Kuantum Kriptografi

Volkan Şenay

YÜKSEK LİSANS TEZİ

Fizik Anabilim Dalı

Haziran 2012

Quantum Cryptography

Volkan Şenay

MASTER OF SCIENCE THESIS

Department of Physics

June 2012

Kuantum Kriptografi

Volkan Şenay

Eskişehir Osmangazi Üniversitesi
Fen Bilimleri Enstitüsü
Lisansüstü Yönetmeliği Uyarınca
Fizik Anabilim Dalı
Genel Fizik Bilim Dalında
YÜKSEK LİSANS TEZİ
Olarak Hazırlanmıştır

Danışman: Prof. M. Selami Kılıçkaya

Haziran 2012

ONAY

Fizik Anabilim Dalı Yüksek Lisans öğrencisi Volkan Şenay'ın YÜKSEK LİSANS tezi olarak hazırladığı "Kuantum Kriptografi" başlıklı bu çalışma, jürimizce lisansüstü yönetmeliğin ilgili maddeleri uyarınca değerlendirilerek kabul edilmiştir.

Danışman: Prof. M. Selami KILIÇKAYA

Yüksek Lisans Tez Savunma Jürisi:

Üye: Prof. M. Selami KILIÇKAYA

Üye: Yrd. Doç. Dr. Ali ÇETİN

Üye: Yrd. Doç. Dr. Ercan UÇGUN

Üye: Yrd. Doç. Dr. Ömer ÖZBAŞ

Üye: Yrd. Doç. Dr. Salih KÖSE

Fen Bilimleri Enstitüsü Yönetim Kurulu'nun ..... tarih ve ..... sayılı kararıyla onaylanmıştır.

Prof. Dr. Nimetullah BURNAK

Enstitü Müdürü

ÖZET

Çalışmanın 1. Bölümde kriptoloji terimleri ve kriptolojinin tarihçesi verilmiş, çeşitli simetrik ve asimetrik şifreleme sistemleri tanıtılmış, bu sistemler içinde doğru uygulandığında kırılamayacağı 1949 yılında bir AT&T mühendisi olan Shannon tarafından teorik olarak da ispatlanmış olan Vernam Şifresi detaylı olarak incelenmiştir. Vernam şifreleme sisteminin sağladığı mutlak güvenlik tamamen rastgele seçilmiş tek kullanımlık anahtarın gizliliğine ve dağıtımının güvenliğine bağlıdır. Fakat prensip olarak, herhangi bir klasik özel kanal kullanıcılara izlenildiklerini fark ettirmeden pasif olarak takip edilebilir ve gizli kalması gereken anahtarın bir rakibin eline geçmesine fırsat verebilir. Bu noktada kuantum kriptografi anahtar dağıtım probleminin çözüldüğü, anahtarın güvenliğinin fizik kuralları ile korunduğu bir anahtar dağıtım tekniği olarak karşımıza çıkmaktadır. Klasik şifreleme sistemlerinin güvenlikleri bazı zor matematiksel problemlerin hesaplanabilme zorluğuna dayanırken, bu teknik kuantum mekaniğine dayanır. Kuantum mekaniğinin ilkelerine göre hatasız iletim hatlarında kaynaktan hedefe iletilmekte olan verinin bozulması arada istenmeyen biri tarafından verinin okunmaya çalışıldığı anlamına gelir. Bu avantajdan yararlanmak suretiyle kullanıcılar arasında eşit anahtar dizilerinin yüzde yüz güvenli biçimde paylaşılabilmesi için BB84, B92, SARG, Ekert protokolü gibi çeşitli anahtar dağıtım protokolleri öne sürülmüştür. Bu protokollerin prensiplerine 2. Bölümde yer verilmiştir.

