ve onu önceki sonuçlarla karşılaştırmak incelikli bir bakış açısı sunar.

Kuantum anahtar dağıtım tekniklerinin kuantum hesaplamayla kesişimi ilgi çekici bir konudur. Kuantum geçitleri kuantum ışınlanması yoluyla gerçekleştirilirken, ölçeklenebilirlik konusundaki pratik zorluklar devam ediyor. Uzun vadeli çabalar arasında mevcut teknolojiye sahip kuantum faktoring makineleri için pratik öneriler bulunması da yer alıyor. Sahte fikirlerin uygulanması gibi QKD'de geliştirilen tekniklerin, kuantum hesaplama bağlamında tek foton kaynakları üzerindeki kısıtlamaları gevşetip gevşetemeyeceğinin araştırılması, daha fazla araştırmayı garanti eden bir konudur.

Kuantum Sonrası Kriptografi (PQC), kuantum bilgisayarların klasik şifreleme sistemlerine yönelik oluşturduğu potansiyel tehdide bir yanıt olarak ortaya çıkmıştır. Bunun ışığında, kafes tabanlı kriptografi, kod tabanlı kriptografi ve çok değişkenli polinom kriptografisi dahil olmak üzere çeşitli PQC yaklaşımları araştırılmaktadır. Bu yöntemler, kuantum bilgisayarları için zorlu olmaya devam eden matematik problemlerinden yararlanarak kuantum saldırılarına dayanmayı amaçlıyor. NIST'in Kuantum Sonrası Şifreleme Standardizasyon projesi, dijital iletişimin gelecekteki güvenliğini sağlamak için farklı PQC önerilerini aktif olarak değerlendiriyor.

Kuantum Anahtar Dağıtımı (QKD), kuantum çağında güvenliği artırmanın başka bir yoludur. Kuantum bilgisayarları mevcut şifreleme yöntemleri için bir tehdit oluştururken, QKD teorik olarak gizlice dinlenmeye dayanıklı gizli anahtarlar oluşturmak için kuantum mekaniğinden yararlanıyor. 1984 yılında Charles Bennett ve Gilles Brassard tarafından geliştirilen BB84 protokolü, anahtar değişimi sırasında

izinsiz müdahaleyi tespit etmek için kuantum bitleri kullanan iyi bilinen bir QKD protokolüdür.

Kuantum kriptanalizinin ortaya çıkışı hem umut verici hem de etik kaygıları beraberinde getiriyor. Kuantum bilgisayarlar, kriptografi de dahil olmak üzere çeşitli endüstrilerde devrim yaratabilir, ancak klasik kriptografik sistemleri kırma yetenekleri, etik hususları gündeme getirmektedir. Güçlü kuantum bilgisayarlara erişimi olan hükümetler, kuruluşlar ve bireyler, gizli bilgilerin şifresini çözmek veya büyük ölçekli siber saldırılar başlatmak için yeteneklerini kötüye kullanabilir.

Kuantum kriptanalizini çevreleyen heyecana rağmen, yerleşik kriptografik sistemleri kırabilecek pratik kuantum bilgisayarları henüz gerçek değil. Mevcut kuantum bilgisayarları, yüksek hata oranları ve sınırlı kübitler gibi zorluklarla karşı karşıyadır ve bu da büyük ölçekli kriptanalizi uzak bir hedef haline getirmektedir. Kuantum sonrası kriptografi olarak bilinen kuantum dirençli kriptografik yöntemlerin geliştirilmesinin aciliyeti, kriptografi topluluğunun proaktif duruşunu vurgulamaktadır.

Kuantum kriptanalizin ve kuantum dirençli kriptografinin gelişen ortamında, araştırmacılar oyunun kurallarını yeniden şekillendiriyor. Bu alan, kuantum bilişimin gücünün güvenliği, gizliliği ve bilgi alışverişini önemli ölçüde etkileyeceği yeni bir çağın ön saflarında yer alıyor. Yolculuk ilerledikçe kırılamaz kodların arayışı, şifrelemenin ve veri korumanın geleceğini şekillendirerek insan yaratıcılığının sınırlarını zorlamaya devam etmektedir.

