T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KUANTUM ANAHTAR DEĞİŞİM PROTOKOLLERİNE KARŞI YAPILAN SALDIRILARIN ANALİZİ VE SAVUNMA YÖNTEMLERİ

İLKER BURAK ADIYAMAN
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

GEBZE
2021

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KUANTUM ANAHTAR DEĞİŞİM PROTOKOLLERİNE KARŞI YAPILAN SALDIRILARIN ANALİZİ VE SAVUNMA YÖNTEMLERİ

İLKER BURAK ADIYAMAN
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMANI
PROF. DR. İBRAHİM SOĞUKPINAR

GEBZE
2021

T.R.

GEBZE TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

ANALYSIS AND DEFENSE METHODS OF ATTACKS AGAINST QUANTUM KEY EXCHANGE PROTOCOLS

İLKER BURAK ADIYAMAN

A THESIS SUBMITTED FOR THE DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF COMPUTER ENGINEERING

THESIS SUPERVISOR

PROF. DR. İBRAHİM SOĞUKPINAR

GEBZE

2021

GEBZE TEKNİK ÜNİVERSİTESİ	**YÜKSEK LİSANS JÜRİ ONAY FORMU**

GTÜ Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 05/02/2021 tarih ve 2021/06 sayılı kararıyla oluşturulan jüri tarafından 22/02/2021 tarihinde tez savunma sınavı yapılan İlker Burak ADIYAMAN'ın tez çalışması Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE
(TEZ DANIŞMANI) : PROF. DR. İBRAHİM SOĞUKPINAR

ÜYE : DOÇ. DR. MEHMET GÖKTÜRK

ÜYE : DOÇ. DR. ALİ GÖKHAN YAVUZ

ONAY

Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
..…/……/…… tarih ve ……/…..... sayılı kararı.

ÖZET

Kuantum anahtar dağıtımı protokollerinin temel amacı ve faydası şifrelemede kullanılan tek kullanımlık anahtarın gönderici ve alıcı tarafında pratik ve güvenli bir şekilde iletimini sağlamaktır. Bu iletim yöntemi temelde kuantum fiziğine dayandığından klasik anahtar dağıtım yöntemlerine göre daha fazla yüksek güvenlik sağlamaktadır.

Günümüzde güvenli iletişim için matematiksel yöntemlere dayanan RSA gibi şifreleme algoritmaları kullanılmaktadır. Ancak kuantum bilgisayarların yaygınlaşmasıyla birlikte bu şifreler yakın gelecekte yüksek işlem gücüyle kısa sürede kırılabilecektir. Halen kötü niyetli kullanıcıların iletişimleri dinleyerek anahtarları depoladığı ve bunları kırmak için kuantum bilgisayar ve işlem gücünü bekledikleri bilinmektedir. İletişimi dinlemeyi engellemek için ve aradaki saldırganın tespitini sağlamak için yine kuantum teknolojileri bizlere yardımcı olacaktır.

Bu çalışmada kuantum fiziği ve kuantum anahtar dağıtım (KAD) protokolleri ele alınmış, ilk öne sürülen ve pratikte en fazla kullanılan BB84 protokolü ve çalışma ilkeleri anlatılmış, ışık kaynakları, detektörler ve BB84 protokolü hakkında genel bilgi verildikten sonra BB84 kuantum anahtar değişim protokolüne karşı yapılan saldırılar ve savunma yöntemleri hakkında bilgilendirme yapılmıştır. Sonraki bölümde kuantum anahtar dağıtımı teknolojisinin mevcut iletişim altyapıları ile birleştirilerek günümüzde gizlilik gerektiren birçok iletişim ağının çok daha güvenli hale getirilebileceği bir sistem önerilmiştir. Önerilen sistemin amacı günümüzde kullanılan açık anahtarlı şifreleme iletişim yöntemlerine kuantum anahtar değişim protokolünü ekleyerek matematiksel ve kuantum fiziği temelli hibrit yapı ile iletişim esnasında araya giren saldırganları belirleyerek 'ortadaki adam' tehdidini tamamen önlemektir. Dördüncü bölümde, tasarımda yer alan kuantum kanalı üzerinden iletişimde aradaki dinleyicinin tespiti farklı parametrelerle benzetim ortamında uygulanmış, sonuçlar detaylı analiz edilmiştir.

Anahtar Kelimeler: Kuantum Anahtar Dağıtım Protokolleri, Kuantum İletişimi, BB84, Yakala/Tekrar Gönder Saldırısı, PNS, QKD, Kuantum Saldırıları.

SUMMARY

The main purpose and benefit of quantum key distribution protocols is to provide a practical and secure transmission of the single-use key used in encryption on the sender and receiver side. Since this transmission method is basically based on quantum physics, it provides higher security than classical key distribution methods.

Today, encryption algorithms such as RSA based on mathematical methods are used for secure communication. However, with the widespread use of quantum computers, these codes will be able to be cracked in a short time with high processing power in the near future. Currently, it's known that there are malicious who are listening communications, storing keys and waiting for quantum computing and processing power to crack them. Quantum technologies also will help us to prevent listening to communication and to detect the attacker in between.

In this study, quantum physics and quantum key distribution (KAD) protocols are discussed, BB84, the first proposed and most widely used protocol and its working principles are explained, after giving general information about light sources, detectors and the BB84 protocol, we gave information about attacks against the BB84 quantum key exchange protocol and defense methods. In the next section, a system is proposed in which many communication networks that require privacy today can be made much more secure by combining quantum key distribution technology with existing communication infrastructures. The purpose of the proposed system is to completely prevent the "man in the middle" threat by adding the quantum key exchange protocol to the public-key encryption communication methods used today, identifying the intruders during communication with a mathematical and quantum physics-based hybrid structure. In the fourth chapter, the detection of the attacker in communication over the quantum channel in the design is applied in the simulation environment with different parameters and the results are analyzed in detail.

Key Words: Quantum Key Exchange Protocols, Quantum Communication, BB84, Intercept/Resend Attack, PNS, QKD, Quantum Attacks.

TEŞEKKÜR

Öncelikle yüksek lisans eğitimim boyunca desteğini ve yardımlarını esirgemeyen ve bu çalışmamın oluşmasını sağlayan danışman hocam Prof. Dr. İbrahim SOĞUKPINAR'a, göstermiş olduğu desteklerinden dolayı aileme en içten teşekkürlerimi sunarım.

İÇİNDEKİLER

	Sayfa
ÖZET	v
SUMMARY	vi
TEŞEKKÜR	vii
İÇİNDEKİLER	viii
SİMGELER ve KISALTMALAR DİZİNİ	x
ŞEKİLLER DİZİNİ	xi
TABLOLAR DİZİNİ	xii
1. GİRİŞ	1
1.1. Tezin Amacı, Önemi ve İçeriği	2
2. KURAMSAL TEMEL BİLGİLER VE İLGİLİ ÇALIŞMALAR	3
2.1. Kuantum Mekaniği	3
2.2. Kuantum Bilgisayarlar ve Kübit Kavramı	4
2.3. Kuantum Anahtar Değişimi ve Anahtar Değişim Protokolleri	6
2.3.1. BB84 Quantum Anahtar Değişim Protokolü	7
2.3.2. B92 Protokolü	8
2.3.3. EPR-Ekert Protokolü	9
2.3.4. SARG Protokol	9
3. KUANTUM ANAHTAR DEĞİŞIM PROTOKOLÜNE KARŞI YAPILAN SALDIRILAR	10
3.1. BB84 Kuantum Anahtar Değişim Protokolüne Karşı Yapılan Saldırılar	10
3.1.1. Foton Numarası Bölme Saldırısı (PNS)	10
3.1.2. Engelle / Tekrar Gönder Saldırısı	11
3.1.3. Truva Atı Saldırısı	11
3.1.4. Sahte Durum Saldırısı	11
3.1.5. Zaman Kaydırma Saldırısı	12
3.1.6. Spektral Saldırısı	12
3.1.7. Yan Kanal Saldırısı	12
3.2. BB84 Protokolü ile Güvenlik Artırımı	12
3.2.1. Önerilen Yöntem	12
4. DENEYSEL ANALİZ VE DEĞERLENDİRME	20

5. SONUÇ VE ÖNERİLER 27

KAYNAKLAR 28
ÖZGEÇMİŞ 32
EKLER 33

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler ve Kısaltmalar		**Açıklamalar**
3DES	:	Triple Data Encryption Algorithm
AES	:	Advanced Encryption Standard
BB84	:	Bennett and Brassard 1984
DH	:	Diffie Hellman
KAD	:	Kuantum Anahtar Dağıtımı
OTP	:	One Time Password
PKE	:	Public Key Encryption
PNS	:	Photon Number Splitting
QKD	:	Quantum Key Distribution
RSA	:	Rivest–Shamir–Adleman
SSL	:	Secure Socket Layer

ŞEKİLLER DİZİNİ

Şekil No:		Sayfa
2.1:	Klasik bit – kübit karşılaştırması.	5
2.2:	BB84 iletişimi esnasında foton gönderimi.	8
3.1:	Kuantum sonrasında kripto sistemlerin güvenlik seviyeleri	14
3.2:	Günümüzde kullanılan açık anahtarlı şifreleme.	14
3.3:	Önerilen yöntem tasarımı.	15
3.4:	Önerilen yöntem çalışma şeması.	16
4.1:	BB84 protokolünün QKD Simülatör ile uygulanmasında seçilen konfigürasyon değerleri.	20
4.3:	Yakala/tekrar gönder saldırısı.	21
4.4:	Sonuç anahtar uzunluklarının karşılaştırılması.	26

TABLOLAR DİZİNİ

Tablo No:		Sayfa
4.1:	Benzetim başlangıç parametreleri.	21
4.2:	Benzetim sonuçları.	24
4.3:	Saldırı durumunda hata oranı.	25
4.4:	Başlangıç konfigürasyonu sabit tutularak saldırı ve saldırı olmadığı durumda anahtar uzunlukları.	25

1. GİRİŞ

Kuantum şifreleme teknolojisinde veri iletimi klasik yöntem olan elektriksel işaretler yerine fotonlar ile yapılmaktadır ve temel olarak alıcı ile gönderici arasındaki fotonların durumlarının iletimine dayanmaktadır. Kuantum şifrelemenin temeli Heinsberg'in belirsizlik ilkesine dayanmaktadır [4]. Buna göre fotonunun dönüş, kutuplanma özellikleri ölçülmek istendiğinde foton değişim gösterir ve bu da iletişim esnasında aradaki dinleyicinin tespit edilmesini sağlar. Fotonların veya elektronların dönüş ve kutuplaşma özellikleri 1 ya da 0 olarak kodlanır [6]. Kuantum mekaniği temelde atom altı parçacıklar dünyasıyla ilgilenen bir bilim dalı olsa da günümüzde elektronik, biyoloji gibi birçok alana bilimsel katkısı olmuştur.

Kuantum durumu fotonların polarizasyon adı verilen fiziksel karakterlerini temsil eder. İletişim kanalı için fiber optik ağ kullanılmaktadır ve iletişimin gürültü, manyetik alan gibi çevresel faktörlerden etkilenmemesi amaçlanır. Bununla birlikte alıcı ve gönderici tarafında foton üreteci ve süzgeçler gerekmektedir. Bir diğer kısıtlama da iletişimin uzak mesafeler arasında mümkün olamamasıdır. Kuantum anahtar dağıtımında fotonun seçilen filtreye göre belirli bir açıda kutuplaşma özelliği kullanılır. Fotonlar seçilen filtrenin türüne göre dikey ve yatayda kutuplaşır. İletimin güvenli bir şekilde tamamlanabilmesi için kuantum kanal ve açık kanal olmak üzere iki kanal kullanılmaktadır.