Çalışmanın diğer bölümlerinde genel olarak 1989 yılında başarıyla gerçekleştirilen ilk kuantum anahtar dağıtımı denemesinden günümüze kadar yapılan ve bu alandaki gelişmelere öncülük eden çalışmalara göz atılmış, KAD sistemlerinde yer alan ışık kaynakları, dedektörler ve kuantum kanallar ile kanal kusurlarından kaynaklanan hataların düzeltilmesi ve anahtarın gizliliğinin artırımı için destekleyici işlemler hakkında bilgi verilmiş, 9. Bölümde kuantum kriptografinin güvenliğine değinilmiş, 10. ve son Bölümde ise kuantum kriptografinin geleceği, beklentiler ve ülkemiz açısından önemi tartışılmıştır.

Anahtar Kelimeler: Kuantum Kriptografi, Kuantum Anahtar Dağıtım Protokolleri, BB84, B92, SARG, Dolanıklık, Bell Eşitsizlikleri, Gizlilik Artırımı, Yan Kanallar.

SUMMARY

In the first part of this study cryptological terms and history of cryptology have been provided, various symmetrical and asymmetrical cryptographic systems have been defined and in these systems Vernam cipher theoretically proven by AT&T engineer Shannon that the system cannot be hacked if practiced properly has been examined in details. Absolute security provided by Vernam cryptographic system completely depends on randomly selected single use of the key's confidentiality and the security of its distribution. But principally any of the classic private channels can passively be eavesdropped without its notice and may give the opportunity to change hands for the key which should be kept confidential. Here the quantum cryptography appears us as a key distribution technique where the problem is solved and the security of the key has been protected by physical rules. Although the securities of the classical cryptographic systems are based on the complication of the calculation of some mathematical problems, this technique depends on quantum mechanics. Principles of quantum mechanics assert that the corruption of the data transferred to the target from accurate transmission lines imply that the data has been tried to be read by an eavesdropper. In order to share equal key indexes hundred percent safely among the users by benefiting from this advantage, various key distribution protocols set forth such as BB84, B92, SARG, Ekert. The principals of those protocols are allowed in the 2nd part of the study.

In the other parts of the study, in general, the studies following the achievement reached first in 1989 regarding key distribution experiment until today and the studies leading to the developments in this field have been looked through and information regarding light sources in QKD systems, detectors and quantum channels with the supporting procedures for correction of the errors originating from channel defects and privacy amplification have been provided, referred to quantum cryptography security in part 9 and the future of quantum cryptography, expectations and its importance regarding our country have been negotiated in tenth and the last part.

Key Words: Quantum Cryptography, Quantum Key Distribution Protocols, BB84, B92, SARG, Entanglement, Bell Inequalities, Privacy Amplification, Side Channels.

TEŞEKKÜR

Çalışmalarımın her aşamasında beni yönlendiren, bilimsel katkılarını ve tecrübelerini esirgemeyen tez danışmanım ve hocam ESOGÜ Fen-Edebiyat Fakültesi Fizik Bölüm Başkanı Sayın Prof. M. Selami KILIÇKAYA'ya en içten saygı ve teşekkürlerimi sunarım.

Yüksek Lisans Eğitimim süresince yardımlarını esirgemeyen ESOGÜ Fen-Edebiyat Fakültesi Fizik Bölümü Öğretim Üyelerinden Doç. Dr. Suat PAT'a, Bayburt Üniversitesi Öğretim Üyelerinden Eğitim Fakültesi Dekan Yardımcısı Yrd. Doç. Dr. Ramis BAYRAK'a ve İlköğretim Bölüm Başkanı Yrd. Doç. Dr. Hakan SÖYÜT'e teşekkür ederim.

Ayrıca hiçbir zaman sevgisini ve desteğini esirgemeyen sevgili eşim Burcu AYDEMİR ŞENAY'a ve bu günlere gelmemizde şüphesiz çok emekleri olan ailelerimize minnet duygularımı bildirmeyi ödemekten zevk duyduğum bir borç telakki ederim.

