T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KUANTUM ŞİFRELEME

HÜSNÜ KARA

YÜKSEK LİSANS TEZİ
FİZİK ANABİLİM DALI

DANIŞMAN
PROF. DR. ZEYNEL YALÇIN

İSTANBUL, 2013

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

KUANTUM ŞİFRELEME

Hüsnü KARA tarafından hazırlanan tez çalışması 19.06.2013 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Fizik Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Prof. Dr. Zeynel YALÇIN

Yıldız Teknik Üniversitesi

Jüri Üyeleri

Prof. Dr. Zeynel YALÇIN

Yıldız Teknik Üniversitesi

Doç. Dr. Kemal ÖZDOĞAN

Yıldız Teknik Üniversitesi

Yrd. Doç. Dr. Vedat ŞİAP

Yıldız Teknik Üniversitesi

ÖNSÖZ

Yüksek lisans eğitimim boyunca bilgi ve deneyimlerinden yararlandığım, güvenini ve desteğini bana her zaman hissettiren değerli danışman hocam Sayın Prof. Dr. Zeynel YALÇIN'a samimi teşekkürlerimi bildiririm.

Yüksek lisans eğitimim sırasında gösterdikleri her türlü destek ve yardımlarından dolayı değerli hocalarım Sayın Prof. Dr. İrfan ŞİAP, Sayın Prof. Dr. Orhan İÇELLİ, Sayın Doç. Dr. Kemal ÖZDOĞAN'a şükranlarımı sunarım.

Değerli arkadaşlarım Kenan YILDIRIM, Mehmet Emin KÖROĞLU ve Mustafa SARI'ya desteklerinden dolayı teşekkür ederim.

Ayrıca, Lisans ve Yüksek Lisans öğrenimim boyunca karşılaştığım zorlukları aşmamda maddi ve manevi yardımlarını esirgemeyen değerli aileme teşekkürlerimi sunarım.

Haziran, 2013

Hüsnü KARA

İÇİNDEKİLER

Sayfa

SİMGE LİSTESİ

C	Karmaşık sayılar kümesi
H	Hilbert uzayı
$\left\| \right\rangle$	Ket vektörü
$\left\langle \right\|$	Bra vektörü
$\sum$	Toplam sembolü
$\otimes$	Tensör çarpımı
ε	İletişim kanalındaki gürültü
δ	Herhangi bir sayı

KISALTMA LİSTESİ

IBM	International Business Machines
CCD	Charge-Coupled Devices
EPR	Einstein-Podolsky-Rozen
RSA	Rivest-Shamir-Adleman Şifreleme Sistemi

ŞEKİL LİSTESİ

Sayfa

ÖZET

KUANTUM ŞİFRELEME

Hüsnü KARA

Fizik Anabilim Dalı

Yüksek Lisans Tezi

Tez Danışmanı: Prof. Dr. Zeynel YALÇIN

Kuantum fiziğinin doğuşundan sonra fizikçiler ve diğer bilim insanları onun büyüleyici doğasından etkilenmiştir. Bunun sonucunda kuantum fiziğinin bilim dünyasına kazandırdığı temel düşünceler fiziksel sistemlerde uygulanmaya başlanmıştır. Öte yandan, bir kısım bilim insanları da iletişim teknolojisinde bilgi iletimi için foton ve benzeri bazı kuantum nesnelerinin kullanımını tasarlamışlardır. Bu düşüncenin kullanılmasıyla bilgi iletişim yöntemlerinde çok daha güvenli iletişim sağlanmaktadır.

Günümüzde bilgi iletişim güvenliği son derece önem kazanmıştır ve önemi her geçen gün artmaktadır. Bu nedenle kuantum şifreleme, kuantum bilgi teorisindeki en önemli alt dallardan biri olmuştur.

Bu tez çalışmasında, birinci bölüm literatür özeti, tezin amacı ve hipotez alanlarını içermektedir. İkinci bölümde kuantum şifreleme için gerekli olan kuantum bilgi, ışığın ve fotonun kutuplanması olayları, kuantum mekaniğinin bazı prensipleri ve kuantum kopyalanamama teoremi verilmiştir. Üçüncü bölümde ise simetrik, asimetrik şifre

sistemleri ve bu alanda temel teşkil eden üç kuantum anahtar dağılım protokolü sunulmuştur.

Anahtar Kelimeler: Kuantum nesneleri, Kutuplanma, Bilgi iletişimi, İletişim güvenliği, Kuantum kopyalanamama teoremi

ABSTRACT

QUANTUM ENCRYPTION

Hüsnü KARA

Department of Physics

MSc. Thesis

Advisor: Prof. Dr. Zeynel YALÇIN

Since quantum physics came into the world, physicists and other scientists have impressed by its magnificent nature. As a result of it, fundamental concepts which belong to quantum physics were started to be practiced to physical systems. On the other hand, some scientists have planned to use photon and some similar quantum objects for information transmission in the communication technology. Because of this concept, in the methods of information communication, secure communication is provided more than before.

Nowadays, communication security has acquired great attention and its prominence has increased day by day. For this reason, quantum encryption has become one of the most important branches in the quantum information theory.

In this thesis, first chapter contains literature abstract, aim and hypothesis of the thesis. In the second chapter, quantum information, polarization of light and photon,

some principles of quantum mechanics and quantum no-cloning theorem which are necessary for quantum encryption are given. Finally, in the third chapter, symmetrical and asymmetrical cryptosystems and three quantum key distribution protocols which are basic in this field are presented.

Key words: Quantum objects, Polarization, Information communication, Communication security, Quantum no-cloning theorem.

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

Kuantum şifreleme düşüncesi ilk defa 1970'lerde Montreal Üniversitesi'nden Gilles Brassard ve IBM'den Charles H. Benett ve Stephen Wiesner tarafından önerilmiştir [1]. Kuantum şifreleme için kullanılmakta olan çok sayıda protokol vardır [1-10]. Bu çalışmada, kuantum şifreleme alanında temel teşkil eden üç protokole değinilecektir. Kuantum şifreleme için ilk protokol olan BB84 protokolü [11] 1984'te Charles H. Benett ve Gilles Brassard tarafından ileri sürülmüştür. Sonrasında sırasıyla, 1991'de Oxford Üniversitesi'nden Arthur Ekert tarafından EPR protokolü [12], 1992'de ise Charles H. Benett tarafından B92 protokolü [13] önerilmiştir.

1.2 Tezin Amacı

Kuantum şifrelemenin bilgi teknolojisindeki yerinin tayini, temel öğelerinin incelenmesi, bilgi güvenliği açısından öneminin vurgulanması ve kuantum anahtar dağılım protokollerinin kuantum şifrelemedeki yerinin tespit edilmesidir. Kuantum şifreleme ve klasik şifreleme arasındaki temel farkların ortaya konulmasıdır.

1.3 Hipotez

Kuantum fiziğinin özellikleri kullanılarak bilginin işlenmesi, şifrelenmesi ve iletilmesi klasik fizik aracılığıyla yapılanlara göre çok daha güvenlidir. Klasik şifrelemede anahtar iletimi esnasında bilgi hırsızlığı farkedilemezken, kuantum şifrelemede ise bilgi hırsızlığı farkedilebilmektedir [14].

BÖLÜM 2

KUANTUM BİLGİNİN TEMELLERİ

Kuantum bilgi kavramı bilginin işlenmesi, depolanması ve iletilmesi için kuantum fiziğinin özelliklerinin kullanımıyla ilgilidir [14]. Kuantum bilgi teorisi başlangıçta temel düşüncelerini kuantum mekaniği, bilgisayar bilimi, bilgi teorisi ve şifreleme alanlarından alarak bu ayrı araştırma alanlarının kesişiminde doğmuştur [15]. Kuantum bilgi teorisinin amacı; bilgiyi işleme, depolama ve iletmek için kuantum mekanik sistemlerin nasıl kullanılabileceğini çalışmaktır. Bu bölüm altı kesimden oluşmaktadır. Bu kesimlerde temel kaynak olarak [14,15] nolu kaynaklar kullanılmıştır.

2.1 Kuantum Bit

Bit, klasik bilginin temel kavramıdır ve genellikle 0 ve 1 ikili dijiti gibi iki mümkün değer alabilen bir değişken olarak tanımlanır. Kuantum bilgi teorisi de benzer bir kavram üzerine inşa edilir: Kuantum bit veya kısaca kubit. Bir kubit karmaşık Hilbert uzayında tanımlanmış iki seviyeli bir kuantum sistemdir.

Bu uzayda, normalize edilmiş ve birbirine dik vektörlerin bir çifti şöyle seçilebilir:

$$|0\rangle = \begin{bmatrix} 1 \\ 0 \end{bmatrix} \; ; \; |1\rangle = \begin{bmatrix} 0 \\ 1 \end{bmatrix}. \tag{2.1}$$

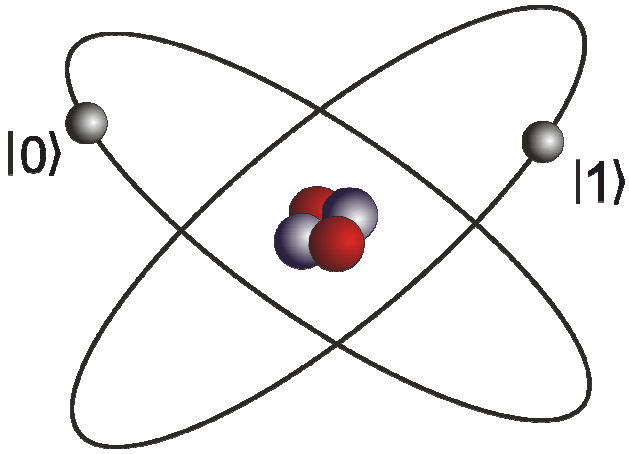
Denklem (2.1) ile verilen iki kuantum durumu iki seviyeli bir kuantum sistemde hesaplama yapmak için bir baz oluşturur ve klasik bitin 0 ve 1 değerlerine karşılık gelir. Üst üste binme ilkesinden, bir tek kubitin bir $|\Psi\rangle$ durumu, bu baz vektörlerinin bir lineer bileşimi olarak yazılabilir:

$$|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle \qquad \alpha, \beta \in C\,. \tag{2.2}$$

Burada α ve β karmaşık genlikleri

$$|\alpha|^2 + |\beta|^2 = 1 \tag{2.3}$$

normalizasyon şartını sağlarlar. $|\Psi\rangle$ kubiti ölçüldüğünde, $|\alpha|^2$ olasılıkla 0 sonucu veya $|\beta|^2$ olasılıkla 1 sonucu elde edilir. Normalizasyon koşulu geometrik olarak bir kubitin durumunun 1 uzunluğuna normalize edilmesi olarak yorumlanabilir. Bu nedenle bir kubit iki boyutlu karmaşık vektör uzayında bir birim vektördür. Kuantum bit ve klasik bit arasındaki temel fark şudur: Klasik bit yalnızca iki ayrı değer alabilirken, kuantum bit iki sürekli değişkenle parametrelendirilmiş bir vektör uzayında sonsuz değer alabilir. Bu bir tek kubitte sınırsız miktarda bilgi depolamanın mümkün olduğu anlamına gelmez, bir tek kuantum ölçümü yalnızca bir tek bilgi bitini verir [16].



Şekil 2. 1 Bir atomdaki iki elektronik seviyenin kubit gösterimi

Bir atom modelinde, elektron sırasıyla $|0\rangle$ veya $|1\rangle$ ile tanımlanan taban veya uyarılmış durumların birinde bulunabilir. Bir atom üzerine yeterli enerjili ışık uygun bir zaman dilimi süresince gönderilirse, elektron $|0\rangle$ durumundan $|1\rangle$ durumuna geçirilebilir veya bunun tam tersi de mümkündür. Fakat daha ilginç olarak, ışığı tutma süresini

azaltmakla, başlangıçta $|0\rangle$ durumunda olan elektron $|0\rangle$ ve $|1\rangle$ arasındaki yarıyolda hareket ettirilebilir. Bu durum

$$|+\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle \tag{2.4}$$

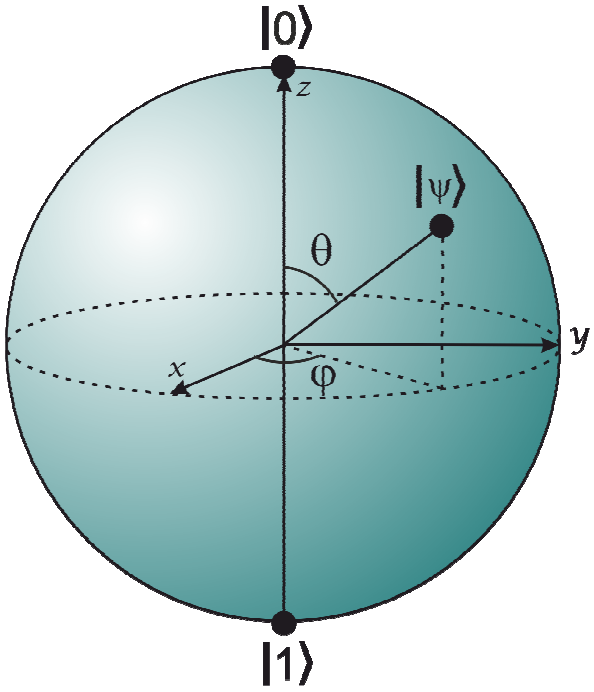
ile verilir. Ölçüm yapıldığında söz konusu atom $\%50$ olasılıkla $|0\rangle$ ve $\%50$ olasılıkla $|1\rangle$ durumunda bulunacaktır. Klasik bitlere göre bu tuhaflıklarına rağmen kubitler gerçek fiziksel nesnelerdir, varlıkları ve davranışları kapsamlı bir biçimde deneylerle doğrulanmıştır [17-20].