Bir çok kuantum anahtar değişimi protokolü bulunmaktadır. Bunlar arasında en bilinenler BB84 [1], B92 [6], Ekert [7] ve SARG [8] protokolleridir. Bu protokollerin temelde çalışma biçimleri benzer olmasına rağmen fotonların nasıl düzenlendiği ve iletildikleri konularında farklılık gösterirler. Kuantum anahtar dağıtımı protokolleri her ne kadar güvenliği artırmış olsa da günümüzde bu protokollere karşı bazı saldırılar mevcuttur. Bu saldırıların pratikte uygulanması oldukça zor olmakla birlikte kuantum bilgisayarlarının ve kuantum iletişim tekniklerinin yaygınlaşmasıyla bu saldırıların önlenmesi önem arz edecektir. Truva atı saldırısı, engelle / tekrar gönder saldırısı, zaman kaydırma saldırısı, foton bölme saldırısı bunlardan birkaçıdır.

Kuantum bilgisayar yakın gelecekte sağladıkları yüksek işlem gücüyle 2048-bit RSA şifresinin dayanıklılık ömrünü yıllardan saatlere indirecektir. Bu durum hükümet, milli savunma, ordu ve büyük elçilikler gibi kurumların birbiriyle iletişimini ve kritik verilerini tehlikeye atmaktadır. Belirtilen kritik yapıların verileri

hâlâ 2048 bit RSA şifreleme veya benzer bir yöntemle gönderiliyorsa bu kuruluşlar önlem almaya başlamalıdır. 2048 bitlik RSA şifresinin kübitler ile 8 saatte kırıldığını gösteren çalışma [16] bu önergeyi kanıtlar niteliktedir.

1.1. Tezin Amacı, Önemi ve İçeriği

Bu tez kapsamında, öncelikle kuantum mekaniği ve kübit kavramı ile kuantum bilgisayarlar hakkında bilgi verilmiş, devamında kuantum anahtar değişim protokolleri ve en yaygın kuantum anahtar değişim protokolü BB84 [1] ve diğer kuantum anahtar değişim protokollerine karşı yapılan saldırılar anlatılmış, saldırı teknikleri ile ilgili önceki çalışmalar hakkında bilgiler verilmiş ve savunma yöntemleri açıklanmıştır. Üçüncü bölümde açık anahtarlı iletişim sistemine kuantum anahtar dağıtım protokolü eklenerek aradaki dinlemeyi kuantum fiziğinin özellikleriyle önleyecek hibrit sistem önerilmiştir. Dördüncü bölümde önerilen sistemde gönderici ve alıcı arasında yer alan kuantum anahtar değişimi benzetim ortamında gerçekleştirilmiş, arada yakala/tekrar gönder saldırısı yapan saldırganın olması durumunda sonuç verilerine etkisi ve saldırganın tespiti üzerine yorumlarda bulunulmuştur. Sonuç bölümünde sonuçlar değerlendirilmiş ve gelecek çalışmalar için önerilerde bulunulmuştur.

2. KURAMSAL TEMEL BİLGİLER VE İLGİLİ ÇALIŞMALAR

2.1. Kuantum Mekaniği

Kuantum mekaniğinin temelleri 20. yüzyılın ilk yarısında Albert Einstein, Werner Heisenberg, John von Neumann gibi dönemin önemli bilim adamlarınca atılmıştır. Belirsizlik ilkesi, dolanıklık, süper pozisyon gibi kavram ve teoriler yine bu alanda kendisini göstermiştir.

Kuantum mekaniği maddenin atom altı seviyelerde enerji ve davranışları ile elektron, foton gibi parçacıkların birbirleriyle olan ilişkisini inceler. Kuantum mekaniğine göre ışık bazen parçacık bazen dalga gibi davranır. 18. yüzyıldan itibaren yapılan deneyler ışığın dalga modeline uyduğunu söylemekteydi ancak kuantum fiziğindeki araştırma sonuçları göstermiştir ki ışık parçacık olarak da özellik göstermektedir.

Kuantum mekaniği foton veya proton gibi, aynı anda hem parçacık hem de dalga halinde olabilen atom altı parçacıklarının ne şekilde davrandıkları ile ilgilenir. Dalganın yerini belirlemeye kalktığımızda bu özelliğin kaybolarak parçacık gibi davranmaya başlaması özelliği aynı zamanda yıldızlar ve galaksiler gibi çok büyük nesneleri ya da büyük patlama gibi olayları analiz etmemizi ve açıklamamızı sağlar. Kuantum kuramında klasik mekaniğin aksine parçacıklar hız ve konum yerine parçacığa ait bütün bilgiyi içeren dalga fonksiyonu ile gösterilir ve bu fonksiyondan donen cevaplara göre parçacık hakkında bilgi sahibi olunur. Parçacık ile dalga ilişkisi en basit şekilde çift yarık deneyinde gözlenebilir. Deneyde elektronlar, yani parçacıklar birbirine çok yakın ve çok ince iki deliğe birer birer ateşlenirler. Bu durumda parçacıklar normalde bilye gibi nesneleri fırlattığınızda olacağın aksine, deliğin öteki tarafındaki perdede iki sütun halinde birikmek yerine çizgili bir desen oluştururlar. Bunun sebebi birbiriyle girişim yapan yani üst üste binen dalgalar gibi davranmalarıdır. Ancak onları gözlemeye, yani yerlerini belirlemeye kalktığımız anda bu desen kaybolur ve tıpkı parçacık davranışı göstererek perdenin arkasında iki sütun olarak birikmeye başlarlar. Çünkü gözlem ile ortama müdahale etmiş oluruz ve bu durum süper pozisyon halinin devam etmeyerek elektronun sadece bir yarıktan geçmesine neden olur. Sonuçta elektronun dalga özelliği kaybolur ve parçacık şeklinde davranır. Elektronlar kuantum nesneleri olduğu için konumunu bilemeyiz.

Örneğin, bir atomun yerini daha hassas bir şekilde bildiğinizde, atomun hızını daha az hassaslıkla bilebilirsiniz. Elektronların yarıkların herhangi birinden geçme olasılığı vardır. Kuantum fiziğinde süper pozisyon ilkesi burada açığa çıkmaktadır, çünkü elektronların her iki yarıktan geçme olasılığı olduğundan aslında her iki yarıktan da aynı anda geçmektedir. Gözlem sonucunda elektronun detektöre çarparak, parlak bir ışık meydana getirmesi de dalga fonksiyonunun çökmesini açıklar. Burada gözlem, kuantum seviyesinde parçacıklara yapılan müdahaledir. Örneğin bir parçacığın konumunu öğrenmek istiyorsanız, o parçacığın üzerine başka bir parçacık (elektron veya foton) göndermeniz gerekir. Bu gönderdiğiniz elektron veya foton sizin gözlem aracınızdır ve gözlemlemek istediğiniz parçacığa çarpar, ondan sekerek geriye detektörünüze gelir ve konumunu öğrenmiş olursunuz. Ancak bu müdahale parçacığın konumunu hatta hızını değiştirir ve konumu değiştiği için artık sadece belli bir yüzdelik değerde tespit edeceğiniz gibi, hızını ve yönü de artık tespit edilemeyecek duruma gelmiş olur. Kuantum mekaniğinde taneciklerin aslında dalga şeklinde hareket ettiği düşünülmektedir. Bu durum klasik fizikte maddenin küçük taneciklerden oluştuğu şeklinde ele alınmasından farklıdır. Kuantum mekaniğini anlamak için klasik mekaniğin yanında ışık dalgaları, dolanıklık ve kopyalanamama teoremi gibi konuları bilmek gereklidir.

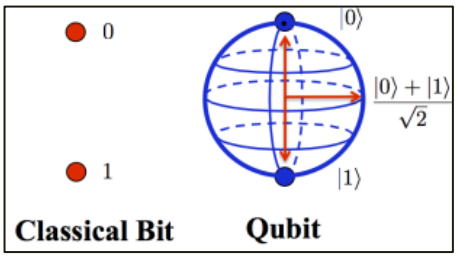
Kuantum fiziğinin önemli ilkelerinden olan dolanıklık durumu sadece kuantum mekaniği prensipleriyle çalışma özelliği olan kuantum bilgisayarlarda olabilecek bir durumdur. Dolanıklık, birbirinden oldukça uzakta olan iki olayın aralarında mesafe olmasına rağmen aralarındaki ilişkiden faydalanılarak olaylardan biri üzerinde yapılan ölçüm ile diğer olay hakkında bilgi edinmektir. Parçacıkların herhangi biri üzerinde yapılan ölçüm ne kadar uzakta olursa olsun diğerini anında etkileyeceği şekilde birbirlerine bağlıdırlar.

2.2. Kuantum Bilgisayarlar ve Kübit Kavramı

Kuantum bilgisayarlarda, klasik bilgisayarlardaki bitlerin yerine iki durumlu kuantum bitleri yani kübitler kullanılır [38]. Foton, elektron gibi atom altı parçacıklar kübit olarak kullanılabilir. Günümüz bilgisayarları çok hızlı işlem yapmalarına rağmen tek seferde yalnızca bir işlem yapabilirler. Ancak bu yoğun hesaplama gerektiren işlemlerde oldukça uzun zaman alır. Kuantum bilgisayarlar ise kuantum

fiziğine dayandığından ve kuantum fiziğinde moleküller aynı anda birçok yerde olabildiğinden kuantum bilgisayar çok fazla sayıda yolu ya da çözümü aynı anda araştırıp doğru olanı çok hızlı şekilde bulabilir çünkü önceki bolümde verilen örnekte anlatıldığı üzere kuantum fiziği bir parçacığın her iki durumda birden olabileceğini bize söylemektedir.

Elektronların dönüşleri (spin), fotonların kutuplanma özelliği gibi iki seviyeli kuantum fiziği yasalarına uyan herhangi bir sistem kübit olarak kullanılabilir. Örneğin elektronların dönüşleri, iki seviyeli sistemlerin bir örneğidir. Bu dönüşler yukarı ve aşağı yönlüdür. Bir parçacığın dönüşü yukarıysa, dolanık durumdaki eşinin dönüşü aşağı doğrudur ve bu gözlemin olduğu anda anlık olarak belirlenir. Bir fotonun dikey ya da yatay kutuplaşması, ya da bir elektronun belirli veya aksi yönde dönmesi ihtimali klasik bilgisayarlarda 0 veya 1 değerini alan bit yapısına karşılık gelir. Ancak klasik fizikten farklı olarak elektron sadece bu iki değeri değil bu iki değer arasında bir değer de alabilir yani sadece bu iki yönde değil başka herhangi bir yönde de olabilir. Dolayısıyla bir elektronun dönüşü sadece 0 ve 1 durumlarını kodlamak için değil bu durumların herhangi bir lineer kombinasyonunu kodlamak için de kullanılabilir. Elektron ve fotonların yanında atom çekirdeklerinin dönüşü de kübit olarak kullanılabilir. İki seviyeli sistemler dışında ikiden fazla seviyeli sistemlerin de kuantum mekaniği ilkelerini sağladığı sürece kübit olarak kullanılması mümkündür.



Şekil 2.1: Klasik bit – kübit karşılaştırması.