İÇİNDEKİLER

Sayfa

İÇİNDEKİLER

ŞEKİLLER DİZİNİ

ÇİZELGELER DİZİNİ

Çizelge **Sayfa**

KISALTMALAR VE SİMGELER DİZİNİ

Kısaltmalar		**Açıklama**
EİK	:	Elektronik İmza Kanunu
M.Ö.	:	Milattan önce
AT&T	:	American Telephone and Telegraph Company
XOR	:	eXclusive OR
RSA	:	Ron Rivest, Adi Shamir ve Leonard Adleman Şifre Sistemi
DES	:	Data Encryption Standard (Veri Şifreleme Standardı)
AES	:	Advanced Encryption Standard (Gelişmiş Şifreleme Standardı)
IBM	:	International Business Machines
ABD	:	Amerika Birleşik Devletleri
CPU	:	Central Processing Unit (Merkezi İşlem Birimi)
ATM	:	Automated Teller Machine (Bankamatik)
OTP	:	One Time Pad (Tek Kullanımlık Şifre)
KAD	:	Kuantum Anahtar Dağıtımı
h	:	Planck sabiti
λ	:	Dalgaboyu
Kübit	:	Bir biti temsil eden kutuplanmış foton
$\|H\rangle$	:	Yatay polarizasyon durumu
$\|V\rangle$	:	Dikey polarizasyon durumu
$\|A\rangle$	:	Anti-diyagonal polarizasyon durumu
$\|D\rangle$	:	Diyagonal polarizasyon durumu
BB84	:	Bennett ve Brassard (1984) Protokolü
B92	:	Bennett (1992) Protokolü
SARG	:	Scarani, Acin, Ribordy ve Gisin Protokolü
PNS	:	Photon Number Splitting Attack (Foton Sayısı Bölme Saldırısı)
η	:	Geçirgenlik
μ	:	Ortalama foton sayısı
LED	:	Light Emitting Diode (Işık Yayan Diyot)
km	:	Kilometre (10^3 m)

nm	:	Nanometre (10^{-9} m)
μm	:	Mikrometre (10^{-6} m)
$\emptyset_A$	:	Alice'in faz kayma açısı
$\emptyset_B$	:	Bob'un faz kayma açısı
L	:	Mach-Zehnder interferometresinin uzun kolu
S	:	Mach-Zehnder interferometresinin kısa kolu
BBO	:	Beta-Baryum Borat
Nd-YAG	:	Neodyum Yitriyum-Aluminyum-Garnet
$KNbO_3$	:	Potasyum Niyobat
Si-APD	:	Silikon çığ fotodiyot
γ	:	Foton frekansı
p_{multi}	:	Çoklu foton olasılığı
$p(1)$	:	Tek foton olasılığı
$p(0)$	:	Boş durum olasılığı
KPAD	:	Kendiliğinden Parametrik Alt Dönüştürme
GaAs	:	Galyum Arsenid
GaAlAs	:	Galyum Alüminyum Arsenik
InP	:	İndiyum Fosfat
K	:	Kelvin
m	:	Metre
$LiIO_3$	:	Lityum İodat
$LiNbO_3$	:	Lityum Niyobat
β-BaB_2O_4	:	Baryum Beta Borat
APD	:	Çığ fotodiyot
MHz	:	Megahertz (10^6 hertz)
^0C	:	Santigrat derece
InGaAs	:	İndiyum Galyum Arsenik
kHz	:	Kilohertz (10^3 hertz)
InAs	:	İndiyum Arsenik
s	:	Saniye
GHz	:	Gigahertz (10^9 hertz)

dB	:	Desibel
ϵ	:	Elenmiş anahtarda bit-hata oranı
$\oplus$	:	XOR işlemi
KDA	:	Kesin Durum Ayırma Saldırısı