2.1.1 Bloch Küresi

Kubitin durum vektörlerine (2.3) normalizasyon şartının uygulanması, fiziksel bir anlamı olmayan çarpanların ihmal edilmesi ve α ve β sayılarının reel sayı olarak seçilmesiyle denklem (2.2) ile verilen eşitlik aşağıdaki gibi yeniden düzenlenebilir:

$$|\Psi\rangle = \cos\frac{\theta}{2}|0\rangle + e^{\phi}\sin\frac{\theta}{2}|1\rangle \qquad \theta \in [0,\pi],\ \phi \in [0,2\pi]. \tag{2.5}$$

Bu durum, kubitler ve onların durumlarına etki edebilen dönüşümler için yararlı geometrik bir temsil sağlar. θ ve ϕ açıları birim yarıçaplı üç boyutlu küre üzerinde bir noktayı tanımlar (Şekil 2.2).



Şekil 2. 2 Bir kubitin Bloch küresindeki gösterimi

Bu küreye Bloch küresi denilir [14,15] ve bir kubitin durumunu hayalimizde canlandırmak için faydalıdır. Tekli kubitler üzerindeki işlemlerin çoğunluğu Bloch küresi temsilinde düzgünce tanımlanılabilir. Bununla birlikte, çoklu kubitler için Bloch küresinin bilinen basit bir genellemesi yoktur. Birim küre üzerinde sonsuz sayıda nokta vardır. Bir kubitin gözlemlendiği andaki davranışı nedeniyle bu durum yanıltıcı olabilir. Çünkü bir kubitin ölçümü 0 veya 1 değerlerinden yalnızca birini verir.

2.1.2 Çoklu Kubitler

En basit durumdan başlanarak n-kubit sistemleri yapılandırılabilir. İlk olarak $00,01,10,11$ ile verilen dört farklı konfigürasyonla meydana gelebilecek iki klasik bitten oluşmuş bir sistem gözönüne alınır. Benzer biçimde , 2-kubit sistemi Hilbert uzayına ait $|00\rangle,|01\rangle,|10\rangle$ ve $|11\rangle$ ile gösterilen dört baz vektörle oluşturulabilir. Artık kubitlerin bir çifti, bu dört durumun herhangi bir şekilde üst üste binmesinden oluşur:

$$|\varphi\rangle = \alpha_{00}|00\rangle + \alpha_{01}|01\rangle + \alpha_{10}|10\rangle + \alpha_{11}|11\rangle . \tag{2.6}$$

Böylece, 2-kubit sisteminin durumunu tanımlamak için

$$|\alpha_{00}|^2 + |\alpha_{01}|^2 + |\alpha_{10}|^2 + |\alpha_{11}|^2 = 1 \tag{2.7}$$

normalizasyon koşulunu sağlayan karmaşık genliklere ihtiyaç duyulur.

2-kubit sistemindeki bir kuantum ölçümünden yalnızca bu dört durum ortaya çıkar. Bu şu anlama gelir: Böyle bir sistemde iki bilgi bitinden daha fazlası depolanamaz [15]. Önemli bir 2-kubit durumu,

$$\frac{|00\rangle + |11\rangle}{\sqrt{2}} \tag{2.8}$$

ifadesi ile verilen ve Bell durumu veya EPR çifti olarak isimlendirilen durumdur [14,15]. Bu durum kuantum hesaplama ve kuantum bilgideki birçok süprizden sorumlu tutulur. Dahası birçok başka ilginç kuantum durumları için bir ilk örnek teşkil eder. EPR durumu birinci kubit ölçülene kadar iki mümkün sonuca sahiptir. $1/2$ olasılıkla 0 sonucunu verir ve ölçüm sonrası durum $|00\rangle$ olur veya $1/2$ olasılıkla da 1 sonucunu verir ve ölçüm sonrası durum $|11\rangle$ olur. Sonuçta, ikinci kubitin ölçümü her zaman birinci kubitin ölçümüyle aynı sonucu verir. Yani, ölçüm sonuçları korelasyonludur [15]. Bu korelasyonlar ilk defa 1935 yılında Einstein, Podolsky ve Rozen'in ortak bir çalışmasında dile getirilmiştir [21]. Sonrasında ise John Bell tarafından bu alandaki çalışmalara devam edilmiştir. Bell durumunda ölçüm korelasyonlarının, klasik sistemler arasındaki korelasyonlardan daha kuvvetli olduğu Bell tarafından kanıtlanmıştır [22].

Çoklu kubit sistemleri, klasik durumda gözlemlenemeyen saf kuantum korelasyonlarını veren dolaşık durumların varlığına imkân sağlar [23]. Dolaşık durumlar, kuantum bilgi süreçleri için temel alet teşkil ederler ve ışınlama gibi pek çok tipik kuantum etkilerden sorumludurlar.

Daha genel olarak, n-kubit sistemi gözönüne alınabilir. n-kubit sistemi, n tane iki boyutlu tekli-kubitin Hilbert vektör uzayında tensör çarpımıyla verilmektedir. Böyle bir sistemin herhangi bir durumu

$$\left|\Psi\right\rangle = \sum_{x_0,.....,x_n} \alpha_{x_0,.....,x_n} \left| x_0, x_1, x_2,...., x_n \right\rangle \ , \quad x_i = 0,1 \tag{2.9}$$

olarak yazılabilir. Bu nedenle, normalizasyon koşulu gözönüne alındığında bir n-kubit sistemi tanımlamak için karmaşık genliklere ihtiyaç duyulur [15].

2.2 Dirac Gösterimi

N. Mermin'e göre matematikçiler Dirac notasyonunu sevmeme eğilimindedirler, çünkü bu durum onları önemli olan bir takım kısıtlamaları yapmaktan alıkoyar. Fizikçiler ise onu sever çünkü onları her zaman unuttukları bir takım kısıtlamaları hatırlamak zorunda olmaktan kurtarır [15]. H^N karmaşık sayılarla tanımlı sonlu N boyutlu Hilbert uzayı ve u, v, w bu uzayın vektörleri olsun. v ve w vektörlerinin skaler çarpımı (v, w) ile gösterilir. Matematikçilerin gösterimi şöyledir:

$$(v, \lambda w + \mu w) = \lambda (v, w) + \mu (v, w') \qquad (v, w) = (w, v') . \tag{2.10}$$

Fizikçilerin gösterimi matematikçilerinkinden farklıdır:

$$(v, \lambda w + \mu w') = \lambda^* (v, w) + \mu^* (v, w') . \tag{2.11}$$

$n = 1,2,....N$ olmak üzere, $\{e_n\}$, $H^{(N)}$ uzayının dik tabanı olsun. Bu tabanda u, v, w vektörleri

$$u_n = (e_n, u) \ , \ v_n = (e_n, v) , \ w_n = (e_n, w) \tag{2.12}$$

bileşenlerine sahiptir. $\{ e_n \}$ tabanında matris temsili ile verilen bir $A(v, w)$ lineer operatörü:

$$A_{nm}(v,w) = v_n w_n^* \tag{2.13}$$

biçimindedir. Bir u vektörüne $A_{nm}(v,w)$ operatörünün etkisi bileşenleri cinsinden

$$u_n' = \sum_m A_{nm}(v,w)u_m = \sum_m v_n w_m^* u_m = \sum_m v_n (w_m^* u_m) = v_n (w,u) \tag{2.14}$$

biçiminde veya vektör formunda

$$u' = A(v,w)u = v(w,u) \tag{2.15}$$

ile verilir. Dirac gösteriminde, vektör v ve skaler çarpım (w,v) :

$$v \to |v\rangle,\ (w,v) \to \langle w|v\rangle \tag{2.16}$$

biçiminde verilir. Bu gösterime göre $A_{nm}(v,w)$ operatörünün bir u vektörüne etkisi

$$|u'\rangle = |A_{nm}(v,w)|u\rangle = |v\rangle\langle w|u\rangle = (|v\rangle\langle w|)|u\rangle \tag{2.17}$$

olarak yazılır, burada

$$A(v,w) = |v\rangle\langle w| \tag{2.18}$$

olarak alınmıştır. Özel olarak $v = w$ durumunda v aşağıdaki gibi normalize edilmiş bir vektördür:

$$A(v,v) = |v\rangle\langle v|. \tag{2.19}$$

$A(v,v)$ operatörünün bir u vektörü üzerine etkisi

$$|A(v,v)\,u\rangle = |v\rangle\langle v|u\rangle \tag{2.20}$$

ile gösterilen P_v izdüşüm operatörüdür. Çünkü $|v\rangle\langle u|$, v boyunca u bileşenidir.

$M \le N$ olmak üzere H^M, H^N in M boyutlu alt uzayı olsun ve $|m\rangle$ $(m = 1,2,3,..,M)$ bu alt uzayda bir taban olsun. H^M üzerine etki eden izdüşüm operatörü

$$P_{H^M} = \sum_{M=1}^{M} |m\rangle\langle m| \tag{2.21}$$

ile tanımlanır.

Eğer $M = N$ ise aşağıdaki tamlık bağıntısı elde edilmektedir:

$$\sum_{M=1}^{M} |m\rangle\langle m| = \mathrm{I}\,. \tag{2.22}$$

Burada I birim operatördür. Bir lineer A operatörünün matris elemanları

$$A_{mn} = \langle m|A_n\rangle \tag{2.23}$$

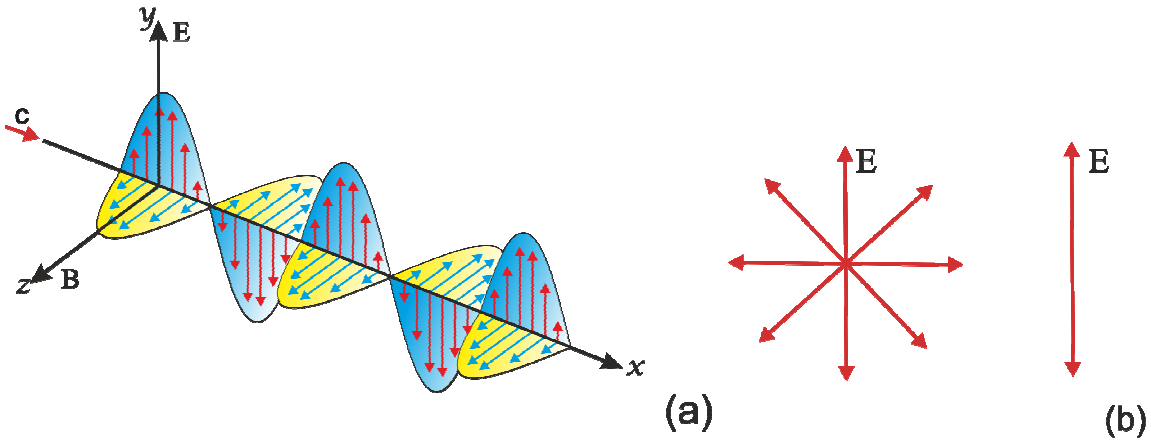
ile verilir. Mesela,

$$(AB)_{mn} = \langle m|AB_n\rangle = \langle m|AIB_n\rangle = \sum_k \langle m|Ak\rangle\langle k|Bn\rangle = \sum_k A_{mk}B_{kn} \tag{2.24}$$

şeklindedir.

2.3 Işığın Kutuplanması

Kubit için ilk somut örneğimiz, fotonun kutuplanması olayıdır. Bu nedenle ışığın kutuplanması konusunu kısaca ele alalım. Işığın kutuplanması ilk defa 1809'da Chevalier Malus tarafından kanıtlanmıştır [14]. Chevalier Malus, pencere camından yansıtılan güneş ışığının kristaldeki iki görüntüsünden birinin, kristal uygun bir biçimde yönlendirildiğinde kaybolduğunu ya da kuvvetli bir biçimde zayıfladığını gözlemlemiştir. Kutuplanma olayı ışık dalgalarının vektör doğasını gösterir. Işık enine titreşim yapar ve ışık dalgasının elektrik alan bileşeni yayılma yönüne diktir (Şekil 2.3).