Kübit süperpozisyon durumundaysa ve süperpozisyonda olan başka bir kübit ile birlikte hesaplama sonucunda 1-0, 1-1, 0-1 ve 0-0 olmak üzere 4 farklı sonuç elde edilir. Bu durumlar klasik bilgisayarlarda hesaplama sonucunda alınan 1-0 veya 0-1 gibi tek bir değer almasından farklı olarak kübitlerin süper pozisyon durumundan belirli bir duruma çökene kadar aldığı değerlerdir. Kübitlerin artırılması ile yapılacak

hesaplama gücü üssel olarak artar, bu da kuantum bilgisayarların işlem hızı ve es zamanlı olarak çoklu işlem yapabilme gücünü sağlar.

Kübitlerin önemli bir dezavantajı kuantum bozunumudur, yani sıcaklık, elektromanyetik alan gibi çevresel faktörlerden kolayca etkilenip bozunuma uğrayabileceğidir, bu nedenle bilgileri yani geçerli hallerini oldukça kısa sureyle koruyabilmektedir ve araştırmacılar bu sürenin uzatılmasının yollarını aramaktadır.

2.3. Kuantum Anahtar Değişimi ve Anahtar Değişim Protokolleri

Kuantum anahtar dağıtımı güvenli olmayan bir kanal üzerinden iki taraf arasında bir şifreleme anahtarının güvenli bir şekilde oluşturulmasını sağlar. Bu teknik kuantum mekaniğinin temel özelliklerine dayanır ve ışığın, lazerlerin, fiber optiğin kuantum özelliklerini ve serbest alan iletim teknolojisini kullanarak gerçekleştirilebilir. Kuantum anahtar değişiminde iletim elektriksel işaretler yerine foton durumları ile fiber optik ağ üzerinden yapılmaktadır. Gönderici tarafında foton üretici cihazlar ile alıcı ve göndericiye ait kristal foton süzgeçlerine ihtiyaç vardır.

Kuantum anahtar dağıtımı geleneksel anahtar dağıtımından çok farklı çalışır çünkü matematiğe dayanmak yerine verileri korumak için doğanın temel yasalarına dayanan bir kuantum sistemini kullanır. Kuantum anahtar değişimi temelde Heisenberg'in belirsizlik ilkesine dayanır. [4]. Belirsizlik ilkesi bir kuantum parçacığının belli ilişkili özelliklerinin (hız ve konum gibi) aynı anda bilinemeyeceğini söyler [4]. Kuantum anahtar değişiminin güvenliği buradan gelir, çünkü araya giren saldırgan foton üzerinde değişikliğe neden olur. Kuantum fiziğinde iletim esnasında verinin bozulması arada bir dinleyici tarafından verinin okunmaya çalışıldığı anlamına gelir.

Kuantum anahtar değişim protokolleri temelde çalışma biçimleri benzer olmasına rağmen fotonların nasıl düzenlendiği ve iletildikleri konularında farklılık gösterirler. Örneğin Ekert protokolünde [7] Heisenberg belirsizlik ilkesi yerine kuantum halleri birbiriyle süper pozisyon durumunda olan iki foton kullanılır, alıcı ve vericiye birer foton gelir ve bu fotonların kuantum halleri birbirlerine ters durumda olduğundan bir taraf diğer taraftaki kuantum durumunu tahmin edebilir, bu şekilde ortak bir kuantum anahtarı elde edilir. Bir diğer protokol olan B92 protokolünde [6] ise iletimden sonra gönderici alıcıya ne zaman bit tespit ettiğini

bildirir fakat kullandığı tabanı açıklamasına gerek yoktur çünkü alıcı fotonu tespit etmişse kullandığı taban göndericinin göndermiş olduğu biti zaten başarılı bir şekilde tanımlar.

2.3.1. BB84 Quantum Anahtar Değişim Protokolü

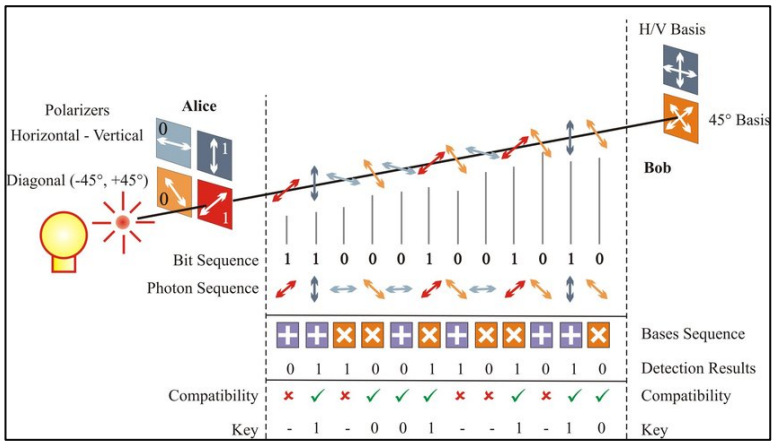
Kuantum şifreleme için ilk protokol olan BB84 bugün hala kullanılmakta olan ilk kuantum şifreleme protokolüdür. 1984 yılında Charles Bennet ve Gilles Brassard tarafından ortaya konmuştur. Daha sonraki yıllarda B92 [6], Ekert [7] ve SARG [8] protokolleri geliştirilmiştir.

BB84 gizli anahtarın güvenli olmayan bir kanal üzerinden güvenli şekilde dağıtımını sağlar. İki yönlü açık ve tek yönlü kuantum kanal olmak üzere iki kanal kullanılır. Temelde iki farklı taban kullanır ve kuantum bir kanal üzerinden iletilen rasgele sıralı dizi (anahtar) oluşturmak için ışığın kutuplaşmasından yararlanır.

BB84 iki taban kullanır, birinci taban kenarsal olarak yatay ve dikey kutuplaşma ve bunlara karşılık gelen 0 ve 90 dereceyi, ikinci taban ise köşegensel olarak 45 ve 135 derecelerini kullanır. Birinci tabanda 0 derece 1'e, 90 derece 0'a eşit, ikinci tabanda ise 45 derece 0'a, 135 derece 1'e eşittir. Gönderici ve alıcıda filtre olarak kullanılan kenarsal ve köşegensel kristal süzgeçler bulunur, iletişim fiber optik ağ üzerinden sağlanır. Alıcı filtrelerden geçen fotonlara ait ölçtüğü sonuçları saklar ancak bunları açıklamaz. Foton iletimi tamamlandıktan sonra alıcı kullandığı filtreleri kimlik doğrulamalı açık bir kanaldan açıklar, gönderici buna karşılık alıcının hangi filtreleri doğru seçtiğini yine aynı kanaldan alıcıya bildirir. Bu aşamada her iki taraf da alıcının ölçümlerinin aynı türde olan durumları saklar, bu aşamada elde edilen veri ham anahtardır ve ileriki adımlarda ortak anahtara dönüşecektir. İletişimi dinleyen üçüncü kişi iletilen fotonun kutuplaşma durumunu bilemediğinden ölçmeye kalktığında foton kutuplanmasının değişimine sebep olacaktır. Bu da aradaki saldırganın tespitini sağlar.

Örnek olarak göndericinin 1101010110 bit dizisini rastgele seçtiği filtrelerle göndermek istediğini varsayalım. Alıcı buna karşın kendisi de + veya x olarak rastgele bir filtre takımı seçer ve çeşitli yönlerde polarize olmuş fotonları elde eder. Alıcı göndericinin göndermiş olduğu bit dizisini ve kullandığı filtreleri bilmediğinden elde ettiği sonuç alıcının göndermiş olduğu veriden farklıdır, ortalama

olarak alıcının elde ettiği verinin yarısı kadarı göndericinin bitleriyle aynıdır. Sonraki aşamada ham anahtarı elde etmek için ortak kullanılan bitlerin belirlenmesi gerekir. Bu adım anahtar eleme aşamasıdır ve göndericinin alıcıya kaçıncı bit için hangi filtreyi seçtiğini kimlik doğrulamalı bir kanaldan söylediği adımdır. Alıcı bu filtrelerden hangilerinin doğru ve yanlış olduğunu iletir, doğru seçilen filtreye karşılık gelen bitler saklanarak ham anahtar elde edilmiş olur. Sonraki adımlarda aradaki saldırganın belirlenmesi için hata oranı tespiti ve gizlilik artırımı adımları uygulanır. 4. bölümde benzetim ortamında bu adımlar gerçek veriler üzerinde detaylı olarak gösterilmiştir.



Şekil 2.2: BB84 iletişimi esnasında foton gönderimi.

Araya giren bir saldırganın iletişimi dinleyip dinlemediğinin belirlenmesi için her iki taraf elde ettiği bit dizileri üzerinde kontrol yaparak hatalı bitleri ve hata oranını belirler. Arada bir dinleme olmuşsa bu ölçum yapmaya çalıştığı anlamına gelir ve bu durum fotonlarda bozulmalara sebep olur. Bu bozulma belirli bir eşik değeri üzerinde ise taraflar iletişimin dinlendiğini ve artık güvenli olmadığını varsayarak iletişimi iptal eder ve ileticimi baştan başlatırlar.

2.3.2. B92 Protokolü

B92 protokolünde [6] iletimden sonra gönderici alıcıya ne zaman bit tespit ettiğini bildirir fakat kullandığı tabanı açıklamasına gerek yoktur çünkü alıcı fotonu tespit etmişse kullandığı taban göndericinin göndermiş olduğu biti zaten başarılı bir

şekilde tanımlar. Bu protokolde kübitler 0 ve 45 derecelik kutuplaşma ile gösterilirler. Alıcının gönderilen fotonları okuma şekli BB84 protokolüyle aynıdır, aynı tabanları kullanır ancak BB84 protokolünden farklı olarak sadece 90 derece ve 135 derece açıya sahip okumaları geçerli sayar.

2.3.3. EPR-Ekert Protokolü

Ekert protokolünde [7] Heisenberg belirsizlik ilkesi [4] yerine süperpozisyon durumundaki iki foton kullanılır. Kullanılan bu fotonların kuantum halleri birbirine ters olduğundan ortak anahtar tarafların birbirlerindeki kuantum hallerini tahmin edebilmesiyle oluşur.

2.3.4. SARG Protokolü

SARG protokolü foton bölme saldırılarına karşı 2004 yılında Scarani ve arkadaşları tarafından öne sürülmüştür [8]. BB84 protokolü ile benzerlik gösterir ancak bitleri kodlamak için filtreler kullanılır. SARG04 protokolü foton numarası bölme (PNS) saldırısına karşı BB84'ten daha sağlamdır. Kuantum anahtar değişimi iletişimi esnasında foton üreteçleri birden fazla aynı kutuplanma durumuna sahip foton üretirler. Bu durum hattı dinleyen saldırganın her kübit için yollanan birden fazla fotondan birini yakalayıp anahtarı elde etmeye çalışmasına yol açabilmektedir. BB84 protokolünün aksine SARG protokolünde gönderici ve alıcı okuma işleminde kullandıkları filtreleri açıklamazlar, bunun yerine gönderici gönderdiği kutuplanma değerini ve bu kutuplaşma değeri ile 45 derece açı yapan başka bir kutulanmayı açıklar. Geçerli okuma olarak okunan bitin ortak anahtara eklenebilmesi alıcının açıklanan kutuplaşma değerlerinden birine ortogonal okuma yapmasıyla sağlanır.

3. KUANTUM ANAHTAR DEĞİŞİM PROTOKOLLERİNE KARŞI YAPILAN SALDIRILAR

Kuantum anahtar değişim protokolünü kullanan ağlar ekstra güvenlik sağlıyor olsalar da bu ağlara karşı geliştirilen birtakım saldırı stratejileri mevcuttur.