Kuantum bilgisayarları ilerledikçe, kuantum dirençli veya kuantum sonrası şifreleme algoritmalarının geliştirilmesi ve standartlaştırılması konusunda artan bir aciliyet vardır. Kriptografi topluluğu, kuantum saldırılarına dayanabilecek ve dijital iletişimin uzun vadeli güvenliğini sağlayacak çözümler üzerinde aktif olarak çalışmaktadır.

Kuantum Anahtar Dağıtımı, geniş ölçekte başarılı bir şekilde uygulanırsa, iletişim kanallarının güvenliğini sağlamak için ana akım teknoloji haline gelebilir. QKD, güvenli şifreleme anahtarları oluşturmak için kuantum mekaniği ilkelerinden

yararlanarak benzersiz bir avantaj sunar ve teknoloji olgunlaştıkça benimsenmesi artabilecektir.

Kuantum dirençli algoritmaların klasik kriptografinin yerini almak yerine mevcut kriptografik sistemlere entegre edilmesi muhtemeldir. Klasik ve kuantum dirençli teknikleri birleştiren hibrit yaklaşımlar, özellikle kuantum bilgisayarların daha güçlü hale geldiği geçiş döneminde ekstra bir güvenlik katmanı sağlayabilecektir.

Genellikle kuantum internet olarak adlandırılan kuantum iletişim ağlarının geliştirilmesi umut verici bir yoldur. Bu ağlar, kuantum dolaşma ve diğer kuantum özelliklerinden yararlanarak uzun mesafelerde güvenli iletişimi mümkün kılabilir. Kuantum tekrarlayıcılar ve kuantum uyduları bu tür ağların gerçekleştirilmesinde kilit rol oynayacaktır.

Kuantum bilgisayarları ilerledikçe kuantum kriptanaliz teknikleri de gelişecek. Araştırmacılar ve kriptanalistler mevcut kriptografik sistemleri kırmak için yeni algoritmalar ve stratejiler keşfetmeye devam edecekler. Kuantum kriptanalizi ile kuantum dirençli kriptografi arasında devam eden bu silahlanma yarışı, dijital güvenliğin geleceğini şekillendirecektir.

Kuantum kriptografisi alanı, kuantum fiziği, bilgisayar bilimi ve matematik dahil olmak üzere çeşitli alanlardan uzmanlık gerektirir. Disiplinlerarası işbirlikleri, karmaşık zorlukların üstesinden gelmede ve kuantum kriptografideki yenilikleri yönlendirmede büyük olasılıkla çok önemli bir rol oynayacaktır.

Kuantum bilgisayarların muazzam hesaplama gücü, olası kötüye kullanıma ilişkin etik kaygıları artırıyor. Olumlu uygulamalar için ilerleyen kuantum teknolojileri ile kuantum kriptanalizinin etik sonuçlarına değinmek arasında bir denge kurmak çok önemlidir.

Kuantum teknolojilerinin ortaya çıkışıyla birlikte eğitim ve farkındalık girişimlerine olan ihtiyaç giderek artacaktır. Bu çabalar, kuantum kriptografisinin, sonuçlarının ve gelecekteki güvenlikteki rolünün kapsamlı bir şekilde anlaşılmasını sağlamak için hem genel halkı hem de alandaki profesyonelleri hedef alacaktır.

Kuantum kriptografisinin geleceği muhtemelen kuantum güvenli kriptografideki gelişmeler, kuantum anahtar dağıtımının artan şekilde benimsenmesi, kuantum iletişim ağlarının evrimi ve etik hususları ele almaya yönelik devam eden çabaların bir kombinasyonu ile işaretlenecektir. Alan dinamiktir ve kuantum teknolojileri ilerledikçe gelişmeye devam edecektir.