Şekil 2. 3 a) Elektromanyetik dalganın şematik gösterimi,
(b) Kutuplanmış ışık demeti ve y – yönünde titreşen lineer kutuplu ışık demeti

z yönünde yol alan düzlemsel ve tek renkli skaler dalganın matematiksel tanımını hatırlayalım. Zamanın fonksiyonu olarak $u(z,t)$ titreşiminin genliği

$$u(z,t) = u_0 \cos(wt - kz) \tag{2.25}$$

şeklindedir. Burada w titreşim frekansı ve k ise dalga vektörüdür. Kutuplanmanın zamana bağlı kısmına yoğunlaşmak için $z = 0$ seçilebilir. Bu durumda $z = 0$ düzlemi içinde zamana bağlı kısmın incelenmesi mümkün olur. Yani

$$u(z = 0,t) = u(t) = u_0 \cos wt \tag{2.26}$$

olur. Bir elektromanyetik dalga polarizör içinden geçtiğinde polarizörden iletilen titreşim xoy düzleminde yayılma doğrultusunun enine titreşen bir vektördür. Polarizörün kutuplanma düzleminin x ekseniyle θ açısı yaptığı durumda, polarizör çıkışında elektrik alanın x ve y bileşenleri,

$$E'_x = E_0 \cos\theta \cos wt \tag{2.27}$$

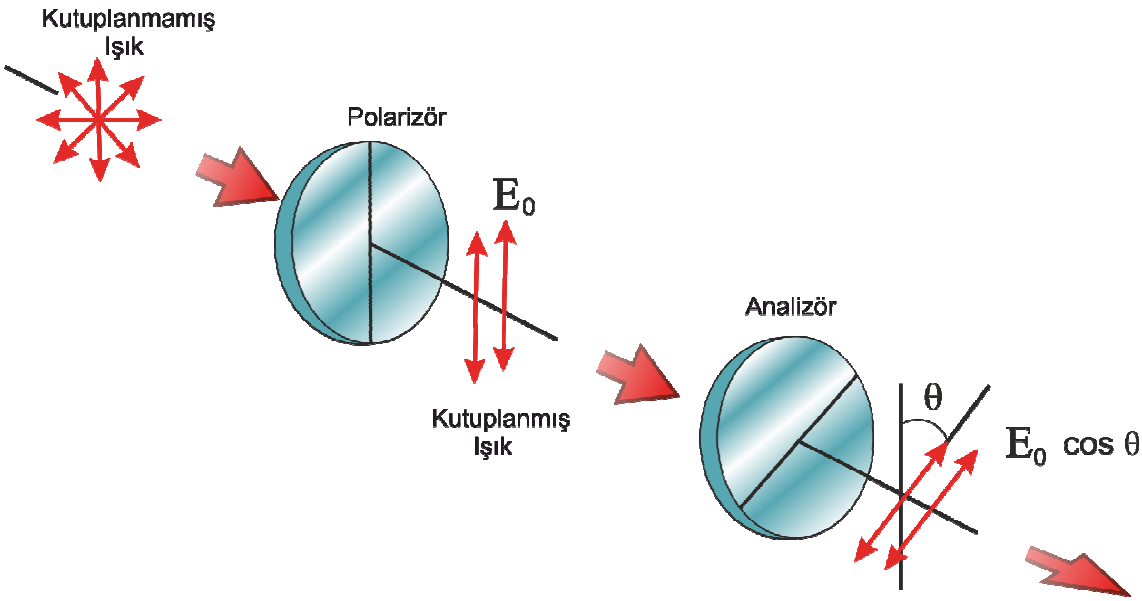
$$E'_y = E_0 \sin\theta \cos wt \tag{2.28}$$

şeklinde verilir. Burada θ filtrenin yönelimine bağlıdır (Şekil 2.4). Bir fotoelektrik hücre kullanılarak ölçülen ışık şiddeti (veya enerji) elektrik alanın karesiyle orantılıdır $(I \propto E_0^2)$. xoy düzleminde $\hat{p}$ birim vektörü,

$$\hat{p} = (\cos\theta, \sin\theta) \tag{2.29}$$

elektromanyetik dalganın lineer üst üste binmesini karakterize eder:

$$\vec{E}' = E_0 \hat{p} \cos wt\,. \tag{2.30}$$



Şekil 2. 4 Kutuplanma eksenleri çakışmayan iki kutuplayıcı levha

$\theta = 0$ ise ışık x ekseni doğrultusunda ve $\theta = \pi / 2$ ise y ekseni doğrultusunda kutuplanır. Doğal ışık $\%50$ Oy ekseni ve $\%50$ Ox ekseni boyunca kutuplanmıştır. Bu durum, ışığın koherent olmayan üst üste binmesinden oluşur.

Polarizör-analizör seti kullanılarak ışığın kutuplanması şöyle incelenebilir. İlkin, ışığın, kutuplanma düzlemi Ox ekseniyle θ açısı yapan bir polarizör içinden geçmesine izin verilir. Sonra, kutuplanma düzlemi Ox ekseniyle α açısı yapan ve analizör adı verilen ikinci bir polarizörden daha geçmesi sağlanır. xoy düzleminde $\hat{n}$ birim vektörü,

$$\hat{n} = (\cos\alpha, \sin\alpha) \tag{2.31}$$

olarak ifade edilir. Analizörden çıkıştaki E'' elektrik alanı (2.30) alanını $\hat{n}$ üzerine izdüşürmekle aşağıdaki gibi elde edilir:

$$\begin{aligned}\vec{E}'' &= (\vec{E}' \cdot \hat{n})\hat{n} = E_0 \cos wt(\hat{p} \cdot \hat{n})\hat{n} \\ &= E_0 \cos wt(\cos\theta\cos\alpha + \sin\theta\sin\alpha)\hat{n} \\ &= E_0 \cos wt\cos(\theta - \alpha)\hat{n}\,. \end{aligned} \tag{2.32}$$

Denklem (2.32) den analizör çıkışındaki şiddet için Malus yasası [14] elde edilir:

$$I'' = I\cos^2(\theta - \alpha)\,. \tag{2.33}$$

Lineer kutuplanma, kutuplanmanın tek biçimi değildir. Örneğin, dairesel kutuplanma, ışığın elektrik alan bileşeninin y bileşeninin fazını $\pm\pi/2$ kaydırmakla ve $\theta = \pi/4$ seçmekle elde edilir. Sağ el yönündeki dairesel kutuplanma için

$$E_x = \frac{E_0}{\sqrt{2}}\cos wt\,, \tag{2.34}$$

$$E_y = \frac{E_0}{\sqrt{2}}\cos(wt - \pi/2) = \frac{E_0}{\sqrt{2}}\sin wt \tag{2.35}$$

ifadeleri elde edilir. Elektrik alan vektörü xoy düzleminde $\left|E_0/\sqrt{2}\right|$ yarıçaplı bir daire çizer. Elektrik alan vektörünün ucunun bir elips çizdiği eliptik kutuplanma en genel durumdur.

$$E_x = E_0\cos\theta\cos(wt-\delta_x) = E_0\,\mathrm{Re}\left[\cos\theta\, e^{-i(wt-\delta_x)}\right] = E_0\,\mathrm{Re}\left[\lambda e^{-iwt}\right] \tag{2.36}$$

$$E_x = E_0\cos\theta\cos(wt-\delta_y) = E_0\,\mathrm{Re}\left[\sin\theta\, e^{-i(wt-\delta_y)}\right] = E_0\,\mathrm{Re}\left[\mu e^{-iwt}\right] \tag{2.37}$$

En genel kutuplanma durumu 1 uzunluğuna normalize edilmiş karmaşık bir vektörle (veya normalize edilmiş bir vektörle), iki boyutlu uzayda, $\lambda = \cos\theta\, e^{i\delta_x}$, $\mu = \sin\theta\, e^{i\delta_y}$ bileşenleriyle tanımlanılır ve $|\lambda|^2 + |\mu|^2 = 1$ şartını sağlar.

Ox ekseni boyunca yönlendirilmiş polarizörle, Oy ekseni boyunca yönlendirilmiş analizör düzeneğinde hiç ışık iletilemez. Eğer Ox ekseniyle θ açısı yapan bir polarizör kullanılırsa, ışığın bir kısmı iletilir. Birinci izdüşüm ışık şiddetinin $\cos\theta$ katını, ikincisi ise ışık şiddetinin $\sin\theta$ katını vereceğinden, analizör çıkışındaki şiddet

$$I'' = I\cos^2\theta\sin^2\theta \tag{2.38}$$

olur. Denklem (2.38) gözönüne alındığında $\theta = 0$ veya $\theta = \pi/2$ olması durumunda analizör çıkışındaki şiddet sıfırdır.

2.4 Fotonun Kutuplanması

A. Einstein'ın 1905'teki çalışmasından beri ışığın fotonlardan veya ışık parçacıklarından oluştuğu bilinmektedir [14]. Işığın yoğunluğu yeterli seviyede azaltılırsa ve CCD kameranın modern bir sürümü olan fotodedektörler kullanılırsa, bir tek fotonun kutuplanması incelenebilmektedir [14]. Bir deneyde N tane fotonun algılanabildiği varsayılır. $N \to \infty$ limitinde dalga optiğinin bir önceki kesimde elde edilmiş olan sonuçları yeniden elde edilir. Bir plaka kullanılarak, kutuplanması Ox ekseniyle θ açısı yapan bir ışık demeti Ox ve Oy eksenleri boyunca kutuplanmış iki demete ayrılırsa, bu iki demetin şiddetleri sırasıyla $I\cos^2\theta$ ve $I\sin^2\theta$ olur. Bu durumda şiddet azalır ve fotonlar plakaya daha düşük şiddette varırlar. Fotonları izlemek için plakalar arkasına D_x ve D_y gibi iki fotodedektör yerleştirilir. Deney, fotonların D_x veya D_y den birine ulaştığını gösterir. Bir foton asla bölünmez [14]. Başka bir deyişle, deneyde bir fotonun $D_x\,(D_y)$ tarafından algılanma olasılığı $p_x = \cos^2\theta$ veya $p_y = \sin^2\theta$ olur. Deneyde N tane foton algılanabilirse, $D_x\,(D_y)$ tarafından gözlemlenen $N_x\,(N_y)$ adet foton vardır.

Kutuplanmış foton optik fiberden geçirilerek bilgi iletiminde kullanılabilir. Keyfi olarak, Ox boyunca kutuplanmış fotonla 0 bit değerini ve Oy ekseni boyunca kutuplanmış fotonun da 1 bit değerini aldığı varsayılabilir. Kuantum bilgi teorisinde, bilgi iletişimi (değiş-tokuşu) yapan insanlar gönderici ve alıcı olarak isimlendirilebilir (İngilizce kaynaklarda gönderici Alice, alıcı ise Bob'tur). Mesela, gönderici alıcıya $yyxyxyyyx$.... olarak kutuplanmış foton serisini gönderir. Alıcı ise bir analizör kullanarak bu fotonların kutuplanmasını analiz eder. Böylece göndericinin yolladığı fotonun şifresini çözer: 110101110.... gibi.

Açıkçası, bu bir mesajı iletmek için çok etkin bir yöntem değildir. Bununla birlikte, bu yöntem kuantum şifrelemenin temelini oluşturur [14]. Fotonun kutuplanması kubitin bir örneğidir. Bu nedenle bilgi taşıma açısından bir kubit yalnızca 0 ve 1 değeri alabilen sıradan bir bitten çok daha zengindir. Bir kubit üst üste binme ilkesi sayesinde 0 ve 1 de dâhil olmak üzere 0 ve 1 arasındaki tüm ara değerleri de alabilir. Bundan dolayı sınırsız bir bilgi içerir.

Lineer üst üste binmeler gözönüne alınarak, kutuplanmanın matematiksel tarifinin yapılması için iki boyutlu Hilbert uzayı kullanılır. Herhangi bir kutuplanma durumu bu uzayda uygun bir vektörle tanımlanabilir. Mesela, fotonun Ox ve Oy eksenleri boyunca olan lineer kutuplanmalarına karşılık gelmek üzere Hilbert vektör uzayının $|x\rangle$ ve $|y\rangle$ dik tabanları seçilebilir [14]. Bu durumda bir $|\Phi\rangle$ kubiti

$$|\Phi\rangle = \lambda|x\rangle + \mu|y\rangle \tag{2.39}$$

şeklinde yazılabilir. Hilbert uzayı vektörleri için Dirac gösterimini kullanmak daha uygun olmaktadır. Hatırlayalım ki; H Hilbert uzayı pozitif tanımlı skaler çarpımla tanımlanmış karmaşık bir vektör uzayıdır. Olasılık genlikleri, bu uzaydaki skaler çarpımla ilişkilidir. (2.38) de verilen $|\Phi\rangle$ ve $|\Psi\rangle = \upsilon|x\rangle + \sigma|y\rangle$ gibi iki vektörün skaler çarpımı $\langle\Psi|\Phi\rangle$

$$\langle\Psi|\Phi\rangle = \upsilon^*\lambda + \sigma^*\mu = \langle\Phi|\Psi\rangle^* \tag{2.40}$$

olarak tanımlanır. C^*, C nin karmaşık eşleniğidir. Skaler çarpım bu nedenle $|\Phi\rangle$ de lineer ve $|\Psi\rangle$ de anti-lineerdir. $|\Phi\rangle$ nin normu $\|\Phi\|$ ile gösterilir ve

$$\|\Phi\|^2 = \langle\Phi|\Phi\rangle = |\lambda|^2 + |\mu|^2 \tag{2.41}$$

olarak elde edilir.