3.1. BB84 Kuantum Anahtar Değişim Protokolüne Karşı Yapılan Saldırılar

Bu bolümde ilk öne sürülen ve en çok kullanılan anahtar değişim protokolü olan BB84 kuantum anahtar değişim protokolüne karşı yapılan saldırlar ve alınabilecek önlemler anlatılmıştır.

3.1.1. Foton Numarası Bölme Saldırısı (PNS)

Donanım tabanlı saldırı türüdür. Saldırganın bir sinyal içinde birden fazla foton olması durumunda fotonlardan birini yakalayarak ölçümleme yapması ve bilgi elde etmesine dayanır. Bu sinyal içindeki iki foton tamamen birbiriyle aynıdır. Saldırgan sadece tek fotonu yakalayacağından alıcının ölçümlemesinde fark edilmemesini amaçlar. Bunun için iletişim esnasında fotonların yarısını dinleyerek ölçümlemeye çalışır. Pratikte uygulanması oldukça zor olan PNS saldırısında saldırgan belirleyici bir şekilde sinyalin bir fotonunu böler ve fotonların polarizasyonunu değiştirmeden kuantum hafızasında saklar, kalan fotonların geçmesine izin verir ve alıcıya iletir. Sonuç olarak saldırgan fark edilmeden birden fazla foton içeren tüm sinyallerden gizli anahtar hakkında bilgi edinecektir

PNS saldırılarının önlenmesi için farklı çözümler önerilmiştir. Geliştirilen bir çözüm PNS saldırılarını tespit etmek için yemleme, yani daha düşük foton numarasına sahip rastgele lazer darbeleri gönderilerek yapılmaktadır, böylece saldırgan gerçek sinyaller ile rastgele oluşturulan bu sinyaller arasında ayrım yapamaz [11][12][36]. Bu yöntem hem tekli hem de çoklu foton darbeleri için işe yarar. Foton bölücünün her seferinde tek bir foton gönderilmesi de saldırıyı önleyecektir [10]. SARG protokolünü [8] kullanmak da bu saldırı türüne karşı önlem

olacaktır çünkü bu protokolde gönderici hangi tabanda gönderdiğini açıklamamaktadır.

3.1.2. Engelle / Tekrar Gönder Saldırısı

Yakala/tekrar gönder saldırısında saldırgan göndericinin ve alıcının sahip olduğu araçların (foton yayıcı ve toplayıcı) aynısına sahiptir. Saldırgan kendi cihazlarını gönderici ve alıcı arasına konumlandırır, böylece göndericinin gönderdiği fotonlara alıcıdan önce ulaşır, göndericinin ilettiği fotonu yakalayarak alıcıya kendi ürettiği fotonu gönderir. Bu atak türünde göndericinin oluşturduğu orijinal fotonları hiçbir şekilde ulaşmaz.

3.1.3. Truva Atı Saldırısı

Oldukça yeni bir saldırı stratejisidir. Önceki saldırı türünde olduğu gibi iletişim kanaldaki fotonlardan bilgi elde etmeye çalışmak yerine saldırgan bu saldırı türünde tüm dikkatini gönderici ve alıcının kullandığı cihazlara verir. Saldırgan gönderici veya alıcının cihazına sinyal gönderir (enjekte eder), yansıyan sinyalden göndericinin seçtiği filtre hakkında edinmeye çalışır [13]. Saldırgan foton hakkında bilgiyi bilgi alıcıya ulaşmadan elde ederse basitçe engelle/yeniden gönder saldırısını uygulayabilir. Göndericinin ve alıcının cihazının girişine optik yalıtıcı konulması önlem olarak uygulanabilir. Bu detektör ışımayı sürekli gözetleyerek gelen ışığın yoğunluğu belirli bir seviye üzerinde olduğunda alarm vermesi sağlanacaktır. Diğer bir metot da kuantum ışık detektörlerinin istenmeyen ışık gelişlerine karşı sürekli gözlemlemesini sağlamaktır. Bu saldırı yöntemi ile saldırganın alıcının seçtiği filtreleri %90 olasılıkla belirleyebildiği görülmüştür [37].

3.1.4. Sahte Durum Saldırısı

Vadim Makarov tarafından bulunmuştur. Temelde alıcının sistemindeki kusuru sömürmeye dayanmaktadır. Engelle / tekrar gönder saldırısının yeni ve ileri seviye bir formudur ancak gelen sinyali tekrar oluşturmak yerine kendi türettiği formda özel olarak oluşturduğu sinyali kullanarak tüm iletişimi ele geçirmeyi amaçlar [15]. Böylece sistemdeki foton detektörlerinin karakteristik özelliklerini öğrenebilecektir. Saldırgan alıcının sahip olduğu detektörün aynısına sahiptir ve alıcının yaptığı gibi

yakalama ve ölçüm yapar. Alıcının detektörünü köreltir ve kendi yaptığı ölçümleri almasına zorlar. Bu saldırı turunun en önemli kusuru saldırganın kullandığı detektör ve senkronizasyona çok fazla bağımlı olmasıdır.

3.1.5. Zaman Kaydırma Saldırısı

Tipik bir kuantum anahtar dağıtım sisteminde 2 detektör bulunur. Bunlardan her biri anahtar biti değerine ilişkilendirilmiştir (1 veya 0). Saldırgan giriş ışığına hangi detektörün yanıt verdiğini bilebilirse anahtar bitinin değerini öğrenebilir. Bu nedenle detektörlerin aynı olması önem arz eder. Ancak foton detektörleri gibi karmaşık nesnelerin birebir olarak aynı olması zordur. Bu durum saldırganın zaman parametrelerini inceleyerek sisteme saldırmasına olanak sağlar.

3.1.6. Spektral Saldırısı

Bu saldırı türünde polarizasyon tespiti yerine renk ölçümlemesi yapılır. Fotonlar her bir diyot bir polarizasyon çeşidini oluşturacak şekilde 4 farklı diyot tarafından oluşturulur. Eğer fotonlar 4 farklı lazer foton diyotu tarafından oluşturmuş ise farklı spektral karakterlere sahip olacaktır. Bu spektral karakterlerin analiz edilmesi ile gizli anahtar hakkında birçok bilgiye ulaşılabilir.

3.1.7. Yan Kanal Saldırıları

Saldırgan cihazlar veya kuantum sinyalleriyle doğrudan etkileşime girmek yerine cihazlardan herhangi bir bilgi sızıntısı olup olmadığı ile ilgilenir. Yan kanal analizinde saldırganın amacı kullanılan cihazların yapısı ve işleyişleri hakkında bilgi sahibi olmaya çalışmak ve bu bilgiyi saldırı amaçlı kullanmaktır.

3.2 BB84 Protokolü ile Güvenlik Artırımı

3.2.1. Önerilen Yöntem

Kuantum bilgisayarlar hem geleneksel açık anahtar algoritmaları (RSA, El Gamal gibi) hem de simetrik anahtar algoritmaları (3DES, AES) için önemli bir risk oluşturmaktadır. Günümüzde kötü niyetli kullanıcıların açık anahtarlı iletişimleri

dinleyerek anahtarları depoladığı ve bunları kırmak için kuantum bilgisayar ve işlem gücünü bekledikleri bilinmektedir. Bu da güvenli olarak bildiğimiz günümüzdeki açık anahtarlı iletişim sistemlerinin yakın gelecekte güvensiz hale gelmesi anlamına gelmektedir. İletişimde ortadaki adam saldırısını bertaraf etmek ve dinleme olanağını ortadan kaldırmak gereklidir.

Bankalar ve finansal hizmetleri merkezleri güvenliğin üç ana unsuru olan erişilebilirlik, bütünlük ve gizliliği sağlayabilmek için geleneksel kriptografi metotları kullanılır. Kurumsal ağ içinde veya veri merkezleri arasında bilgi aktarımı için kullanılan yedekleme donanım veya yazılımlarda AES şifrelemesi uygulanır. SWIFT ağı genelinde bankalar arası finansal mesajlaşma, ödeme emirlerini şifreli şekilde transfer etmek için açık anahtar şifreleme yöntemi kullanılır. Veri transferinde kullanılan şifreleme yöntemi geleneksel simetrik anahtar metodudur. Depolanan verilerin hem lokal hem bulut erişimlerinde geleneksel AES şifreleme metodu kullanılır. Çevrimiçi bankacılık, web trafiğini erişimlerinde TLS protokolünü kullanır ve X.509 sertifikaları ile RSA genel anahtarları kullanılarak sunucu kimlik doğrulaması yapılır.

Açık anahtarlı şifrelemede herkese açık olan anahtar gönderici tarafından mesajı mühürlemek ve alıcıya göndermek için kullanılır. Alıcı mesajın doğru kişi tarafından gönderildiğini göndericinin açık anahtarıyla doğrulayabilir. Alıcı mesajı ancak kendi özel anahtarıyla açıp okuyabilir. Açık anahtarlı şifreleme yine dijital imza, SSL gibi teknolojilerde kullanılmaktadır. Ancak açık anahtarlı şifrelemede kullanılan algoritmaların şifreleme yönteminin kuantum bilgisayar ile kırılabildiği ispatlanmıştır. Bu durumda araya giren saldırgan elde ettiği şifreleme anahtarını kuantum bilgisayar yardımıyla çözebilecek, anahtarı tekrar oluşturarak iletilmek istenen bilgilere ulaşabilecektir. Örneğin 1994'te geliştirilen shor algoritması [34] kuantum bilgisayarlarında çok büyük sayıları kolaylıkla asal çarpanlarına ayırabilmektedir. Klasik bir bilgisayarın belirli bir 56 bitlik şifrelemeyi kırması bir gün sürerse kuantum bilgisayarı yalnızca 0,322 milisaniye kadar bir sürede bu şifrelemeyi kırabilir. Benzer şekilde klasik bir bilgisayarın 64 bit şifrelemeyi kırması bir yıl sürerse bir kuantum bilgisayar bunu 7,3 milisaniyede yapar. 2048 bit RSA şifreleme metodu kuantum dönüşümü ile sadece sekiz saat içerisinde kırılabilmektedir. Bu örneklerden görüldüğü üzere hükümet, milli savunma, ordu ve büyük elçilikler gibi kurumların kritik finansal varlıklarının verileri ciddi tehlike

altındadır. Bu nedenle RSA şifrelemeyi kullanan kuruluşlar kuantum dirençli yeni şifreleme algoritmalarına geçmeyi bir an önce değerlendirmelidirler.