Kuantum bilgisayarları daha güçlü hale geldikçe, Shor algoritması gibi kriptanaliz için kuantum algoritmalarının etkinliği artacaktır. Bu, yaygın olarak kullanılan şifreleme şemaları, özellikle de tamsayı çarpanlara ayırma veya ayrık logaritmalara dayananlar için potansiyel bir tehdit oluşturmaktadır. Araştırmacılar, klasik şifreleme sistemlerini daha da tehlikeye atabilecek yeni kuantum algoritmalarını keşfetmeye ve geliştirmeye devam edecektir.

Kuantum sonrası kriptografik algoritmaların geliştirilmesi ve konuşlandırılması, kuantum çağında güvenli iletişimi sürdürmek için çok önemlidir. PQC, kuantum saldırılarına karşı dayanıklı şifreleme yöntemleri oluşturmayı amaçlamaktadır. NIST'in Kuantum Sonrası Şifreleme Standardizasyon projesi gibi standardizasyon çabaları, kuantum dirençli algoritmaların değerlendirilmesinde ve seçilmesinde önemli bir rol oynayacaktır.

QKD, kriptografik anahtarlar oluşturmak için kuantum mekaniği ilkelerinden yararlanarak güvenli iletişim kanalları sağlama potansiyeline sahiptir. QKD teknolojisindeki ilerlemeler, daha pratik uygulamalara ve kritik uygulamalarda daha fazla benimsenmeye yol açacaktır. QKD'nin klasik kriptografik sistemlerle entegrasyonu daha yaygın hale gelebilir ve gelişmiş güvenlik için hibrit çözümler sunulacaktır.

Genellikle kuantum internet olarak adlandırılan kuantum güvenli iletişim ağlarının geliştirilmesi, güvenli iletişimi yeniden tanımlayabilir. Dolaşma ve kuantum ışınlanma gibi ilkelere dayanan kuantum ağları, uzun mesafelerde güvenli iletişime olanak sağlayacaktır.

Kuruluşlar ve endüstriler, kuantum sonrası dönemde dijital iletişimin güvenliğini sağlamak için muhtemelen kuantum dirençli kriptografik standartlar

oluşturacaktır. Klasikten kuantum dirençli algoritmalara geçiş, dikkatli planlama ve koordinasyon gerektirecektir.

Kuantum bilgisayarların güçlü yetenekleri mahremiyet, veri güvenliği ve olası kötüye kullanıma ilişkin etik kaygıları artırıyor. Politika yapıcıların ve araştırmacıların, kuantum teknolojilerinin geliştirilmesi ve kullanımını çevreleyen etik yönergeler ve düzenlemeler oluşturmak için işbirliği yapması gerekecek.

Kuantum güvenliği küresel bir endişe kaynağıdır ve kuantum kriptanalizinin ortaya çıkardığı zorlukların çözümünde uluslararası işbirliği hayati önem taşıyacaktır. Araştırmaların, en iyi uygulamaların ve standartların paylaşılması, daha güvenli bir dijital ortama katkıda bulunacaktır.

Kuantum teknolojilerinin güvenlik açısından etkileri konusunda halkı, işletmeleri ve politika yapıcıları eğitmeye daha fazla odaklanılacak. Farkındalığı artırmak ve anlayışı teşvik etmek, bilinçli kararlar almak için gerekli olacaktır.

Kuantum kriptanalizinin ve güvenliğinin geleceği, kuantum güvenli kriptografideki gelişmeler, güvenli iletişim ağlarının geliştirilmesi ve kuantum teknolojilerinin mevcut altyapılara entegrasyonunun birleşimiyle şekillenecek. Devam eden araştırma, işbirliği ve etik hususlar, gelişen kuantum güvenliği ortamında yön bulmada hayati önem taşıyacaktır.