$|x\rangle$ ve $|y\rangle$ vektörleri (2.40) skaler çarpımına göre diktirler ve normları 1 olur.

$$\langle x|x\rangle = \langle y|y\rangle = 1 \quad , \qquad \langle x|y\rangle = 0 \tag{2.42}$$

$\{|x\rangle, |y\rangle\}$ seti Hilbert uzayının dik tabanıdırlar. Zorunlu olmamakla birlikte, fiziksel bir durumu tanımlamak için uygun normalizasyon koşulu eklenebilir,

$$\|\Phi\|^2 = |\lambda|^2 + |\mu|^2 = 1. \tag{2.43}$$

Matematiksel olarak, kutuplanma durumları Hilbert vektör uzayında, kutuplanmanın durum vektörleri olarak adlandırılan normalize edilmiş vektörlerle temsil edilir.

2.5 Kuantum Mekaniğinin Prensipleri

Kuantum mekaniğinin ilkeleri fotonun kutuplanması durumunda elde edilen sonuçları genelleştirir [14]:

Prensip 1: Kuantum sisteminin fiziksel durumu sonsuz boyutlu Hilbert vektör uzayına ait $|\Phi\rangle$ vektörüyle temsil edilir ve kuantum sisteminin durum vektörü olarak adlandırılır. Kuantum bilgi teorisinin amaçları doğrultusunda sonlu boyutlu uzay yeterlidir. $|\Phi\rangle$ normalize edilmiş bir vektör olarak seçilir: $\|\Phi\|^2 = 1$.

Prensip 2: $|\Psi\rangle$ ve $|\Phi\rangle$ iki fiziksel durumu temsil etsin. Ψ de Φ bulmanın olasılık genliği

$$a(\Phi \to \Psi) = \langle \Psi | \Phi \rangle \tag{2.44}$$

skaler çarpımıyla verilir. Ayrıca Φ için Ψ testini geçme olasılığı

$$p(\Phi \to \Psi) = |a(\Phi \to \Psi)|^2 \tag{2.45}$$

olarak elde edilir. Bir polarizör kullanarak kuantum sistemini $|\Psi\rangle$ durumuna geçirme işleminin matematiksel karşılığı $|\Psi\rangle$ üzerine bir dik izdüşüm operatörünü uygulamaktır. P_Ψ izdüşüm operatörü olsun. P_Ψ nin Φ durumuna etkisi

$$|P_\Psi \Phi\rangle \equiv P_\Psi |\Phi\rangle = |\Psi\rangle\langle\Psi\|\Phi\rangle = \left(|\Psi\rangle\langle\Psi|\right)|\Phi\rangle \tag{2.46}$$

ile verilir. İzdüşüm operatörü daha uygun bir formda yazılabilir:

$$P_\Psi = \langle \Psi | \Psi \rangle . \tag{2.47}$$

Özetle, bir ölçüme karşılık gelen matematiksel işlem o durumun izdüşümünü almaktır. Karşılık gelen ölçüm, izdüşürücü ölçüm olarak adlandırılır. Bununla birlikte, $P_\Psi|\Phi\rangle$ vektörü başta normalize edilmemiştir, normalize edilmelidir:

$$P_\Psi |\Phi\rangle \to |\Phi'\rangle = \frac{P_\Psi |\Phi\rangle}{\langle \Phi \| P_\Psi \Phi \rangle} . \tag{2.48}$$

Kuantum mekaniğinin geleneksel yorumunda durum vektörünün izdüşümünün alınmasına durum vektörünün çöküşü veya dalga paketinin çöküşü denir. Dalga paketinin çöküşü, kuantum mekaniğinin tamamlayıcı temel ilkesi olarak görülür [14].

Bir kuantum sisteminin, $\{|x\rangle, |y\rangle\}$ tabanları üzerinde P_x, P_y izdüşüm operatörleri:

$$P_x = |x\rangle\langle x| = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \tag{2.49}$$

$$P_y = |y\rangle\langle y| = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \tag{2.50}$$

biçiminde tanımlanır. I birim operatörü P_x ve P_y izdüşüm operatörlerinin toplamı olarak yazılabilir:

$$P_x + P_y = |x\rangle\langle x| + |y\rangle\langle y| = I\ . \tag{2.51}$$

Denklem (2.51) ile verilen ifade Kesim 2.2 de değinilen tamlık bağıntısının özel bir durumudur ve N boyutlu Hilbert uzayının dik tabanına genelleştirilebilir:

$$\sum_{i=1}^{N} |i\rangle\langle i| = I\ , \tag{2.52}$$

$$|i\rangle\langle j| = \delta_{ij}\ . \tag{2.53}$$

P_x ve P_y izdüşüm operatörleri komütatiftir, yani

$$[P_x, P_y] \equiv P_x P_y - P_y P_x = 0 \tag{2.54}$$

eşitliğini sağlar. Burada $|x\rangle$ ve $|y\rangle$ testlerine uyumlu testler denir. Öte yandan $|\theta\rangle$ ve $|\theta_\perp\rangle$ durumlarına karşılık gelen izdüşüm operatörleri

$$P_\theta = |\theta\rangle\langle\theta| = \begin{pmatrix} \cos^2\theta & \sin\theta\cos\theta \\ \sin\theta\cos\theta & \sin^2\theta \end{pmatrix}, \tag{2.55}$$

$$P_{\theta_\perp} = |\theta_\perp\rangle\langle\theta_\perp| = \begin{pmatrix} \sin^2\theta & -\sin\theta\cos\theta \\ -\sin\theta\cos\theta & 0 \end{pmatrix} \tag{2.56}$$

olarak elde edilir. Bu operatörler P_x ve P_y ile komütatif değildirler. Böyle olduğu

$$[P_x, P_\theta] = \begin{pmatrix} 0 & \sin\theta\cos\theta \\ -\sin\theta\cos\theta & 0 \end{pmatrix} \tag{2.57}$$

ifadesinden açıkça görülmektedir. Bu nedenle $|x\rangle$ ve $|\theta\rangle$ testlerine uyumsuz testler denir. Foton $x,.....,\theta_\perp$ eksenleri boyunca polarize edildiğinde $P_x,.....,P_{\theta_\perp}$ izdüşüm operatörleri kuantum sisteminin fiziksel özelliklerini matematiksel olarak temsil ederler. Eğer P_x ve P_θ komütatif değilse eş zamanlı olarak bu kuantum sisteminin özelliklerini ölçmek mümkün değildir.

N boyutlu H^N Hilbert uzayı, bu uzayın bir dik tabanını $|n\rangle$, $n = 1,2,...N$ ile verilen N tane $|n\rangle$ testlerinin kümesiyle ilişkilendirir. Bir kuantum sistemi $|\Phi\rangle$ durumundaysa, testi geçme olasılığı

$$p_n = |\langle n|\Phi\rangle|^2 \tag{2.58}$$

ile verilir ve

$$\sum_n p_n = 1 \tag{2.59}$$

eşitliğini sağlar. $|n\rangle$ testleri maksimal bir test oluştururlar. Bu durumda $\{|\alpha\rangle\}$ öncekiyle uyumsuz diğer maksimal test H^N in farklı bir dik tabanına karşılık gelir. Hilbert uzayında $\{|n\rangle\}$ ve $\{|\alpha\rangle\}$ $n, \alpha = 1,2,...N$ tabanlarında maksimal olarak uyumsuzluk tanımlanabilir.

$$|\langle\alpha|n\rangle|^2 = \frac{1}{N} \tag{2.60}$$

(2.60) ile verilen tanımdan $|\langle\alpha|n\rangle|^2$, α ve n den bağımsızsa, yani α ve n tamamlayıcıysa, iki tabanın maksimal olarak uyumsuz olduğu görülür. Tamamlayıcılığı

bir örnekle söylemek gerekirse $\{|x\rangle,|y\rangle\}$ ve $\left\{\left|\theta=\frac{\pi}{4}\right\rangle,\left|\theta=-\frac{\pi}{4}\right\rangle\right\}$ tabanları tamamlayıcıdırlar.

Tamamlayıcı tabanların fiziksel anlamı şöyle izah edilir [14]: Varsayalım ki, hepsi, $|n\rangle$ tabanının bilmediğimiz bir durumunda olan çok sayıda kuantum sistemi bulunsun. Bu kuantum sistemleri $|n\rangle$ tabanı kullanılarak test edilirse, sonuçların biri, mesela m, $\%100$ olasılıkla çıkar, yani ölçüm durumun maksimum bilgisini verir. Eğer aksine $|\alpha\rangle$ tabanını kullanarak test edilirse, o zaman da $1/N$ olasılıkla tüm diğer mümkün sonuçlar elde edilir. Bu sonuçtan adı geçen durum hakkında minimum bilgiye ulaşılır.

2.6 Kuantum Kopyalanamama Teoremi

Göndericinin alıcıya yolladığı fotonun durumu bilgi hırsızı tarafından kopyalanamıyorsa, bu kuantum şifrelemede kulanılan yöntemin mükemmel güvenilir olduğu anlamına gelir. Kuantum kopyalanamama teoremi keyfi bir kuantum durumunun kopyalanamayacağını ifade eder [24] ve kuantum şifrelemenin mutlak güvenliği için temel dayanak oluşturur [3]. Bir bilgi hırsızının müdahalesine rağmen alıcının ölçüm sonucu göndericinin yolladığı orjinal durumla aynı ise, mesajın başkaları tarafından ele geçirilip geçirilmediği anlaşılamaz. Kuantum kopyalanamama teoremi göndericinin alıcıya yolladığı fotonların bilgi hırsızı tarafından çoğaltılmasını imkansız kılar. Yani müdahale varsa kuantum durumu değişecektir. Bilgi hırsızı bu kopyalama işlemini yapabilseydi, o zaman öyle fotonlardan çok sayıda üretebilir ve kopyalama işlemini problemsiz yapmış olurdu.

Bu teorem şöyle izah edilebilir [14]: Bilinmeyen bir kuantum durumu olan $|x_1\rangle$ durumunun kopyasının yapılmak istendiği varsayılır. Eğer $|x_1\rangle$ bilinseydi hazırlanma işlemi bilinmiş olacağından kopyalamak sorun olmayacaktı. Kopyası yazılmak istenen sistem $|\varphi\rangle$ ile gösterilir ve bir boş kâğıda eşdeğerdir. Mesela spin ½ durumuna karşılık gelen $|x_1\rangle$ çoğaltılmak istenirse, o zaman $|\varphi\rangle$ durumu spin ½ nin bir durumu olur. Çoğaltma sürecinde durum vektörünün gelişimi (2.61) formunda olmalıdır:

$$\left|x_1 \otimes \varphi\right\rangle \rightarrow \left|x_1 \otimes x_1\right\rangle \tag{2.61}$$

Bu gelişim üniter U operatörüyle kontrol edilir:

$$\left|U(x_1 \otimes \varphi)\right\rangle = \left|x_1 \otimes x_1\right\rangle . \tag{2.62}$$

Denklem (2.62) de verilen U operatörü evrensel olmak zorunda (çünkü fotokopi işlemi kopyalanan duruma bağlı değil) ve bu nedenle bilinemeyen $\left|x_1\right\rangle$ durumundan bağımsız olduğu varsayılır. İkinci bir orjinal $\left|x_2\right\rangle$ durumu çoğaltılmak istenirse şöyle yapılmalıdır:

$$\left|U(x_2 \otimes \varphi)\right\rangle = \left|x_2 \otimes x_2\right\rangle . \tag{2.63}$$

Burada skaler çarpım değerlendirilirse:

$$X = \left\langle x_1 \otimes \varphi \middle| U^{+}U(x_2 \otimes \varphi)\right\rangle \tag{2.64}$$

ifadesi elde edilir ve bu ifadeyi açıklamak için iki farklı yol vardır:

$$X = \left\langle x_1 \otimes \varphi)\middle| x_2 \otimes \varphi\right\rangle = \left\langle x_1 \middle| x_2\right\rangle \tag{2.65}$$

ve

$$X = \left\langle x_1 \otimes x_1 \middle| x_2 \otimes x_2\right\rangle = \left(\left\langle x_1 \middle| x_2\right\rangle\right)^2 . \tag{2.66}$$

Sonuç her ikisinde de $\left|x_1\right\rangle \equiv \left|x_2\right\rangle$ veya $\left\langle x_1 \middle| x_2\right\rangle = 0$ olur. İki durumun lineer üst üste binmesi dışında bir $\left|x_1\right\rangle$ durumu veya bir dik durumun çoğaltılması mümkündür [14]. Kuantum kopyalanamama teoreminin ispatı birilerinin neden kuantum şifrelemede fotonlar için birbirine dik $\left|x\right\rangle$ ve $\left|y\right\rangle$ kutuplanma durumlarıyla kendini kısıtlamadığını izah eder [13]. Bir ajanın varlığının farkedilmesine yol açan şey $\left|x\right\rangle$ ve $\left|y\right\rangle$ kutuplanma durumlarının lineer üst üste binmelerinin kullanılmasıdır.