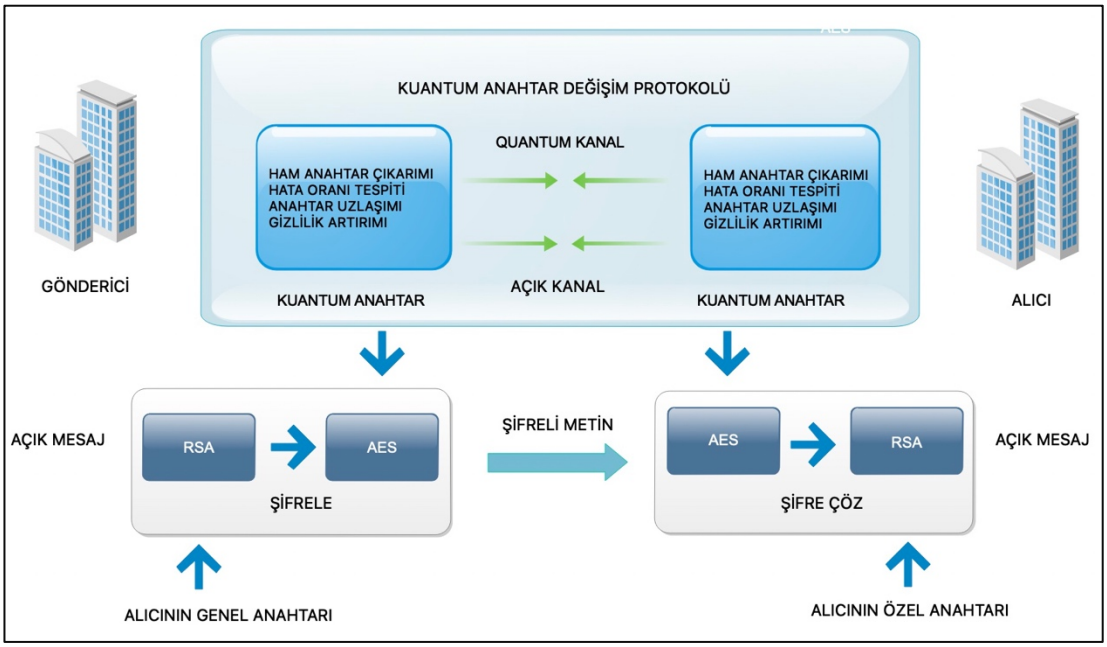
Kriptosistem	Tip	Amaç	Güvenlik Seviyesi	Kuantum Sonrasındaki Güvenlik Seviyesi	Kriptoistemi Kırmak için Gereken Kübit Sayısı*
AES-128	Simetrik	Şifreleme	128-bit	64-bit (Grover alg.)	-
AES-256	Simetrik	Şifreleme	256-bit	128-bit (Grover alg.)	-
SHA-256	-	Özet Fonksiyonu	256-bit	128-bit (Grover alg.)	-
RSA (n-bit)	Asimetrik	Şifreleme İmzalama Anahtar Değişimi	128-bit	0-bit (Shor alg. ile kırıldı)	$2n$
DH/DSA (n-bit)	Asimetrik	İmzalama Anahtar Değişimi	128-bit	0-bit (Shor alg. ile kırıldı)	$2n$
Curve25519 (n-bit)	Asimetrik	Şifreleme İmzalama Anahtar Değişimi	128-bit	0-bit (Shor alg. ile kırıldı)	$6n$
ECDH/ECDSA (n-bit)	Asimetrik	İmzalama Anahtar Değişimi	128-bit	0-bit (Shor alg. ile kırıldı)	$6n$

Şekil 3.1: Kuantum sonrasında kripto sistemlerin güvenlik seviyeleri.

Bu nedenle, kuantum saldırılarına karşı koymak için daha büyük anahtar boyutları kullanılmalıdır. Simetrik şifrelemenin kuantuma dayanıklı olarak kabul edilebilmesi için 256 bitlik bir anahtar uzunluğuna sahip olması gerekir. AES-256 gibi bir şifreleme sistemi, kuantum sonrası bir dünyada AES-128'e eşdeğer olacaktır.

Şekil 3.2: Günümüzde kullanılan açık anahtarlı şifreleme.

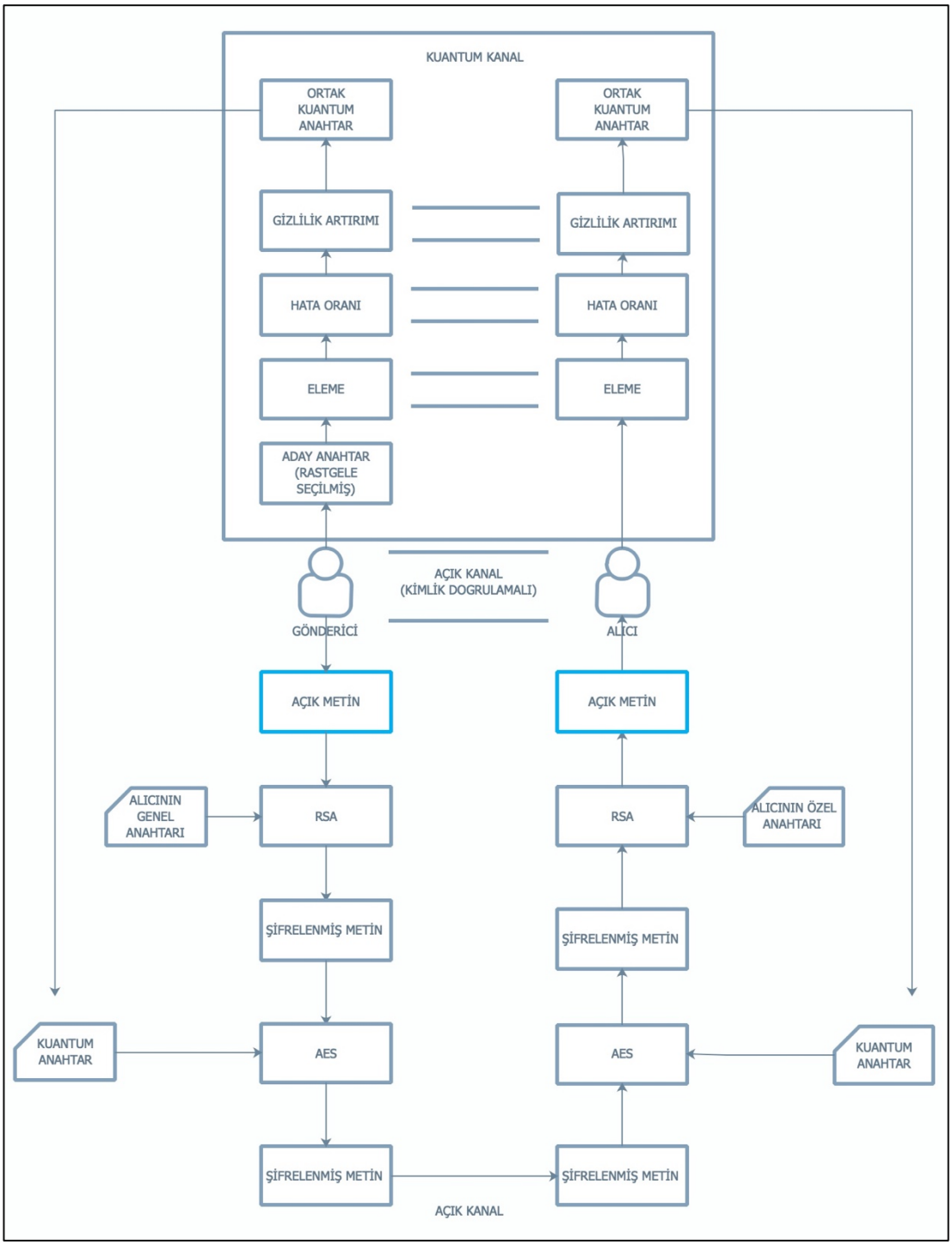
Bu bölümde kuantum anahtar dağıtımı teknolojisinin mevcut iletişim altyapıları ile birleştirilerek günümüzde gizlilik gerektiren birçok iletişim ağının çok daha güvenli hale getirilebileceği tasarlanmıştır. Var olan şifreli iletim yöntemlerine kuantum anahtar değişim protokolü eklenerek kuantum fiziği ile iletişim esnasında araya giren saldırganları belirleyerek 'ortadaki adam' tehdidini tamamen önlemektir. Kuantum anahtar değişim protokolü ile tek kullanımlık anahtar (OTP) oluşturularak her iki tarafın ortak anahtara sahip olması sağlanır. Kuantum kanalı ile iletişim esnasında dinlemeden kaynaklı değişiklikler belirli bir seviyeye ulaştığında iletişim ve gizli anahtar üretimi durdurulur. Güvenliği artırmak için RSA genel anahtarı kullanılarak şifrelenen bir mesaj, kuantum anahtarı kullanılarak AES şifreleme yöntemiyle bir kez daha şifrelenmektedir. Mesajı engellemek için saldırganın hem kuantum anahtarını hem de klasik anahtarı kırması gerekir. Ayrıca oluşturulan anahtarlar en az mesaj kadar uzun olmalı, belirli aralıklarla oluşturulmalı, sadece bir kez kullanılmalı, kullanıldıktan sonra imha edilmelidir. Anahtarın yeniden üretimi yüksek güvenlikli sistemlerde dakikada bir, daha az güvenlik gerektirebilecek sistemlerde günlük olabilir.



Şekil 3.3: Önerilen yöntem tasarımı.

Önerilen yöntem var olan sisteme ek bir güvenlik katmanı oluşturmaktadır. Şifreleme sadece matematiksel yöntemlere değil aynı zamanda kuantum fiziğine

bağlıdır. Kuantum kanal verinin güvenliğini ölçüm yapılmak istendiğinde verinin değişmesi ve düzensiz hale gelmesi olarak ifade edilen Heisenberg'in belirsizlik ilkesi ile yine kuantum fiziğinde verinin kopyasının oluşturulamaması ilkelerine dayandırır [4]. Böylece iletime herhangi bir dinleme veya müdahale doğrudan fark edilerek iletişim iptal edilir.



Şekil 3.4: Önerilen yöntem çalışma şeması.

Kuantum anahtar oluşturma aşamasında kuantum kanal ve açık kanal olmak üzere iki kanal kullanılmaktadır. Fotonların iletildiği ve ölçümlerin yapıldığı aşama kuantum aşamasıdır. Ham anahtar çıkarımı kuantum kanalın kullanıldığı tek adımdır. Diğer kanal da kimlik doğrulamalı açık kanaldır. Alıcı bu kanalda seçtiği filtreleri göndericiye bildirerek hangilerinin doğru olduğunu belirler.

Anahtar eleme, hata oranı tespiti ve gizlilik artırımı bu aşamada uygulanır ve temel amaç aday anahtarda damıtma işlemleri yapılarak anahtar tespitini zorlaştırmaktadır. Eleme adımında iletişimde kaybolan, iletilemeyen fotonlar elenir. Hata tespitinde hatalar belirli bir eşik değerini aştığında iletişimin dinlendiği varsayılır ve iletişim iptal edilerek yenisi başlatılır. Örneğin yakala / tekrar gönder saldırısı %25 hata oranı oluşturur. Bu hata oranı:

$$\text{Hata oranı} = \frac{\text{Toplam hatalı bit sayısı}}{\left(\text{Toplam doğru bit sayısı}\right) + \left(\text{Toplam yanlış bit sayısı}\right)} \tag{3.1}$$

formülü ile hesaplanır. İdeal durumda yani gürültüsüz ve arada saldırgan olmadığı durumda hata oranı 0 olmalıdır. Hata düzeltme kısmında gürültü veya başka nedenlerden oluşan hatalar düzeltilir. Ancak hala saldırganın anahtarın bir kısmını ele geçirmiş olabileceği düşünülerek bir sonraki adım olan gizlilik artırımı adımı uygulanır. Bu aşamada elde edilen anahtardan daha kısa ama daha güvenli anahtar oluşturulur. Burada belirtilen adımlar bir sonraki bölümde benzetim ortamında uygulanarak detaylı olarak analiz edilmiştir.