KAYNAKLAR

2.1 - A Short History of Cryptography. (n.d.). **http://all.net/edu/curr/ip/Chap2-1.html**

A. K. Ekert, (1991). Quantum cryptography based on bell's theorem. Phys. Rev. Lett.

Anderson, D. (2018). Review of Code Girls: The untold story of the American women code breakers of World War II by Liza Mundy. Cryptologia, 42(3), 258–261.https://doi.org/10.1080/01611194.2018.1428837

Betz, H. D. (2022). *The Greek Magical Papyri in Translation, Including the Demotic Spells, Volume 1*. University of Chicago Press. **http://books.google.ie/books?id=BNKREAAAQBAJ&printsec=frontcover&dq=The+Greek+Magical+Papyri+in+Translation,+Including+the+Demotic+Spells,+Volume+1&hl=&cd=1&source=gbs_api**

Betz, H. D. (2022). *The Greek Magical Papyri in Translation, Including the Demotic Spells, Volume 1*. University of Chicago Press. **http://books.google.ie/books?id=BNKREAAAQBAJ&printsec=frontcover&dq=The+Greek+Magical+Papyri+in+Translation,+Including+the+Demotic+Spells,+Volume+1&hl=&cd=1&source=gbs_api**

C. A. Fuchs, N. Gisin, R. B. Griffiths, C.-S. Niu, and A. Peres. (1997) Optimal eavesdropping in quantum cryptography. i. information bound and optimal strategy. Phys. Rev. A, 56:1163,

C. H. Bennett and G. Brassard. (1984). Quantum cryptography: Public key distribution and coin tossing, In Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, pages 175–179, Bangalore, India. IEEE, New York

C. Shannon, (1949). Communication theory of secrecy systems. Bell System Technical Journal, 28(4):656

Censoring crypto not the answer says Schneier. (2001). *Network Security, 2001*(10), 4. **https://doi.org/10.1016/s1353-4858(01)01011-x**

D. Bruss, (1998). Optimal eavesdropping in quantum cryptography with six states. Phys. Rev. Lett. , 81:3018.

D. Mayers, (2001). Unconditional security in quantum cryptography. Journal of the ACM, 48(3):351406.

Dale, C. (2023). *History of Encryption | SANS Institute*. **https://www.sans.org/white-papers/730/**

Dynes, J. F., Takesue, H., Yuan, Z. L., Sharpe, A. W., Harada, K., Honjo, T., Kamada, H., Tadanaga, O., Nishida, Y., Asobe, M., & Shields, A. J. (2009). Efficient entanglement distribution over 200 kilometers. *Optics Express*, *17*(14), 11440. **https://doi.org/10.1364/oe.17.011440**

F. (2001). *A Brief History of Cryptography*. **https://cryptozine.blogspot.com/2008/05/brief-history-of-cryptography.html**

Froomkin, D., & Froomkin, A. M. (2021). Fixing the Senate: A User's Guide. *SSRN Electronic Journal*. **https://doi.org/10.2139/ssrn.3797782**

Gasbarri, G., Belenchia, A., Carlesso, M., Donadi, S., Bassi, A., Kaltenbaek, R., Paternostro, M., & Ulbricht, H. (2021). Testing the foundation of quantum physics in space via Interferometric and non-interferometric experiments with mesoscopic nanoparticles. *Communications Physics*, *4*(1). **https://doi.org/10.1038/s42005-021-00656-7**

Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. Reviews of Modern Physics, 74(1), 145–195. https://doi.org/10.1103/revmodphys.74.145

Gottesman, D., Lo, H. K., L\"utkenhaus, N., & Preskill, J. (2004). Security of quantum key distribution with imperfect devices. *Quantum Information and Computation*, *4*(5), 325–360. **https://doi.org/10.26421/qic4.5-1**

***History of Cryptography*.** (n.d.). (2006). **http://www.cypher.com.au/crypto_history.htm**

Ji, L., Gao, J., Yang, A. L., Feng, Z., Lin, X. F., Li, Z. G., & Jin, X. M. (2017). Towards quantum communications in free-space seawater. *Optics Express*, *25*(17), 19795. **https://doi.org/10.1364/oe.25.019795**