BÖLÜM 3

KUANTUM ŞİFRELEME

Şifreleme karmaşık ve ilginç tarihiyle birlikte antik bir sanattır [25]. İnsanlık tarihi boyunca şifreleme hiçbir zaman değerini kaybetmemiştir ve teknoloji ilerledikçe daha da önem kazanmaya devam edecektir. Özellikle, 20. yüzyılın başlarında büyüleyici doğasıyla kuantum fiziği bilim dünyasının gündemine girmiş ve şifreleme sistemleri üzerine kuantum fiziğinin temel yasalarının uygulanması önemli bir araştırma alanı olmuştur. Şifreleme 1949'dan sonra bilgi teorisinin en önemli dallarından biri olmuştur [26,3]. Shannon, kırılamaz kodların veya mükemmel gizli sistemlerin varlığını kanıtlamıştır [27]. Kuantum şifreleme kuantum bilginin en dikkate değer uygulamalarından birisidir. Kuantum şifreleme veya kuantum anahtar dağılımı olarak bilinen bir işlem, özel bir bilginin kanıtlanabilir güvenlikli dağılımına olanak sağlamak için kuantum mekaniğinin özelliklerini kullanır [27]. Kodlamada güvenli yöntemler elde etmek için kuantum fiziğinin özelliklerinin kullanılması düşüncesi Stephen Wiesner tarafından 1969 da önerilmiştir [28].

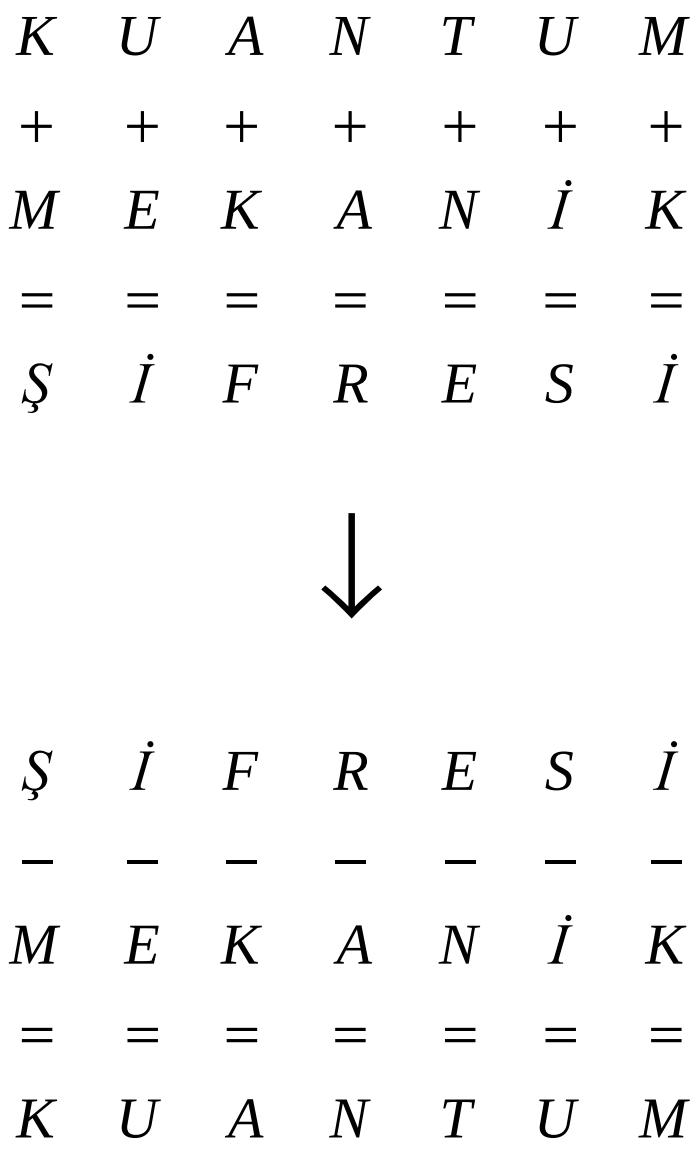
Mesaj şifrelemenin farklı yolları vardır. Gizli anahtar şifreleme sistemleri, açık anahtar şifreleme sistemlerine [29] göre şifrelemenin çok daha eski bir formudur ve onun prensipleri kuantum şifre sistemlerinde de kullanılır.

3.1 Simetrik (Gizli Anahtar) Şifreleme Sistemi

1970'lerde açık anahtar şifreleme yönteminin keşfine kadar bütün şifreleme sistemleri, şimdi gizli anahtar şifreleme yöntemi olarak bilinen farklı bir prensibe dayalı olarak çalışmıştır. Gizli anahtar şifreleme sistemlerinde, gönderici alıcıya mesaj yollamak istediğinde mesajını şifrelemek için bir şifreleme anahtarına sahip olurken, alıcının da şifreli mesajı çözmek için bir şifre çözme anahtarına sahip olması gerekmektedir. Şifreleme ve şifre çözme anahtarı aynı anahtardır (Şekil 3.1). Basit ve hala son derece etkin olan gizli anahtar şifreleme sistemi Vernam şifresidir [30].

Gönderici ve alıcı özdeş olan n bit gizli anahtar dizisiyle başlarlar. Gönderici mesaja anahtarı eklemekle n bit mesajı kodlar. Alıcı ise şifrelenmiş mesajdan şifre çözme anahtarını çıkarmakla mesajı çözer. Bu sistemin önemli özelliği şudur: Anahtar dizileri hakikaten gizli olduğu sürece kanıtlanabilir güvenliktedir. Bilgi hırsızı her zaman iletişim kanalında parazit yapabilir, fakat gönderici ve alıcı bu parazitliği fark edebilir ve bozukluğu ilan edebilirler. Bilgi hırsızının kullandığı herhangi bir gizli dinleme stratejisi için, gönderici ve alıcı onların kodlanmamış mesajlarıyla bilgi hırsızının bilgisinin istenildiği kadar küçük yapılabileceğini garanti edebilirler [15]. Aksine, yaygın olarak kullanılmasına rağmen, açık anahtar şifrelemenin güvenliği klasik bilgisayarlarla çarpanlarına ayırma gibi belirli problemleri çözmenin zorluğu ile ilgili ispatsız matematiksel varsayımlara dayanır. Mesela, herhangi büyük bir tam sayı yeterince kısa bir zamanda çarpanlarına ayırma problemi kuantum bilgisayarlarında Shor algoritması [31] uygulanarak aşılabilir. Gizli anahtar şifreleme sistemlerinin en büyük zorluğu anahtar bitlerinin güvenlikli dağılımıdır. Özellikle Vernam şifresi yalnızca, anahtar bitlerin sayısı en azından kodlanmış mesajın boyutu kadar büyük olduğu sürece güvenlidir ve anahtar bitler tekrar kullanılamaz. Bu nedenle ihtiyaç duyulan çok sayıdaki anahtar bitler genel kullanımda pratik olmayan uzun dizilere neden olur. Daha da ötesi, anahtar bitler ileride kullanılana kadar da dikkatli bir biçimde korunmak zorunda, sonrasında ise bozulur. Diğer taraftan, prensipte, böyle klasik bilgi orjinali bozulmaksızın kopyalanalabilir, bundan dolayı tüm protokolün güvenliği tehlikeye girebilir. Bu olumsuzluklarına rağmen Vernam şifresi gibi gizli anahtar şifreleme sistemleri gizli toplantılar, güvenilir kuryeler veya gizli güvenli iletişim linkleriyle teslim edilmiş anahtar materyalleriyle kanıtlanabilir güvenliklerinden dolayı kullanılmaya

devam edilmektedirler [15]. Bir simetrik (gizli anahtar) şifreleme örneği Şekil 3. 1 de verilmiştir.



Şekil 3. 1 Herkesin erişimine açık kanalda gizli anahtar şifreleme yöntemi, Vernam şifresi

3.2 Asimetrik (Açık Anahtar) Şifreleme Sistemi

Bu şifreleme sistemi, şifreleme ve şifre çözme için farklı anahtarların kullanımını gerektirir. Bu sistemin prensipleri ilkin Stanford Üniversitesi'nden Whitfield Diffie ve Martin Hellman tarafından 1976'da önerilmiştir [32]. İlk gerçek uygulama Massachusetts Institute of Technology'den Ronald Rivest, Adi Shamir ve Leonard Adleman tarafından 1978'de gerçekleştirilmiştir [33]. Bu şifreleme yöntemi adı geçen üç kişinin ikinci isimlerinin baş harflerinin biraraya getirilmesiyle RSA olarak anılır ve günümüzde de yaygın olarak kullanılır [27].

Alıcı, açık anahtar şifreleme sistemi ile şifrelenilmiş mesajlar almak isterse, gizli tuttuğu özel bir anahtar seçmelidir. Sonra, bu özel anahtardan herhangi bir ilgili şahsın ortaya çıkarabileceği bir açık anahtarı hesaplar. Gönderici bu açık anahtarı kullanarak mesajını şifreler. Gönderici şifrelediği mesajı özel bir anahtar kullanarak onu çözebilecek olan alıcıya yollar. Açık anahtar şifreleme sistemleri kullanışlıdır ve son 30 yıldır son derece yaygın olmuşlardır. Mesela internetin güvenliği böyle sistemlere dayanır. Açık anahtar şifreleme sistemi herhangi birinin mektup atabileceği bir mektup kutusunda kullanılabilir. Yalnızca yasal sahibi özel anahtarıyla onu açmakla erişebilir.

Açık anahtar şifreleme sistemlerinin güvenliği matematiksel hesaba dayalı karmaşıklığa güvenir. Amaç tek yol fonksiyonları olarak bilinen matematiksel nesneleri kullanmaktır. Tanım aracılığıyla, verilen x değeri için $f(x)$ fonksiyonunu hesaplamak kolaydır, fakat hesabın tersini yapıp $f(x)$ ten x i çıkarmak zordur. Sezgisel olarak, $61x43$ çarpımını hesaplamanın birkaç saniye ve 2623 sayısını asal çarpanlarına ayırmanın ise çok uzun zaman almasını anlamak kolaydır. Çarpanlarına ayırma işleminin iyi bir yanı vardır. Bunun anlamı bir ipucu verilmesi halinde sonucun çok basitleşeceğidir. Mesela 2623 ün bir asal çarpanı olan 61 söylenildiğinde, hesap öncekine kıyasla çok daha basit olur. RSA nın güvenliği gerçekten büyük sayıların çarpanarına ayrılmasına dayanır.

Zarifliğine rağmen, bu teknik büyük bir kusurun sıkıntısını çeker. Çarpanlarına ayırmanın zor mu, kolay mı olduğu henüz kanıtlanılmadı [15]. Henüz çarpanlarına ayırma işlemini hızlı bir biçimde yapacak bir algoritma mevcut değildir. Benzer olarak, tüm açık anahtar şifreleme sistemi güvenlikleri için teorik ve pratik ilerlemelerle örtpas edilebilen veya zayıflatılabilen kanıtsız varsayımlara güvenir. Bugüne kadar hiçkimse

güvenli asimetrik şifreleme sistemlerinin varlığını kanıtlayamadı. Bu durum bu şekilde işleyen şifreleme sistemlerine bir takım tehditler oluşturur. Güvenlikli bilgi iletişiminin son derece önemli olduğu yaşam koşullarında böyle tehditlere tahammül edilemez. Mesela matematikteki yeni bir buluş ansızın elektronik parayı değersiz yapabilir. Böyle ekonomik ve sosyal riskleri sınırlandırmak için simetrik şifreleme sistemlerini kullanmaktan başka çare yoktur.

Örnek: RSA şifreleme [14]

Alıcı iki asal sayı seçer, p ve q. $N = p.q$ olarak tanımlanır ve bir c sayısı $(p-1)(q-1)$ çarpımıyla hiçbir ortak bölene sahip değildir. $Mod(p-1)(q-1)$ in c ye bölümüyle d hesaplanır.

$$c.d \equiv 1 \bmod (p-1)(q-1) \tag{3.1}$$

Güvensiz bir yolla, alıcı N ve c sayılarını göndericiye yollar (p ve q yu ayrı ayrı değil!). Gönderici alıcıya bir $a < N$ sayısıyla temsil edilmek zorunda olan şifrelenmiş bir mesaj yollamak ister (Mesaj çok uzunsa, gönderici onu alt mesajlara bölebilir). Sonra

$$b \equiv a^c \bmod N \tag{3.2}$$

yi hesaplar. Alıcıya b yi yollar, her zaman güvensiz bir yolla, çünkü yalnızca N, b ve c yi bilen bir bilgi hırsızı orjinal mesajı a yı çıkaramaz. Alıcı mesajı aldığında

$$b^d \bmod N = a \tag{3.3}$$

yı hesaplar. Sonucun kesin olarak a olduğu gerçeği, yani göndericinin ilk mesajı sayı teorisinin bir sonucudur. Özetlersek N, b ve c sayıları herkesin erişimine açık bir yolla, güvensiz bir şekilde yollanılır.

Alıcının seçtiği sayısal değerler $p = 3$ ve $q = 7$ olsun. $N = p.q = 3.7 = 21$ ve $(p-1)(q-1) = (3-1).(7-1) = 12$ olur. $c = 5$ sayısının 12 ile hiçbir ortak böleni yoktur ve $\bmod 12$ çarpımına göre tersi $d = 5$ tir. Çünkü $5X5 = 24+1$. Alıcı $N = 21$ ve $c = 5$ sayılarını göndericiye yollar. Gönderici ise $a = 4$ seçer ve (3.2) yi kullanarak

$$4^5 = 1024 = 21x48 + 16 \tag{3.4}$$

$$4^5 \equiv 16 \bmod 21 \tag{3.5}$$

hesabını yapar ve (3.5) ifadesinden b yi 16 olarak hesaplar ve alıcıya yollar. Alıcı b mesajını aldıktan sonra (3.3) ifadesini kullanarak a yı bulur:

$$b^5 = 16^5 = 49932x21 + 4 \tag{3.6}$$

$$16^5 \equiv 4 \bmod 21 . \tag{3.7}$$

Böylece $a = 4$ orjinal mesajını keşfeder.