Rastgele oluşturulan anahtar kuantum kanal aracılığıyla fiber optik ağ üzerinden ulaştırılır. İletim hattında kuantum kanal üzerinde olabilecek herhangi bir dinleme tespit edilmiş ise iletişim iptal edilir. Saldırgan kuantum kanal üzerinden iletilen anahtarı elde edemeyeceğinden açık anahtarlı şifreleme güvenli hale getirilmiş olur. Burada iletişim güvenliğini kuantum fiziğinin kopyalanamama teoreminden almaktadır. Ayrıca yine kuantum seviyesinde iletişim hızıyla saniyede yüzlerce defa yeni tek kullanımlık anahtar oluşturmak mümkündür. Kuantum kanalın eklenmesi iletilen mesajın gizliliğinin ve bütünlüğünün güvenliğini artırmaktır.

Sonraki aşama RSA şifreleme algoritmasının kullanıldığı aşamadır. RSA algoritmasının sağlamlığı büyük tam sayıların kabul edilebilecek zaman dilimi içerisinde kendisini oluşturan asal çarpanlarına ayrılamamasına dayanır. Temelde simetrik şifrelemede kullanılan tek anahtarın aksine genel ve özel anahtar olmak üzere iki anahtar kullanılır. Taraflar şifreyi çözmek için özel anahtarını, mesajı

göndereni doğrulamak için göndericinin genel anahtarını kullanır. İletişimde alıcı genel anahtar şifresi olan (n,e)'yi yayınlar.

- m = Düz metin
- d = Alıcının özel anahtarı
- KA = Kuantum Anahtar
- ASM = Asimetrik Şifrelenmiş Metin
- SSM = Simetrik Şifrelenmiş Metin

olarak şifreleme işlemi

$$\mathrm{ASM} = \mathrm{m}^{\mathrm{e}} \bmod \mathrm{n} \tag{3.2}$$

$$\mathrm{SSM} = \mathrm{AES}\ (\mathrm{ASM}, \mathrm{KA})$$

ile gösterilir. Şifre çözme aşamasında alıcı yukarıdaki adımları tersten uygulayarak açık metni elde eder. Önce AES ile şifrelenmiş veriyi ortak kuantum anahtarı ile çözer. Daha sonra elde ettiği RSA ile şifrelenmiş veriyi kendi özel anahtarıyla çözer. n taban değeri olan modülüs olmak üzere bu adım:

$$\mathrm{ASM} = \mathrm{AES}\ (\mathrm{SSM}, \mathrm{KA}) \tag{3.3}$$

$$\mathrm{m} = \mathrm{ASM}^{\mathrm{d}} \bmod \mathrm{n}$$

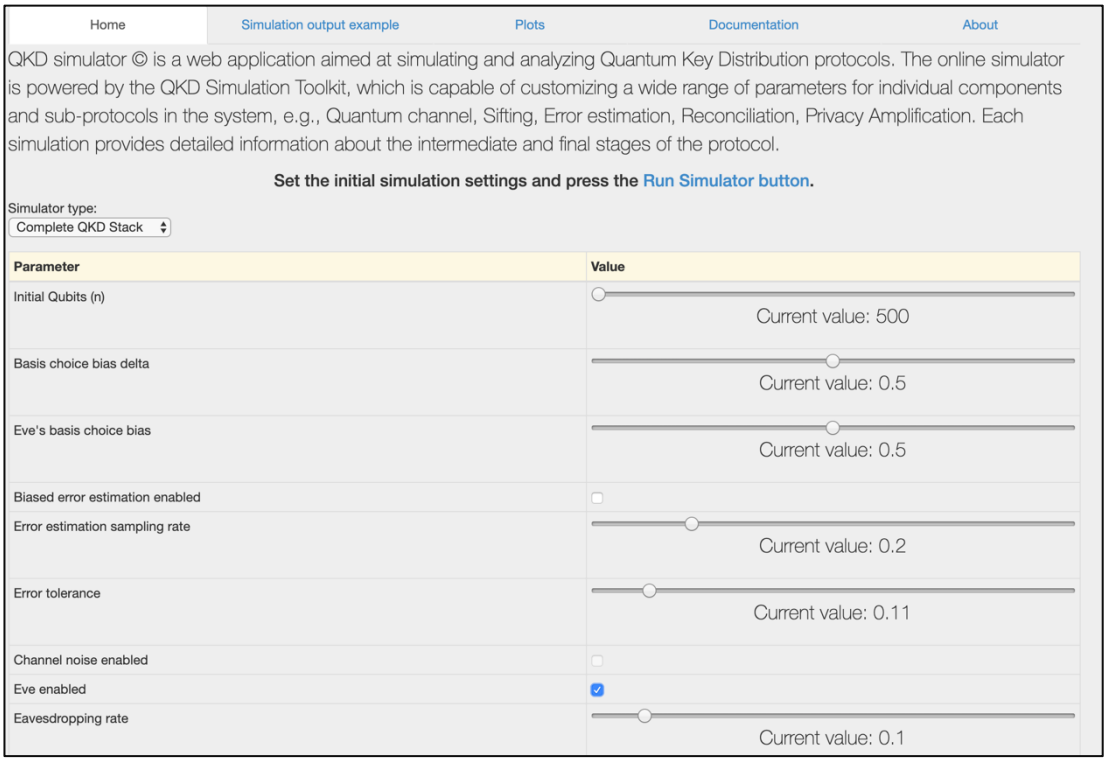
şeklinde belirtilir. Şifreleme adımında alıcının genel anahtarı ile şifrelenmiş veri, oluşturulan ortak kuantum anahtarı ile AES simetrik şifreleme yöntemiyle tekrar şifrelenir. AES şifreleme algoritmasında veriyi şifrelemek ve şifreyi çözmek için aynı anahtar kullanılır. AES için girdi ve çıktı matrisleri her zaman 128 bit olmak zorundadır ancak anahtar uzunluğu 128, 192 veya 256 bit olabilir. Kullanılan bit sayısı AES şifrelemesinin farklı tur sayılarında tamamlanmasını gerektirir. Örneğin 192 bit için 12 turda tamamlanan şifreleme ve şifre çözme işlemi 256 bitlik anahtar için 14 turda tamamlanır.

Benzetim sonuçlarında Tablo 4.4' de görüldüğü üzere en az 128 bitlik bir kuantum anahtar elde etmek için saldırı olma ve olmama ihtimalleri göz önüne alınarak en az 750 kübitlik bir başlangıç verisi kullanılmalıdır.

Bir sonraki bölümde tasarımda yer alan kuantum kanalı üzerinden iletişimde aradaki dinleyicinin tespiti benzetim ortamında detaylı analiz edilmiştir. Kuantum kanalı ile iletim sistemi fiber optik kablolarla 60 mil ile sınırlıdır ancak birden çok kuantum düğümleri oluşturmak suretiyle düğümler arasında bilgi aktarılarak bu sorunun yakın dönemde aşılabileceği düşünülmektedir.

4. DENEYSEL ANALİZ VE DEĞERLENDİRME

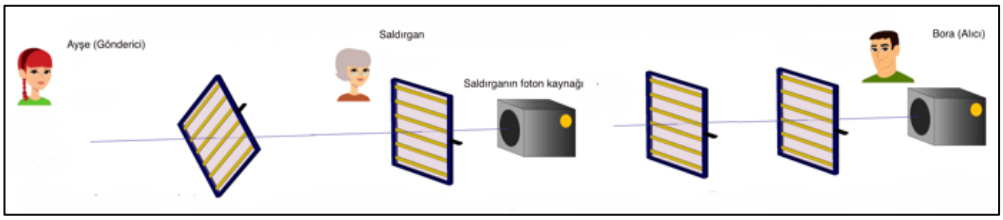
Bu kısımda önceki bölümde önerilen sistemin kuantum anahtar değişimi iletişiminde uygulanan adımları detaylı açıklanmış, QKD Simülatör yazılımıyla [35] gerçekleştirilerek ortadaki adam saldırılarına karşı sistemin güvenliği analiz edilmiştir. QKD Simülatör kuantum anahtar değişim protokollerini analiz etme amaçlı geliştirilmiş web tabanlı bir yazılımdır. Hata tahmini, gizlilik artırımı, bilgi uzlaşımı, eleme gibi birçok özellikte parametre kullanımını desteklemektedir.



Şekil 4.1: BB84 protokolünün QKD Simülatör ile uygulanmasında seçilen konfigürasyon değerleri.

BB84 protokolünde gönderici (Ayşe) rastgele bir tek kullanımlık anahtar seçer ve dört kutuplaşma açısından rastgele birini seçerek gönderir. Alıcı (Bora) gelen fotonların ölçümü için sahip olduğu filtrelerden türlerden biri olarak seçer ölçüm yapar. Alıcı kuantum aktarım tamamlanana kadar ölçüm sonuçlarını gizli tutar, aktarım tamamlandıktan sonra seçmiş olduğu filtreleri açıklar. Ölçüm sonuçlarını kesinlikle açıklamaz. Sonraki aşamada alıcı kendi seçmiş olduğu açıklayarak alıcıya seçtiği ölçüm filtrelerin hangilerinin doğru olduğunu söyler. Alıcı ve göndericinin

ölçümlerinin aynı olduğu durumlar 1 ve 0 bitlerine dönüştürülerek ortak anahtar elde edilir. İletişimin dinlenmesi bazı hatalara neden olacaktır, çünkü saldırganın fotonların polarizasyon türünü bilmeden dinleme yapmak iletişime müdahale anlamına gelmekte ve fotonların polarizasyonunu değiştirecektir. Kuantum anahtar iletişimin önemi bu noktada kendini gösterir, çünkü haberleşen taraflar hata oranı belirli bir eşik değerinin üstündeyse aradaki saldırganı tespit edebilirler.



Şekil 4.3 : Yakala/tekrar gönder saldırısı.

Benzetim ortamında Ayşe ve Bora arasında BB84 protokolü üzerinden gürültüsüz ortamda ortak anahtar oluşturma esnasında saldırganın yakala/tekrar gönder saldırısı yaptığı durum oluşturulmuştur. Bu saldırı türünde saldırgan göndericinin ve alıcının sahip olduğu araçların (foton yayıcı ve toplayıcı) aynısına sahiptir. Saldırgan bu kendi cihazlarını gönderici ve alıcı arasına konumlandırır, böylece göndericinin gönderdiği fotonlara alıcıdan önce ulaşır [14]. Saldırgan bu noktada alıcıdan gelen fotonlar üzerinde ölçümleme yaparak ve sonuçlarına dayanarak yeni oluşturduğu fotonları alıcıya gönderir. Oluşan hata oranının belirli bir eşik değerini aşması durumunda arada saldırgan olduğu varsayılarak iletişim iptal edilir. Benzetim aşağıdaki başlangıç değerleriyle çalıştırılmıştır.

Tablo 4.1: Benzetim başlangıç parametreleri.

Başlangıç kübit sayısı	500
Temel seçim yakınsaması	0.5
Saldırgan seçim yakınsaması	0.5
Sapmalı hata tahmini	Yok
Hata tahmini örnekleme oranı	0.2
Hata toleransı	0.11
Gürültü	Yok
Saldırgan	Var
Dinleme oranı	0.1

İlk aşamada gürültüsüz bir ortamda arada dinleyici olması durumunda 500 kübit için her adım incelenmiş, ikinci bölümde 500,550…900 olarak farklı başlangıç kübit değerleri ile sonuç anahtar uzunluğu değerleri ve hata oranı analiz edilmiştir.

BB84 protokolünde anahtar değişimi açık ve kuantum olmak üzere iki kanaldan yapılmaktadır. İletim esnasında ham anahtar çıkarımı, hata tahmini, güvenlik artırımı gibi ek adımlar uygulanmaktadır. Benzetimin çalışması esnasında bu adımlar aşağıda detaylı anlatılmıştır.