Kahn, D. (1996). *The Codebreakers*. Simon and Schuster. **http://books.google.ie/books?id=3S8rhOEmDIIC&printsec=frontcover&dq=The+Codebreakers+David+Kahn&hl=&cd=1&source=gbs_api**

Kurtsiefer, C., Zarda, P., Halder, M., Weinfurter, H., Gorman, P. M., Tapster, P. R., & Rarity, J. G. (2002). A step towards global key distribution. *Nature*, *419*(6906), 450–450. **https://doi.org/10.1038/419450a**

Kutash, G. (2023). Enigma Code of "The Secret Sharer." The AnaChronisT, 21(2). https://doi.org/10.53720/xwma9014

Lo, H. K., & Chau, H. F. (1999). Unconditional Security of Quantum Key Distribution over Arbitrarily Long Distances. Science, 283(5410), 2050–2056. https://doi.org/10.1126/science.283.5410.2050

Mo, X. (2010). Quantum-key distribution using quantum frames. SPIE Newsroom. **https://doi.org/10.1117/2.1201008.003132**

M. Aspelmeyer, T. Jennewein, M. Pfennigbauer, W. R. Leeb, and A. Zeilinger. (2003). Long-distance quantum communication with entangled photons using

satellites. IEEE Journal of Selected Topics in Quantum Electronics, special issue on Quantum Internet Technologies, 9:1541–1551,

Popkin, G. (2017). Spooky action achieved at record distance. *Science*, *356*(6343), 1110–1111. **https://doi.org/10.1126/science.356.6343.1110**

Pugh, C. J., Kaiser, S., Bourgoin, J. P., Jin, J., Sultana, N., Agne, S., Anisimova, E., Makarov, V., Choi, E., Higgins, B. L., & Jennewein, T. (2017). Airborne demonstration of a quantum key distribution receiver payload. *Quantum Science and Technology*, *2*(2), 024009. **https://doi.org/10.1088/2058-9565/aa701f**

R. Renner (2005)., Security of Quantum Key Distribution. PhD thesis, Swiss Federal Institute of Technology.

Quantum Cryptanalysis: Hype and Reality. (n.d.). Default. **https://www.lawfaremedia.org/article/quantum-cryptanalysis-hype-and-reality**

Salomon, D. (2006). *Coding for Data and Computer Communications*. Springer Science & Business Media.

The Project Gutenberg EBook of The Kama Sutra of Vatsyayana, by Richard Francis Burton, Bhagavanlal Indrajit, and Shivaram Parashuram Bhide. (n.d.). **https://www.gutenberg.org/files/27827/27827-h/27827-h.htm**

Watrous, J. (2009). Zero-Knowledge against Quantum Attacks. *SIAM Journal on Computing*, *39*(1), 25–58. **https://doi.org/10.1137/060670997**

Weier, H., Schmitt-Manderbach, T., Regner, N., Kurtsiefer, C., & Weinfurter, H. (2006). Free space quantum key distribution: Towards a real life application. *Fortschritte Der Physik*, *54*(8–10), 840–845. **https://doi.org/10.1002/prop.200610322**

Winick, A., Lütkenhaus, N., & Coles, P. J. (2018). Reliable numerical key rates for quantum key distribution. Quantum, 2, 77. **https://doi.org/10.22331/q-2018-07-26-77**

X. Ma. Security of quantum key distribution with realistic devices, (2004). arXiv: quantph/0503057

Zhao, Y., Fung, C. H. F., Qi, B., Chen, C., & Lo, H. K. (2008). Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. Physical Review A, 78(4). **https://doi.org/10.1103/physreva.78.042333**

ÖZGEÇMİŞ

Ad-Soyad **:** Fatih Ali KOÇ

ÖĞRENİM DURUMU **:**

- **Lisans** **:** 2021, Beykent Üniversitesi, Fen Edebiyat Fakültesi, Matematik
- **Yüksek Lisans** **:** 2024, Haliç Üniversitesi, Matematik Anabilim Dalı, Uygulamalı Matematik Tezli Yüksek Lisans Programı