Diğer bir örneğimiz şöyle olsun: Alıcı $p = 2$ ve $q = 5$ i seçsin. $N = p.q = 2.5 = 10$ ve $(p-1)(q-1) = (2-1).(5-1) = 4$ olur. $c = 3$ sayısının 4 ile hiçbir ortak böleni yoktur ve $\bmod 4$ çarpımına göre tersi $d = 3$ tür. Çünkü $3X3 = 8+1$. Alıcı $N = 10$ ve $c = 3$ sayılarını göndericiye yollar. Gönderici ise $a = 6$ seçer ve (3.2) yi kullanarak

$$6^3 = 10x21 + 6 \tag{3.8}$$

$$6^3 \equiv 6 \bmod(10) \tag{3.9}$$

hesaplarını yapar. (3.9) ifadesinden $b = 6$ bulur ve bu sonucu alıcıya iletir. Alıcı ise (3.3) ifadesini kullanarak a yı bulur:

$$b^5 = 6^5 = 777x10 + 6 \tag{3.10}$$

$$6^5 \equiv 6 \bmod 10 . \tag{3.11}$$

Böylece $a = 6$ orjinal mesajını elde eder.

3.3 Kuantum Anahtar Dağılım Protokolleri

Kuantum anahtar dağılım protokolü bir açık kanal üzerinden iki kişi arasında gizli anahtar bitler aracılığıyla oluşturulabilen kanıtlanabilir güvenlikli bir protokoldür. Kişilere güvenli iletişim imkânı sağlayan klasik gizli anahtar şifreleme sistemini yürürlüğe koymak için anahtar bitler kullanılabilir. Kuantum anahtar dağılım protokolü için tek gereksinim kubitlerin bir eşik değerinden daha küçük bir hata oranıyla açık kanal üzerinden iletilebilmesidir. Meydana gelen anahtarın güvenliği kuantum bilginin özellikleri ile garanti altına alınır ve bu nedenle yalnızca fiziğin kurallarına şartlandırılır. Kuantum anahtar dağılımı arkasındaki ana düşünce aşağıdaki temel gözlemdir: Birincisi, bilgi hırsızı, durumlarını pertürbe etmeksizin iletilen kubitlerden herhangi bir bilgi elde edemez. Yani, kuantum kopyalanamama teorisi nedeniyle bilgi hırsızı, göndericinin kubitini koplayamaz. İkinci olarak, birbirine dik olmayan iki kuantum durumunu ayırtetmek için herhangi bir denemede bilgi eldesi ancak sinyali bozma pahasına mümkündür. Bu durum şöyle izah edilebilir:

$|\Psi\rangle$ ve $|\Phi\rangle$ bilgi hırsızının, hakkında bilgi elde etmeyi denediği dik olmayan kuantum durumları olsun. Bilgi hırsızının bilgi elde etmek için kullandığı süreç $|\Psi\rangle$ veya $|\Phi\rangle$ durumunu standart bir $|u\rangle$ durumunda bulunan bir yardımcıyla üniter olarak etkileştirmektir. Bu sürecin durumları bozmadığı kabul edilirse aşağıda verilen iki durum ortaya çıkar:

$$|\Psi\rangle|u\rangle \rightarrow |\Psi\rangle|v\rangle, \tag{3.12}$$

$$|\Phi\rangle|u\rangle \rightarrow |\Phi\rangle|v'\rangle. \tag{3.13}$$

Bilgi hırsızı $|v\rangle$ ve $|v'\rangle$ durumlarının farklı olmalarını isterdi ki durumun kimliği hakkında bilgi elde edebilsin. Bununla birlikte üniter dönüşümler altında iç çarpımlar korunumlu olduğundan,

$$\langle v|v'\rangle\langle\Psi|\Phi\rangle = \langle u|u\rangle\langle\Psi|\Phi\rangle, \tag{3.14}$$

$$\langle v|v'\rangle = \langle u|u\rangle = 1 \tag{3.15}$$

şeklinde olmak zorundadır, burada $|v\rangle$ ve $|v'\rangle$ durumlarının özdeş olmak zorunda olduğu vurgulanır. Bu nedenle $|\Psi\rangle$ ve $|\Phi\rangle$ durumlarını ayırtetmeye çalışmak kaçınılmaz olarak bu durumların en az birinin bozulmasıyla sonuçlanır. Gönderici ve alıcı arasında dik olmayan kubit durumlarının iletiminde de bu düşünce kullanılır. Gönderici ve alıcı iletilen durumdaki bozulmayı kontrol ederek iletişim kanalında meydana gelen herhangi gürültü veya gizli dinlemede bir üst sınırı tayin eder. Bu kontrol kubitleri bilgi kubitleri arasına rasgele karıştırılarak bu üst sınırı bilgi kubitlerine de uygulanır. Bu karışık durumdan anahtar bitler daha sonra çıkarılır. Gönderici ve alıcı o zaman paylaşılmış bir gizli anahtar dizisi biçimlendirmek için bilgi uzlaştırma ve güvenlik artırma uygularlar. Maksimum kabul edilebilir hata oranı için eşik değeri en iyi biçimde, bilgi uzlaştırma ve güvenlik artırma protokollerinin etkisiyle belirlenir.

Kuantum bilgi düşüncelerinin belirli kuantum anahtar dağılım protokollerinin güvenliğini kanıtlamada faydalı olabileceği önerilir. Kuantum hata düzeltme teorisi kuantum şifrelemenin güvenliğini kanıtlar. Bu kesimde kuantum anahtar dağılımı için üç farklı protokol verilecektir: Sırasıyla BB84 [11], B92 [13] ve EPR [12].

3.3.1 BB84 Protokolü

Kuantum şifrelemede kullanılmış ilk protokoldür ve dört durum tertiblidir [11]. Gönderici ve alıcı bu protokol aracılığıyla yüksek güvenliği nedeniyle Vernam şifresinde kullanılabilecek gizli bir anahtar elde eder.

Bu işlemde gönderici ve alıcı kuantum kanalını ve herkesin erişimine açık olan başka klasik kanalı da kullanırlar. Genellikle bir optik fiber olan kuantum kanalı fotonları teker teker yollamak için kullanılır.

Bu protokol kısaca şöyle tanımlanabilir:

Gönderici, $(+, X)$ tabanlarının özdurumları olan 0^o,90^o,45^o ve 135^o de lineer olarak polarize edilmiş fotonları hazırlar. Bu işlemi rasgele yapar ve hazırlanmış durumların dizisini kaydeden kuantum kanalı içinden bu fotonları yollar. H, D, V ve A olarak isimlendirilen ve sırasıyla yatay, 45^o, düşey ve 135^o kutuplanmış ilk iki durum için 0 ve son ikisi için ise 1 değerlerini verir. Bu yolla, gönderici tamamen rasgele bit dizisini elde

eder. Sonrasında ise üç farklı sıralanış yazar. Birincisi kutuplanma tabanları için, diğeri kutuplanma durumları için ve sonuncusu bitlerin sıralanışı içindir [26]:

```
X+X+XXXX+++X++X+X+XXXX+++++++XXXX+++X+XXXXXX++X+...
DVAHADAAVVHDHHDHAVDADAHHVHVHVDDADHVVDVAAADADHHDH...
01101011110000011010100101010010011011110100000...
```

Şekil 3. 2 Göndericinin kutuplanma tabanları, kutuplanma durumları ve bit dizilerinin sıralanışı

Alıcı $+$ tabanında ve X tabanında ölçüm alan iki aleti kullanarak gönderici tarafından yollanan fotonları analiz eder. Herbir fotonu ölçmek için kullanılacak analizörü rasgele seçer, herbir fotonun ölçümü için kullanılmış tabanın dizisini ve bu ölçümlerin sonucunu da yazar. Tıpkı gönderici gibi alıcıda H ve D durumlarını 0, V ve A durumlarını ise 1 ile gösterir. Bu yolla alıcı, aşağıdaki dizileri elde eder [26]:

```
X+X+XXXX+++X++X+X+XXXX+++++++XXXX+++X+XXXXXX++X+...
DVAHADAAVVHDHHDHAVDADAHHVHVHVDDADHVVDVAAADADHHDH...
01101011110000011010100101010010011011110100000...
```

Şekil 3. 3 Alıcının kullandığı kutuplanma tabanları, ölçtüğü kutuplanma durumları ve bit dizilerinin sıralanışı

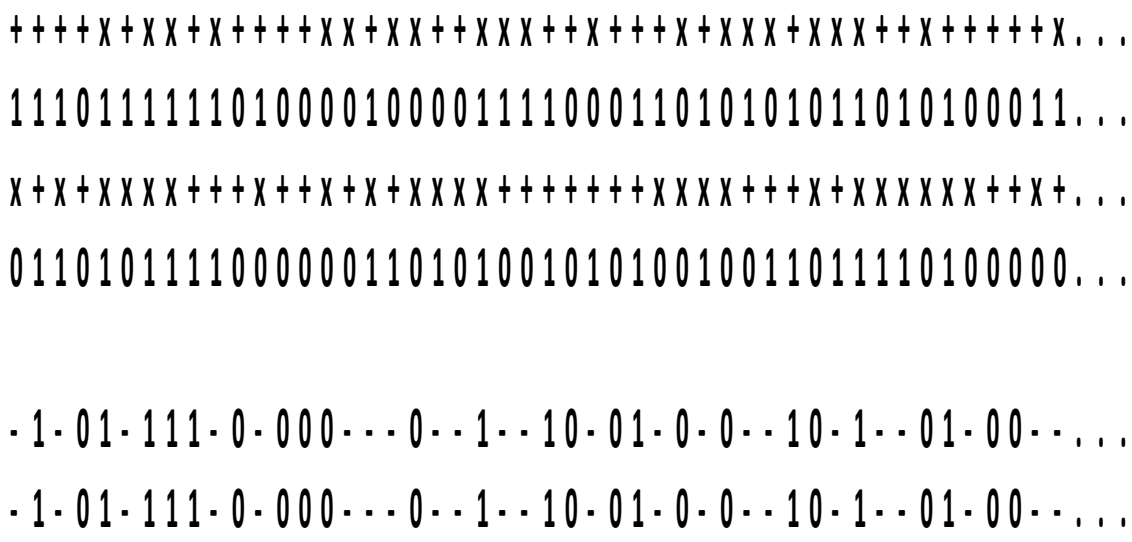
Gönderici ve alıcı aynı tabanı kullanırlarsa, ölçüm sonucunun her ikisi içinde aynı olacağına dikkat edilmelidir. Aksi halde $\%50$ olasılıkla aynı sonucu elde ederler.

Herkesin erişimine açık bilgi kanalı kullanmakla, gönderici ve alıcı kutuplanma durumlarının dizisini ve kullanılan analizörleri ortaya koyarlar. Hazırlanmış durumları ve alıcının ölçümüyle elde edilmiş durumları iletişim kurmak için kullanmazlar.

```
++++X+XX+X++++XX+XX++XXX++X+++X+XXX+XXX++X+++++X...
X+X+XXXX+++X++X+X+XXXX+++++++XXXX+++X+XXXXXX++X+...
```

Şekil 3. 4 Göndericinin durumları hazırladığı kutuplanma tabanları ve alıcının ölçümde kullandığı kutuplanma tabanları

Göndericinin fotonları hazırlamak için kullandığı kutuplanma tabanı ile alıcının ölçümde kullanıldığı analizör tabanının çakışmadığı ve ayırt etmede hata yapılan durumları dikkate almazlar.



Şekil 3. 5 Gönderici ve alıcının bit dizilerinin kıyaslanmasıyla anahtarın elde edilmesi

Bu nedenle anahtar

$$10111100000110010010 10.... \tag{3.16}$$

olur. Gönderici tarafından yollanan tüm fotonların alıcı tarafından alındığı varsayılırsa, anahtarın ortalama uzunluğu ilk dizinin yarısı kadardır. Gönderici ve alıcının her ikisinin de aynı tabanı kullanma olasılığı vardır bu nedenle anahtar dizisinin uzunluğu ilk durumun tam olarak yarısı kadardır.

Sonra gönderici yalnızca bitlerin serisi olarak alıcıya mesaj yazar ve rasgele mesaj oluşturduktan sonra paylaşılmış gizli anahtar eklerler. Klasik kanal içinden bu mesaj iletilir. Son olarak, alıcı anahtarı çıkarmakla mesajı çözer.