Aşama 1: BB84 Kuantum Kanal Üzerinden İletim

Ayşe 500 kübitlik bir dizi hazırlar ve bunları kuantum kanalı üzerinden Bora'ya gönderir. Aynı zamanda her bir kübit icin doğrusal polarizasyon (yatay / 0 derece ve dikey / 90 derece) veya çapraz polarizasyon (+45 derece ve -45 derece) için rastgele bir polarizasyon filtresi seçer. Daha sonra yatay ve dikey kübit durumlarını | 0> ve | 1>, +45 derece ve -45 derece | +> ve | -> durumlarıyla sırasıyla eşler.

Bu adımda Ayşe, 0.5 temel seçim eğilimi ile Bora'ya 500 kübit göndermiştir. Bu esnada saldırgan kuantum kanalı üzerinde 0,1 oranında ve temel seçim eğilimi 0,5 olarak kuantum kanalını dinlemektedir. Saldırgan kübitleri keserek iki filtreden birinde rastgele ölçer ve böylece orijinalleri yok eder ve daha sonra ölçümlerine ve temel seçimlerine karşılık gelen yeni bir kübit grubunu Bora'ya gönderir (Yakala/tekrar gönder saldırısı). Saldırgan doğru filtreyi ortalama sadece % 50 olarak doğru bildiğinden bitlerinin yaklaşık 1/4'ü Ayşe'den farklı olacaktır.

Aşama 2.1: Eleme

Bora, klasik bir kanalda başarılı bir şekilde ölçmeyi başardığı kübitleri duyurur. Ayşe ve Bora daha sonra kullandıkları filtreleri açıklar. Polarizasyon filtreleri ortalama zamanın yaklaşık % 50'si eşleştiğinde, her ikisi de karşılık gelen bitlerini kişisel anahtarlarına ekler. Kanal gürültüsünün olmaması durumunda kulak misafiri olmadıkça iki anahtar aynı olmalıdır. Kullanılan parametrelere göre eleme aşaması 500 aktarılmış kübit ile başlamış ve elde edilen bit dizisi 260 bite indirilmiştir. Ayşe ve Bora'nın seçilen ölçüm tabanlarının 0,52'si eşleşir. Seçtikleri filtrelerin 0,48'i eşleşmemektedir. İki tarafın ölçülen kübitlerinin 0.746'sı eleme öncesi eşleşir ve 0.254'ü eşleşmez. İki tarafın ölçülen kübitlerinin 0.9615'i eleme sonrasında eşleşir ve 0.0385 tanesi eşleşmez.

Aşama 2.2: Eleme Aşaması Kimlik Doğrulaması - Linear Feedback Shift Register (LFSR)

Ayşe ve Bora, LFSR evrensel hash şemasını ve kimlik doğrulama için karşılıklı olarak paylaşılan bir gizli anahtarı kullanarak temel değişim mesajlarını doğrular. Eleme aşamasında 3 mesaj doğrulanır. Bora, Ayşe'yi başarılı bir şekilde ölçmeyi başardığı kübitlerden haberdar eder ve mesajına bir kimlik doğrulama etiketi ekler. Anahtar açısından kimlik doğrulama maliyeti 64'tür. Bora, kübitleri ölçmek için seçtiği filtreleri Ayşe'ye bildirir ve mesajına bir kimlik doğrulama etiketi ekler. Ayşe, Bora'yı kübitleri hazırlamak için seçtiği filtrelerden haberdar eder ve mesajına bir kimlik doğrulama etiketi ekler.

Aşama 3.1: Uzlaşma / Hata Oranı Tespiti

Ayşe ve Bora hata düzeltmesine devam edip etmeyeceklerini veya protokolü önceden tanımlanmış bir hata tolerans eşiğine (genellikle yaklaşık %11) dayanarak iptal edip etmeyeceklerini belirlemek için elenmiş anahtarlarındaki hata oranı tespiti yapar.

Aşama 3.2: Uzlaşma / Kademeli Hata Düzeltme

Ayse ve Bora elenmiş bit dizelerindeki hatalı bitleri bulmak ve düzeltmek için genel kanalda Cascade adlı etkileşimli bir hata düzeltme şeması uygular. Art arda sıralı hataları düzeltmek için işlem 5 defa uygulanmıştır. 7 hatalı bit tespit edilmiş ve düzeltilmiştir. Hataları tespit etmek ve düzeltmek için 57 bit sızdırılmıştır.

Aşama 4: Hata Düzeltme Onayı ve Kimlik Doğrulaması

Bu adımda Ayşe ve Bora hata düzeltmeli anahtarlarının karma değerini karşılıklı olarak önceden paylaşılan gizli anahtarlarını kullanarak ve ilgili özetlerini karşılaştırarak hata düzeltme aşamasını doğrular. Kimlik doğrulaması için 64 bit anahtar (önceden paylaşılmış gizli anahtar) kullanılmıştır. Kimlik doğrulama için Linear Feedback Shift Register (LFSR) evrensel karma şeması kullanılmıştır.

Aşama 5: Gizlilik Artırımı

Bu adımda amaç saldırganın anahtarda tespit edebildiği bit sayısını en aza indirmektir. Ayşe ve Bora, genel bilgi sızıntısını hesaplar ve saldırganın kanala kulak misafiri olacak şekilde elde ettiği bilgiyi azaltmak/en aza indirmek için bir dizi gizlilik yükseltme protokolü çalıştırır. Bunu yerel olarak Toeplitz matrislerine

dayanan evrensel bir karma şema uygulayarak yaparlar. Ayrıca bir güvenlik parametresi tanımlayabilirler. Gizlilik artırımı çalıştırmadan önceki anahtar uzunluk 208 bit, son anahtar uzunluğu 94 bit olmaktadır.

Benzetim 500, 550, 600, …, 900 olarak 9 kez farklı başlangıç kübit değerleri ile çalıştırılarak gürültüsüz ortamda arada saldırgan olması durumunda sonuç anahtar uzunluğu değerleri ve hata oranı analiz edilmiştir. Sabit 500 başlangıç kübit sayısı için ulaşılan sonuç verileri Tablo 4.2' de görülmektedir.

Tablo 4.2: Benzetim sonuçları.

Başlangıç kübit sayısı	500
Sonuç anahtar uzunluğu	108
Dinleme aktif	Evet
Dinleme oranı	0.1
Gönderici/alıcı temel seçim yanlılığı	0.5
Saldırgan temel seçim yanlılığı	0.5
Hata düzeltmesinden önce ham anahtar uyuşmazlığı	0.0191
Hata düzeltmesinden sonra ham anahtar uyuşmazlığı	0
Bilgi kaçağı (toplam bit)	82
Kimlik doğrulama için genel anahtar maliyeti	256
Hata düzeltmeden önceki anahtar uzunluğu	210
Bit hatası olasılığı	0.0238
Hata düzeltme sırasında sızdırılan bit sayısı	50
Sızıntı için Shannon sınırı	35
Güvenlik parametresi	20

Gürültüsüz ortamda arada dinleyici bulunması durumunda farklı başlangıç kübit sayısı için hata oranları Tablo 4.3' de görülebilir.

Tablo 4.3: Saldırı durumunda hata oranı.

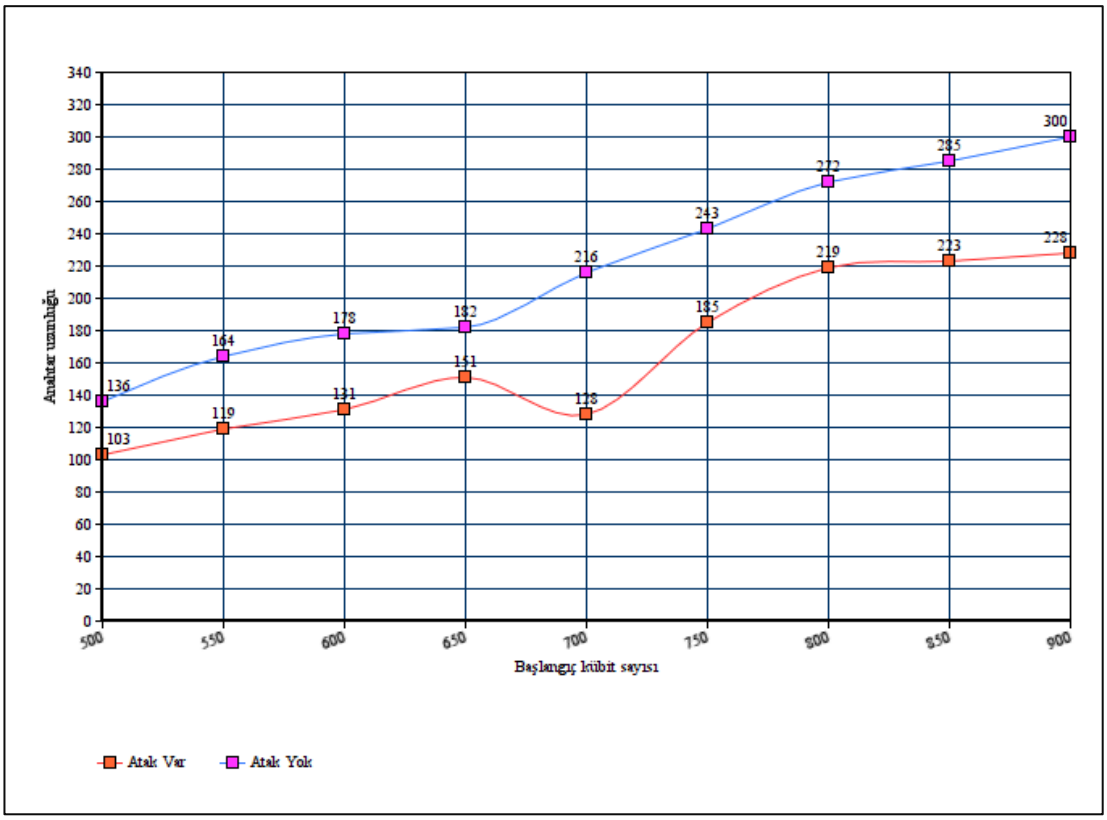
Başlangıç kübit sayısı	Hata oranı
500	0.0741
550	0.0392
600	0.0345
650	0.0161
700	0.0758
750	0.0282
800	0.0256
850	0.012
900	0.0549

Saldırı olması durumunda ortalama hata oranının belirgin seviyede olduğu görülmektedir. Benzetimde dinleme oranı başlangıç parametresi 0.1'dir. Hata oranının belirli bir değerinde olması iletimin dinlendiğini ve artık güvenilir olmadığını göstermektedir. Sonuç değerlerinden görüldüğü üzere yakala/tekrar gönder saldırısının belirlenmesi en etkili şekilde anahtardan hata oranı tespitiyle gerçekleştirilebileceği sonucu ortaya çıkmaktadır. Başlangıç dinleme oranı artırıldığında sonuç hata oranı verileri de artma göstermektedir.

Tablo 4.4: Başlangıç konfigürasyonu sabit tutularak saldırı ve saldırı olmadığı durumda anahtar uzunlukları.

Başlangıç kübit sayısı	Anahtar uzunluğu (Saldırı var)	Anahtar uzunluğu (Saldırı yok)
500	103	136
550	119	164
600	131	178
650	151	182
700	128	216
750	185	243
800	219	272
850	223	285
900	228	300

Tablo 4.4’ de görüldüğü üzere saldırı olması durumunda elde edilen anahtar uzunluğu saldırı olmama durumuna göre çok daha düşük olmaktadır. Başlangıç kübit sayısı ile sonuçta elde edilen anahtar uzunluğu arasında direkt ilişki görülmemekte, genel olarak gönderilen başlangıç kübit sayısının %20 - %25’i civarında anahtar uzunluğu elde edilmektedir. Arada saldırı bulunması bu oranı düşürmektedir.



Şekil 4.4 : Sonuç anahtar uzunluklarının karşılaştırılması.

5. SONUÇ VE ÖNERİLER

Kuantum mekaniğinin prensiplerinin ve kuantum kopyalanamama teoreminin anahtar dağıtımına uyarlanması kötü niyetli saldırganların anahtara habersiz bir şekilde erişemeyeceği sonucunu vermektedir. Kuantum anahtar değişim protokollerine karşı birtakım saldırılar mevcuttur, ancak bu saldırıları pratikte uygulamak oldukça zordur. Kuantum bilgisayarlarının her geçen gün gelişmesiyle finans ve ödeme sistemleri güvenlik omurgası acilen kuantum dönüşümüne girmelidir. Bunun yanında yakın gelecekte sağlık sistemleri, devletler arası yazışmalar, silahlı kuvvetler gibi yüksek güvenlik gerektiren iletişim sistemlerinin güvenliği kuantum protokolleriyle güçlendirilmelidir. Geleneksel güvenlik, şifreleme metodolojileri ve protokollerinin yakın gelecekte etkisiz hale gelebileceği gerçeği unutulmamalıdır.

Kuantum anahtar dağıtımı cihazları henüz ticari olarak yaygınlaşmamakla birlikte kuantum teknolojilerinin gelişmesi ile birlikte bu tez kapsamında üzerinde çalışılmış olan konu ve yöntemin önemi daha da artmış olacaktır. Kuantum anahtar değişiminin en önemli sınırlandırmalarından biri uzak mesafeleri günümüz koşullarında desteklememesidir. Ancak ileride uydu haberleşmelerinin gelişmesiyle bu kısıtlamanın aşılacağı öngörülmektedir. Tezde önerilen hibrit yöntem online bankacılık, dijital imzalar, veri gizleme, bankalar arası iletişim, nesnelerin interneti, online seçim sistemlerinde ve üst düzey güvenlik gerektiren sistemlerde uygulanabilecektir. Kuantum iletim teknolojilerinin gelişmesiyle telefon, tablet gibi cihazların, bankamatiklerin kuantum iletişim protokollerini desteklemesi ile birlikte kuantum anahtar değişimi teknolojisi ile gelecekte iletişimde oldukça güçlü güvenlik sağlanacağı öngörülmektedir.

KAYNAKLAR

[1] Bennett C. H., Brassard G., (1984), “Quantum Cryptography: Public Key Distribution and Coin Tossing”, Theoretical Computer Science, Vol. 560 (Part 1), 2014, 7-11.

[2] Wootters W. K., Zurek W., (1982), “A Single Quantum State Can Not Be Cloned”, Nature 299, 802–803.

[3] Nielsen, M. A., Chuang, I. L. (2000), “Quantum Computation and Quantum Information“ , Cambridge University Press.

[4] Heisenberg, W., (1927), “About the descriptive content of quantum theoretical kinematics and mechanics“, Z. Physik, 43, 172-198.

[5] Gisin, N., Ribordy, G., Tittel, W. & Zbinden, H., (2002), “Quantum cryptography“, Rev. Mod. Phys., 4, 145–195.

[6] Bennett C.H., (1992), “Quantum cryptography using any two nonorthogonal states“, Phys. Rev. Lett., 68 (21), 3121-3124.

[7] Ekert A.K., (1991), "Quantum cryptography based on Bell's theorem", Physical Review Letters, 67 (6), 661–663.

[8] Scarani V., Acín A., Ribordy G., Gisin N., (2004), "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations", Physical Review Letters. 92 (5), 057901.

[9] Brassard G., Lütkenhaus N., Mor T., Sanders B. C. (2000), "Limitations on Practical Quantum Cryptography". Physical Review Letters", American Physical Society (APS), 85 (6), 1330–1333.

[10] Intallura, P. & Ward, M. & Karimov, Otabek & Yuan, Zhiliang & See, P. & Shields, A. & Atkinson, P. & Ritchie, David, (2007), "Quantum key distribution using a triggered quantum dot source emitting near 1.3μm". Applied Physics Letters. 91 (16), 161103.

[11] Scarani V, Acín A, Ribordy G, Gisin N, (2004), "Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations", Phys. Rev. Lett. 92, 057901.

[12] Brassard G., Lutkenhaus N., Mor T., Sanders B. C. (2000), "Security aspects of practical quantum cryptography", In Proceedings of the 19th international conference on Theory and application of cryptographic techniques (EUROCRYPT'00), Springer-Verlag, Berlin, Heidelberg, 289–299.

[13] Jain N., Anisimova E., Khan I., Makarov V., Marquardt C., Leuchs G., (2014), "Trojan-horse attacks threaten the security of practical quantum cryptography", New Journal of Physics, 16 (12), 123030.

[14] Wang X., (2005), "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography". Physical Review Letters, 94 (23), 230503.

[15] Makarov V., Hjelme D. R., (2005), "Faked states attack on quantum cryptosystems", Journal of Modern Optics, 52, 691-705.

[16] Gidney C., Eker M. (2019), “How to factor 2048 bit RSA integers in 8 hours using 20 million noisy qubits”, arXiv:1905.09749v2.

[17] Murdopo A., Ioanna T., Stylianou M., (2011), "Quantum Cryptography and Possible Attacks", SSI Project Report, Universitat Polite`cnica de Catalunya.

[18] Makarov V., (2007), "Quantum cryptography and quantum cryptanalysis", Doctoral Thesis, Norwegian University of Science and Technology.

[19] Lütkenhaus N., Jahma M., (2002), "Quantum key distribution with realistic states: photon-number statistics in the photon-number splitting attack", New Journal of Physics, 4, 44-44.

[20] Lucamarini M., Shields A., Alléaume R., Chunnilall C., Pietro Degiovanni I., Gramegna M., Hasekioglu A., Huttner B., Kumar R., Lord A., Lütkenhaus N., Makarov V., Martin V., Mink A., Peev M., Sasaki M., Sinclair A., Spiller T., Ward M., White C., Yuan Z., (2018) "Implementation Security of Quantum Cryptography Introduction, challenges, solutions", ETSI White Paper, 27.

[21] Kohnle A., Rizzoli A., (2017), "Interactive simulations for quantum key distribution", European Journal of Physics, 38, 035403.

[22] Jain .N, Stiller B., Khan I., Elser D., Marquardt C., Leuchs G., (2016), "Attacks on practical quantum key distribution systems (and how to prevent them)", Contemporary Physics, 57, 336-387.

[23] Mubashir M., (2011), "A Taxonomy of Attacks on Quantum Key Distribution", International Journal of Latest Trends in Computing, 2 (3).

[24] Aggarwal R., Sharma H., Gupta D., (2011), "Analysis of Various Attacks over BB84 Quantum Key Distribution Protocol", International Journal of Computer Applications, 20 (8), 0975 – 8887.

[25] Bouwmeester D., Ekert A., Zeilinger A. , (2010), "The Physics of Quantum Information: Quantum Cryptography, Quantum Teleportation, Quantum Computation", Springer Publishing Company.

[26] Mehić M., (2017), "Using Quantum Key Distribution for Securing Real-Time Applications", Doctoral Thesis, Technical University of Ostrava.

[27] Elliott C., Pearson D., Troxel G., ((2003), "Quantum Cryptography in Practice", In Proceedings of the Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications (SIGCOMM'03), 227.

[28] Gisin N., Fasel S., Kraus B., Zbinden H., Ribordy G., (2006), "Trojan-horse attacks on quantum-key-distribution systems", Physical Review A, 73 (2).

[29] Zeng G., "A simple eavesdropping strategy of BB84 protocol", XiDian University, arXiv:quant-ph/9812064.

[30] Zhou T., Shen J., Li X., Wang C., Shen J., (2018), "Quantum Cryptography for the Future Internet and the Security Analysis", Hindawi Security and Communication Networks Volume 2018, Article ID 8214619.

[31] Wang S., Rohde M., Ali A., (2020), "Quantum Cryptography and Simulation: Tools and Techniques", ICCSP 2020.

[32] Hughes R. J., Alde D. M., Dyer P., Luther G. G., Morgan G. L., Schauer M., (1995), "Quantum Cryptography", Contemporary Physics, 36 (3), 149-163.

[33] Zeng G., Wang X., (1999), "Quantum key distribution with authentication", arXiv:quant-ph/9812022.

[34] Shor P.W., (1994), "Algorithms for quantum computation: discrete logarithms and factoring". Proceedings 35th Annual Symposium on Foundations of CS, 124–134.

[35] Web 1, (2020), https://www.qkdsimulator.com, (Erişim Tarihi: 27/11/2020).

[36] Lo H., Ma X., Chen K., (2005), "Decoy state quantum key distribution", Physical Review Letters, 94 (23), 230504.

[37] Jain N., Stiller B., Khan I., Makarov V., Marquardt C. Leuchs G., (2015), "Risk Analysis of Trojan-Horse Attacks on Practical Quantum Key Distribution Systems", IEEE Journal of Selected Topics in Quantum Electronics, 21 (3), 168-177.

[38] Abushgra A., Elleithy K., "Security of Quantum Key Distribution", (2015), 2015 ASEE Northeast Section Conference, ABD.

[39] Sağıroğlu Ş., Bayındır R., Bilge Y., Bensghır T. K., Akleylek S., Sakallı. M. T., Cenk M., Doğru İ. A., Dörterler M., Efe A., Vural Y., Tür M. R., Kaya M. B., Tekerek A., Vadi S., Akın M., Seyhan K., Soysaldı M., Canbek G., Tombul H., Tunçkanat M., (2019), "Siber Güvenlik ve Savunma: Problemler ve Çözümler", Bilgi Güvenliği Derneği Siber Güvenlik ve Savunma Kitap Serisi, 2, 140-141.

[40] Web 2, (2020), https://tr.wikipedia.org/wiki/Kuantum_kriptografi, (Erişim Tarihi: 25/11/2020).

[41] Web 3, (2020), https://bilimgenc.tubitak.gov.tr/makale/kubit-turleri, (Erişim Tarihi: 04/12/2020).

ÖZGEÇMİŞ

İlker Burak ADIYAMAN 1979 yılında Bursa'da doğdu. Selçuk Üniversitesi Bilgisayar Mühendisliği Bölümünden 2005 yılında mezun olduktan sonra Bursa ve İstanbul'da birçok firmada çeşitli yazılım geliştirme projelerinde görev aldı. 2010 – 2017 yılları arasında Los Angeles ve San Francisco'da çeşitli firmalarda kıdemli yazılım geliştirici olarak çalıştı. Halen yurtiçi ve yurtdışındaki çeşitli firmalara bilgi güvenliği ve yazılım geliştirme konularında destek vermektedir.

EKLER

Ek A: Tez Çalışması Kapsamında Yapılan Yayınlar

İlker Burak Adıyaman, İbrahim Soğukpınar, (2020), "Simulation of BB84 Quantum Key Exchange Protocol and Attack Analysis", Computer Science and Engineering (UBMK), 2020 International Conference on, IEEE, 2020.