Şimdiye kadar foton iletiminde bilgi hırsızlıklarının olmadığı ideal durum incelenmiştir. Bilgi hırsızlığının olması durumu fakat iletişimin iyi olması halini inceleyelim. Bilgi hırsızının kuantum kanalını kestiği ve alıcıyla aynı ölçüm araç gereçlerine sahip olduğu varsayılsın. Bilgi hırsızının, göndericinin fotonlarını saptadığı ve yenisiyle değiştirip alıcıya yolladığı varsayıldığında, bigi hırsızı hataya neden olabilir. Bilgi hırsızının analizörünün tabanı göndericinin fotonlarının kutuplanma tabanıyla aynıysa, bilgi

hırsızı denk bir foton oluşturabilir. Bu durumda böyle olmasına karşın, göndericinin ve bilgi hırsızının tabanları aynı değilse, bilgi hırsızının denk foton oluşturma olasılığı $1/2$ dir. Bilgi hırsızının oluşturduğu foton göndericinin fotonuyla aynı kutuplanmaya sahip veya 90^{o} kaymış olabilir. Bu yolla bilgi hırsızı $1/4$ olasılıkla bir hataya neden olabilir. Bilgi hırsızının, göndericinin yolladığı fotonlardan şu sıralanışı elde ettiği varsayılsın [26]:

```
X++X++++X++XXX+++++++X+XXXX++XX+X+++X+XXX+X...
DVVAVVVVDVHADAVHVHHHAVAAADHHADHDVVVDHAADVD...
```

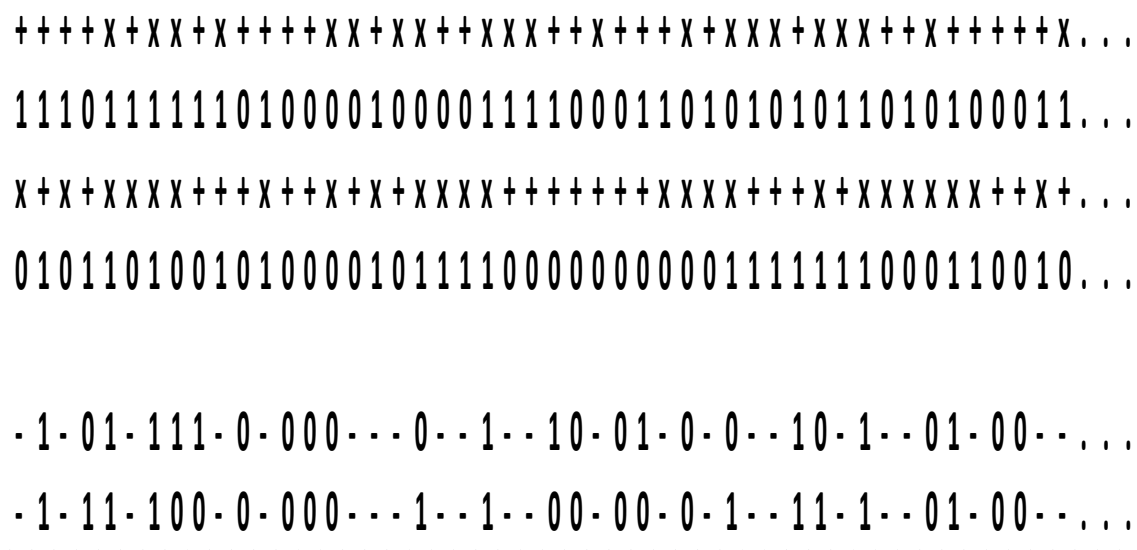
Şekil 3. 6 Bilgi hırsızının ölçüm yaptığı kutuplanma tabanı ve ölçtüğü kutuplanma durumlarının dizisi

Sonra, bilgi hırsızı ölçtüğü fotonları alıcıya yollar, alıcı analizörlerini kullanarak şu sıralanışı yazar [26]:

```
X+X+XXXX+++X++X+X+XXXX+++++++XXXX+++X+XXXXXX++X+...
DVDVADADHVHAHHDHAHAAAAHHHHHHHDDDAVVVAVADDDAAHHAH...
0101101001010000101111000000000011111110001100 10...
```

Şekil 3. 7 Alıcının bilgi hırsızının etkisinden sonra analizörden ölçtüğü dizi sıralanışı

Son olarak, gönderici ve alıcı anahtar elde etmek için taban dizilerini birbirlerine haber verirler.



Şekil 3. 8 Bilgi hırsızının etkisinin olduğu ve gönderici ve alıcının taban dizilerinin kıyaslanması

Şekil 3.8 de görüldüğü gibi, bilgi hırsızının neden olduğu hatalar görünür, durumların yaklaşık dörtte birinde gönderici ve alıcı, fotonları hazırlamak ve ölçmek için aynı tabanı kullandıkları halde anahtar dizisi çakışmaz. Benzer şekilde, artık kullanamayacakları bir anahtar parçasını ortaya koymakla bilgi hırsızının varlığını doğrulayabilirler. Uzunluğu N bit olan anahtarın bir parçası kurban edildiğinde, bilgi hırsızının etkilerinin farkedilmeme olasılığı $(3/4)^N$ dir.

Matematiksel olarak bu protokol şu şekilde açıklanabilir. Gönderici $(4+\delta)n$ rasgele klasik bitlerin herbirinin iki dizisi ile başlar: a ve b. Gönderici o zaman $(4+\delta)n$ kubitlerinin bir kütüğü olarak bu dizileri kodlar:

$$\left|\Psi\right\rangle = \bigotimes_{k=1}^{(4+\delta)n} \left|\Psi_{a_k b_k}\right\rangle . \tag{3.17}$$

Bu genel bir ifadedir ve burada a_k a nın, b_k ise b nin k. bitidir. Herbir kubit aşağıdaki dört durumdan birindedir [15].

$$\left|\Psi_{00}\right\rangle = \left|0\right\rangle \tag{3.18}$$

$$|\Psi_{10}\rangle = |1\rangle \tag{3.19}$$

$$|\Psi_{01}\rangle = \left(|0\rangle + |1\rangle\right)/\sqrt{2} \tag{3.20}$$

$$|\Psi_{11}\rangle = \left(|0\rangle - |1\rangle\right)/\sqrt{2} \tag{3.21}$$

Bu işlemin amacı X veya Z tabanında, b ile sınırlandırılmış olarak, a yı kodlamaktır. Dört durum birbirine dik olmadığından hiçbir ölçümün kesinlikle onları ayırtedemeyeceği açıktır. Gönderici daha sonra açık kuantum iletişim kanalı üzerinden alıcıya $|\Psi\rangle$ durumunu yollar. Alıcı da $\varepsilon|\Psi\rangle\langle\Psi|$ yi alır.

Burada ε, kanalın ve bilgi hırsızının etkilerinin birleşiminden kaynaklanan kuantum işlemini tanımlar. Alıcı daha sonra açık olarak bu gerçeği duyurur. Bu aşamada gönderici, alıcı ve bilgi hırsızının herbiri ayrı yoğunluk matrisleriyle tanımlanmış kendi durumlarına sahipler. Gönderici b yi açığa çıkarmadığından bilgi hırsızı iletişim kanalını gizli dinleyebilmek için hangi tabanı kullanması gerektiğini bilmez. Sadece tahmin edebilir ve tahmini yanlış olursa, o zaman alıcının alacağı durumu bozmuş olur. Daha da ötesi gerçekte ε gürültüsü kısmen bilgi hırsızının gizli dinlemesine ek olarak (zayıf bir kanal) çevreden kaynaklansaydı, bilgi hırsızının kanal üzerinde tam kontrol sağlamasına yardımcı olmazdı, bu yüzden bilgi hırsızı ε dan tamamen sorumludur. Tabi ki alıcı $\varepsilon|\Psi\rangle\langle\Psi|$ den herhangi bir bilgi alamaz. Çünkü alıcı b hakkında herhangi birşey bilmez. Buna rağmen, alıcı işleme devam edebilir ve X veya Z tabanında herbir kubiti ölçer. Alıcının ölçüm sonucu a' olsun. Daha sonra gönderici açıkça b yi duyurur ve bir açık kanal üzerinden karşılaştırarak, alıcı ve gönderici b' ve b ye karşılık gelen bitlerin eşit olduğu durumlar dışında $\{a', a\}$ daki kalan bitleri çöpe atarlar. Alıcının ölçtüğü bu bitler göndericinin hazırladığıyla aynı tabanda olduğundan, kalan bitler $a' = a$ yı sağlar. b nin alıcının ölçümünden kaynaklanan a ve a' bitlerinin her ikisi hakkında da hiçbir şey açığa çıkarmadığına dikkat edilmelidir. Fakat bunun şartı şudur: Alıcının, göndericinin yolladığı kubitleri aldığını bildirmesinden sonrasına kadar, göndericinin b yi ilan etmemesidir. Aşağıdaki izahta basitlik için, gönderici ve alıcı sonuçlarının yalnızca $2n$ bitini tutsun, eksponansiyel olarak yüksek olasılıkla δ yeterince büyük seçilebilir.

Gönderici ve alıcı iletişim esnasında ne kadar gürültü veya bilgi hırsızlığı olduğunu belirlemek için bazı testler uygularlar. Gönderici $2n$ bit içerisinden rasgele n bit seçer ve alenen seçimi anouns eder. Alıcı ve gönderici o zaman bu kontrol bitlerinin değerlerini yayınlarlar ve kıyaslarlar. t bitten daha fazlası uyuşmazsa o zaman iptal ederler ve protokolü başlangıçtan yeniden uygularlar. Test geçerse, t seçilir, sonra kalan n bitten makul olarak m, gizli paylaşılmış anahtar bitlerini elde etmek için bilgi uzlaştırma ve güvenlik artırma yöntemleri uygulanabilir.

Mucitlerinden sonra BB84 olarak bilinen protokol aşağıda özetlenilir [15]:

Gönderici bir rasgele $(4+\delta)n$-bit dizisi b yi seçer. Herbir bilgi bitini, b nin karşılık gelen biti sıfırsa $\{|0\rangle,|1\rangle\}$ veya bir ise $\{|+\rangle,|-\rangle\}$ olarak kodlar. Gönderici sonuçlanan durumu alıcıya yollar. Alıcı $(4+\delta)n$ kubiti alır, bu gerçeği ilan eder ve herbir kubiti rasgele olarak X veya Z tabanında ölçer. Gönderici b dizisini anouns eder. Gönderici ve alıcı, alıcının, göndericinin hazırladığından farklı bir tabanda ölçtüğü herhangi bitleri yok sayarlar. Yüksek olasılıkla en az $2n$ artık bit vardır (protokol durdurulmamışsa), $2n$ biti korurlar. Gönderici, bilgi hırsızının müdahalesi hakkında bir kontrol hizmeti verecek olan n bitin bir alt kümesini seçer ve alıcıya kendi seçtiği bitlerin hangi bitler olduğunu söyler. Gönderici ve alıcı n kontrol bitlerinin değerlerini ilan eder ve kıyaslarlar. Çıkan sonuçta kabul edilebilir sayıdan daha fazlası uyumsuzsa protokolü iptal ederler. Gönderici ve alıcı m paylaşılmış anahtar bitleri elde etmek için kalan n bite bilgi uzlaştırma ve güvenlik artırma uygularlar.

3.3.2 B92 Protokolü

BB84 protokolü diğer durumları ve bazları kullanmak için genellenebilir ve benzer sonuçlar alınabilir. Basit bir protokol, yalnızca iki durum kullanıldığında ortaya çıkar. Basitlik için, bir anda bir tek bite ne olduğunu gözönüne almak yeterlidir. Tanım şöyle yapılır: Klasik bir a bitinin hazırlandığı ve sonuca bağlı olarak alıcıya yollandığı varsayılır. Bit (3.22) ve (3.23) de görülen iki durumdan birindedir.

$$\Psi = |0\rangle \qquad a = 0 \tag{3.22}$$

$$\Psi = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \qquad a = 1 \tag{3.23}$$

Göndericinin ürettiği bir rasgele a' bitine bağlı olarak, alıcı sonuçta Z tabanında

$$|0\rangle, |1\rangle \qquad (a' = 0) \tag{3.24}$$

veya X tabanında

$$|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2} \qquad (a' = 1) \tag{3.25}$$

göndericiden aldığı kubiti ölçer. Ölçümünden X ve Z tabanının -1 ve $+1$ özdurumuna karşılık gelen, 0 veya 1 olan b sonucu elde edilir. Alıcı o zaman b yi açıkça ilan eder, fakat a' yü gizli tutar. Gönderici ve alıcı $b = 1$ için yalnızca $\{a, a'\}$ çiftlerini tutmakla, bir açık tartışma iletirler. $a = a'$ olduğunda, her zaman $b = 0$ olduğuna dikkat edilmelidir. Yalnızca $a' = 1 - a$ ise alıcı $b = 1$ i elde edecek ve bu durum $1/2$ olasılıkla meydana gelir. Son anahtar gönderici için a ve alıcı için $1 - a'$ olur [15].

B92 olarak bilinen bu protokol, dik olmayan durumlar arasındaki mükemmel ayrımın imkânsızlığının kuantum şifrelemenin kalbinde nasıl yattığını aydınlatır [15]. BB84 teki gibi, gönderici ve alıcının son olarak alıkoyduğu bitler arasındaki korelasyonu bozmaksızın göndericinin durumları arasını ayırtetmek herhangi bir gizli dinleyici için imkânsız olduğundan, bu protokol gönderici ve alıcıya, bir de iletişimleri esnasında gizli dinleme ve gürültüde bir üst sınır koyar ve ortak kullanılmış bitler için müsade eder.

Daha sonra, meydana gelen korelasyonlu rasgele bit dizilerinden gizli bitler elde etmek için bilgi uzlaştırma ve güvenlik artırma uygulanabilir [15].

3.3.3 EPR Protokolü

BB84 ve B92 protokollerinde, protokolün ürettiği anahtar bitler gönderici tarafından oluşturulmuş izlenemine neden olabilmektedir. Sonuçta, dolaşıklık özelliklerinin neden olduğu ve rasgele bir süreçten meydana geldiği görülebilen anahtar ortaya çıkmaktadır [15]. Bu aşağıdaki protokolle örneklenebilir. Gönderici ve alıcının

$$\left(|00\rangle + |11\rangle\right)/\sqrt{2} \tag{3.26}$$

durumundaki dolaşık kubit çiftlerinin bir kümesini paylaştıkları varsayılır. Bu durumlar EPR çiftleri olarak bilinirler. Bu durumların elde edilmesi çok farklı yollarla meydana gelmiş olabilir. Örneğin gönderici çiftler hazırlayabilir ve sonra herbirinin yarısını alıcıya yollayabilir. Alternatif olarak üçüncü kişi çiftler hazırlayabilir ve yarısın göndericiye ve diğer yarısını da alıcıya yollayabilir. Veya geçmişte onlar görüşüp bu bilgileri paylaşmışlar ve şimdiye kadar depolamışlardır. Gönderici ve alıcı o zaman EPR çiftlerinin rasgele bir alt kümesini seçerler ve onların Bell eşitsizliğini veya başka uygun doğruluk testini ihlal edip etmediğine bakarlar. Testin geçilmesi onların kalan EPR çiftlerinin doğruluğuna bir alt sınır koyar ve yeterince saf, dolaşık kuantum durumlarının düzenlenmesi için devam ettiğini bildirir. Ve onlar bunları eşlenik olarak belirlenmiş rasgele tabanlarda ölçtüğünde, gönderici ve alıcı, BB84 ve B92 protokollerinde olduğu gibi anahtar bitler elde edebilecekleri korelasyonlu klasik bit dizilerini elde ederler [15].

EPR protokolünde anahtar bitler şöyle elde edilir. Gönderici ve alıcı kubitlerine eş zamanlı olarak özdeş işler uygulasalar bile, protokol simetrik olduğundan gönderici ve alıcının her ikisinden birinin anahtar ürettiği söylenemez. EPR protokolüyle üretilen anahtar hakikaten rasgeledir. Gerçekte aynısını BB84 protokolü de uygular. Çünkü BB84 protokolü EPR protokolünün genelleştirilmiş sürümünün bir örneğine indirgenebilir [15]. Göndericinin rasgele bir klasik b biti hazırladığı ve ona göre, EPR çiftlerinin yarısını

$$|0\rangle, |1\rangle \tag{3.27}$$

veya

$$|\pm\rangle = \left(|0\rangle \pm |1\rangle\right)/\sqrt{2} \tag{3.28}$$

bazlarının birinde a yı hesaplamak için ölçtüğü düşünülür. Alıcı özdeş olarak aynı işlemleri yapar, b' tabanında ölçer ve a' yü elde eder. Şimdi onlar bir açık kanal üzerinden b ve b' ile iletişim kurarlar ve anahtar olarak $b = b'$ için yalnızca $\{a, a'\}$ leri tutarlar. Bu anahtarın, gönderici ve alıcının EPR çiftlerinin yarısına bir ölçüm uygulanıncaya kadar belirlenemeyeceğine dikkat edilsin. Benzer gözlemler B92 protokolü hakkında da yapılabilir. Bu sebepten kuantum şifreleme gizli anahtar değişimi veya transferi düşüncesi değil gizli anahtar üretimi düşüncesidir [15]. Ne gönderici ne de alıcı, protokolün sonuçlanmasıyla açığa çıkacak olan anahtarı önceden belirleyemezler.

BÖLÜM 4

SONUÇ VE ÖNERİLER

Bilgi iletiminde davranışları klasik fizikle açıklanabilen klasik nesneler yerine bireysel fotonlar gibi kuantum nesnelerinin kullanılması bilgi teknolojisinde kuantum fiziğinin özelliklerinin kullanılabilmesini de beraberinde getirir.

Kuantum bilgi zengin bilgi depolama hafızasına sahiptir. Kuantum fiziğinin temel özelliklerinden olan üst üste binme ilkesinin kullanımı kuantum bilgiyi klasik bilgiye göre çok daha zengin yapar.

Bilgi güvenliği açısından bilginin güvenli bir biçimde şifrelenmesi yine son derece önemlidir. Kuantum kopyalanamama teoreminin bilgi teorisine uygulanması kuantum bilginin bilgi hırsızları tarafından habersiz bir şekilde kopyalanamayacağı sonucunu verir.

İletişim teknolojisinde, bilgi iletiminde gizli mesaj kuantum nesneleriyle iletilmez. Onun yerine mesajı çözmeye yarayan anahtar kuantum nesneleriyle yollanılır. Bu sayede, bilgi hırsızı anahtarı ele geçirse, gönderici ve alıcı bunu farkeder. Gönderici ele geçirilmiş olan anahtarın çözebileceği mesajı yollamaz. Bunun sonucunda mesajın bilgi hırsızının eline geçmesi imkansız olur.

Ciddi anlamda güvenlik gerektiren anahtar iletimi durumlarında, açık anahtar şifreleme sistemleri kanıtlanabilir güvenliğe sahip olmaları nedeniyle kanıtlanabilir güvenliğe sahip olmayan gizli anahtar şifreleme sistemlerine tercih edilirler.

Bilgi iletişim teknolojisinde, iletilecek anahtarın üst düzey güvenliğinin sağlanması amacıyla kullanılan protokoller bilgi hırsızının anahtar iletimi esnasında elde edebileceği bilgiyi en alt seviyeye indirmeyi hedeflerler. Bu nedenle bu alanda yapılan

çalışmalar, bilgi hırsızının bilgi eldesi için kullanabileceği çeşitli saldırı tekniklerinin zararlarını en alt seviyeye indirmeyi hedeflemektedir[34-40].

KAYNAKLAR

[1] Gisin, N., Ribordy, G., Tittel, W. and et al., (2002), ‘’Quantum Cryptohraphy’’, Rev. Mod. Phys. , 74:145.

[2] Scarani, V., Acín A., Ribordy, G., and Gisin, N., (2004), “Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks forWeak Laser Pulse Implementations”, Phys. Rev. Lett., 92:057901.

[3] Acín, A., Gisin, N., and Scarani, V., (2004), “Coherent-pulse implementations of quantum cryptography protocols resistant to photon-number-splitting attacks”, Phys. Rev. A, 69: 012309.

[4] Shor, P. W. and Preskill, J., (2000), “Simple Proof of Security of the BB84 Quantum Key Distribution Protocol”, arXiv:quant-ph/0003004 v2

[5] Hirota, O., (2007), “Practical security analysis of a quantum stream cipher by the Yuen 2000 protocol”, Phys. Rev. A, 76:032307.

[6] Lau, H-K. and Lo, H-K., (2011) , “Insecurity of position-based quantum-cryptography protocols against entanglement attacks”, Phys. Rev. A, 83: 012322.

[7] Qin, S-J., Gao, F., Guo, F-Z., and Wen, Q-Y., (2010), “Comment on “Two-way protocols for quantum cryptography with a nonmaximally entangled qubit pair””, Phys. Rev. A, 82: 036301.

[8] Avella, A., Brida, G., Degiovanni, I. P., Genovese M., Gramegna, M., and Traina, P., 2010, “Experimental quantum-cryptography scheme based on orthogonal states”, Phys. Rev. A, 82: 062309.

[9] Lo, H-K., Curty, M., and Qi, B., (2012), “Measurement-Device-Independent Quantum Key Distribution”, Phys. Rev. Lett., 108:130503

[10] Ralph, T. C., (2000), “Security of Continuous-Variable Quantum Cryptography”, Phys. Rev. A, 62:062306

[11] C. H. Bennett and G. Brassard, (1984), “Quantum Cryptography: Public Key Distribution and Coin Tossing”, Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, IEEE press, 175.

[12] Ekert, A. K., (1991), “Quantum Cryptography Based on Bell's Theorem”, Phys. Rew. Lett., 67: 661-663.

[13] Bennett, C. H., (1992), “Quantum Cryptography Using Any Two Nonorthogonal States’’, Phys. Rev. Lett., 68: 3121–3124.

[14] Bellac, M. L., (2006), A Short Introduction to Quantum Information and Quantum Computation.

[15] Nielsen, M. A., Chuang, I. L., (2000), Quantum Computation and Quantum Information. Cambridge.

[16] Benenti, G., Casati, G., and Strini, G., (2004), Principle of Quantum Computation and Informatio, Volume 1. World Scientific.

[17] Sakurai, J. J., (1995), Modern Quantum Mechanics. Addison-Wesley, Reading, Mass.

[18] Feynman, R. P., Leighton, R. B., and Sands, M., (1965),The Feynman Lectures on Physics. Volume 3, Addison-Wesley, Reading, Mass.

[19] Cohen-Tannoudji, C., Diu, B., and Laloe, F., (1977), Quantum Mechanics, Vol. I. John Wiley and Sons, New York.

[20] Cohen-Tannoudji, C., Diu, B., and Laloe F., (1977),Quantum Mechanics, Vol. II. John Wiley and Sons, New York.

[21] Einsten, A., Podolsky, B., and Rosen, N., (1935), “Can Quantum-Mechanical Description of Physical Reality Be Considered Complete?”, Phys. Rev. Lett., 47.

[22] Bell, J. S., 1964, “On The Einstein Podolsky Rosen Paradox”, Physics 1(3): 195-200

[23] Horodecki, R., Horodecki, P., Horodecki, M., and Horodecki, K., (2009), “ Quantum entanglement”, Rev. Mod. Phys., 81.

[24] Wootters, W. K., and Zurek, W. H., (1982), “A Single Quantum State Can Not Be Cloned”, Nature (London) 299: 802.

[25] Kahn, D., (1996), Codebreakers: the Story of Secret Writing, Scribner, New York.

[26] Galindo, A., and Mart´ın-Delgado, M. A., (2002), “Information and computation: Classical and quantum aspects”, Rev. Mod. Phys., 74:347.

[27] C. E. Shannon, (1949), “Communication Theory of Secrecy Systems”, Bell System Technical Journal, 28: 656.

[28] Wiesner, S., (1983), “Conjugate Coding”, SIGACT News, 15(1):78-88

[29] Rivest, R., Shamir, A., and Adleman, L., (1991), “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of the ACM, 21:120.

[30] Vernam, G.S., (1926), “Cipher Printing Telegraph Systems For Secret Wire and Radio Telegraphic Communications”, J. Am. Inst. Electr. Eng., 45:109.

[31] Shor, P. S., (1995), “Algorithms for Quantum Computation: Discrete Logarithms and Factoring”, 35th Annual Symposium on Foundations of Computer Sciene, IEEE Press, Los Alamitos, CA.

[32] Diffie, W., and Helman, M., (1976), “New Directions in Cryptography”, IEEE Transaction on Information Theory, 22(6): 644-654.

[33] Rivest, R. L., Shamir, A., and Adleman, L., (1978), “A Method for Obtaining Digital Signatures and Public-Key Cryptosystems”, Communications of ACM, 21(2): 120-126.

[34] Brub, D., and Macchiavello, C., (2002), “Optimal Eavesdropping in Cryptography with Three-Dimensional Quantum States”, Phys. Rew. Lett., 88: 127901.

[35] Grosshans, F., and Cerf, N. J., (2004), “Continuous-Variable Quantum Cryptography is Secure against Non-Gaussian Attacks”, Phys. Rew. Lett., 92: 047905.

[36] Scarani, V., Acin, A., Ribordgy, G., and Gisin, N., (2004), “Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations”, Phys. Rew. Lett., 92: 057901.

[37] Navascues, M., Grosshans, F., and Acin, A., (2006), “Optimality of Gaussian Attacks in Continous-Variable Quantum Cryptography”, Phys. Rew. Lett., 97: 190502.

[38] Acin, A., Brunner, N., Gisin, N., Massar, S., Pironio, S., and Scarani, V., (2007), “Device-Independent Security of Quantum Cryptography against Collective Attacs”, Phys. Rew. Lett., 98: 230501.

[39] Sun, S-H., Jiang, M-S., and Liang L-M., (2012), “Single-photon-detection attacks on the phase-coding continuous-variable quantum cryptography”, Phys. Rew. A, 86:012305.

[40] Barett, J., Colbeck, R., and Kent, A., (2013), “Memory Attacks on Device-Independent Quantum Cryptography”, Phys. Rew. Lett., 110: 010503.

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Hüsnü KARA

Doğum Tarihi ve Yeri : 14.04.1987-Aksaray

Yabancı Dili : İngilizce

E-posta : hkara@yildiz.edu.tr

ÖĞRENİM DURUMU

Derece	Alan	Okul/Üniversite	Mezuniyet Yılı
Lisans	Fizik	İstanbul Üniversitesi	2009
Lise	Fen Bilimleri	Eyüp Anadolu Lisesi	2004

İŞ TECRÜBESİ

Yıl	Firma/Kurum	Görevi
2012-Devam	Yıldız Teknik Üniversitesi	Araştırma Görevlisi
2011-2012	Konya Necmettin Erbakan Üniversitesi	Araştırma Görevlisi
2010-2011	Hava Harp Okulu	Öğretim Görevlisi