1. GİRİŞ

Elektronik iletişimin ve veri aktarımının modern toplumun temel ihtiyaçlarından biri haline gelmiş olduğuna şüphe yoktur. Bilgi çağı olarak anılmakta olan çağımızda ülkelerin ve kişilerin değerli varlıkları artık bilgisayarlarda depolanan ve elektronik ağlarda taşınan verilerden ibarettir. Bu tip verilere askeri amaçlı bilgiler, banka hesapları, devletlerin ve ticari kuruluşların gizli bilgileri gibi pek çok farklı örnek verilebilir (Dereli vd., 2009). Bu denli önemli verilerin aktarımını ve güvenlik açısından zaafa meydan vermeden saklanmasını güvenceye almak açısından yeni metot ve teknikler geliştirilmesi gerekmektedir. Kriptolojinin hedefi de budur. Etimolojik olarak Yunanca gizli veya sır anlamına gelen "kruptos" ile bilim anlamındaki "logia" kelimelerinden türetilmiş olan kriptoloji, genel olarak mesajların gizliliklerinin, gerçekliklerinin, bütünlüklerinin korunmasını ve inkar edilmemelerini garantiye almak amacıyla şifrelenmesi ve deşifre edilmesi ile ilgilenen bilim dalı olarak tanımlanabilir. Kriptografi –ki Türkçesi şifre yazımı olarak bilinmektedir-, şifre kırma sanatı kriptanaliz alanını da içine alan kriptoloji biliminin bir dalıdır. Bir başka deyişle kriptografi ve kriptanaliz birlikte kriptolojiyi oluştururlar.

Bir kriptografik algoritma, şifreleme ve deşifreleme için kullanılan matematiksel fonksiyonlardan oluşur. Şifreleme ve deşifreleme işlemlerinde ayrıca, bir anahtar değeri kullanılmaktadır (Nabiyev ve Günay, 2006). Bilindiği gibi pek çok şifreleme algoritmasının tanımını ve gerçeklemelerini İnternette, kitaplarda, dergilerde ve diğer herkese açık ortamlarda bulmak mümkündür. O halde gizlilik artık kullanılan algoritmaya bağlı değildir. Yeterince güçlü olan günümüz algoritmalarında kullanılan anahtarların gizliliğine ve dağıtımının güvenliğine bağlıdır. Kuantum kriptografi, anahtar dağıtım probleminin çözüldüğü, anahtarın fizik kuralları ile korunduğu bir kriptografi tekniğidir. Yani Kuantum kriptografi aslında bir anahtar dağıtım yöntemidir (Toyran, 2003). Kuantum kriptografinin bilinen matematiksel temellere dayalı klasik yöntemlerden farkı kesin ve değişmez olan doğa/fizik yasalarını kullanıyor olmasıdır (Toyran, 2006).

1.1. KRİPTOGRAFİK GÖREVLER

Bilginin güvenli bir şekilde elektronik olarak iki taraf arasında iletilmesi için iletim kanalından bağımsız olarak; gizlilik, bütünlük, kimlik doğrulama ve reddedilmezlik şeklinde sayılabilecek güvenlik kriterlerinin sağlanması gerekmektedir.

1.1.1. Gizlilik (Privacy\Confidentiality)

Elektronik veri iletiminde gönderilen mesajlar başkaları tarafından öğrenilemeyecek şekilde şifrelenerek anlaşılmaz bir hale getirilir. Mesajı alan kullanıcı aynı algoritmayı kullanarak mesajı deşifre eder (Özler, 2007). Burada amaç, iki kullanıcının iletişimlerini üçüncü bir kişinin anlayamayacağı bir şekle dönüştürmek, aynı zamanda iki yasal kullanıcı için de anlaşılabilir kalmasını sağlamaktır.

1.1.2. Bütünlük (Integrity)

Yasal kullanıcılar arasında iletilen mesajın içeriğinde istenmeyen biri tarafından ekleme ya da çıkarma yapılıp yapılmadığını ifade eder. Veri bütünlüğü olarak da tanımlanmaktadır. Şifrelenen mesajın bir başkası tarafından ele geçirilmesi durumunda saldırgan mesajın içeriğini bilmediği için değişiklik yapamayacaktır. Değişiklik yapsa dahi yeni mesaj anlamsız olacağı için bütünlüğe zarar verildiği anlaşılacaktır (Özler, 2007).

1.1.3. Kimlik Doğrulama (Authentication\Identification)

Kriptografik protokollerde kimlik tanımlama (identification) ve kimlik doğrulama (authentication) yapılır ("RFID Mahremiyet Protokolleri Raporu", 2009). Alınan bir mesajın kimden geldiğinin kanıtlanması gerekmektedir. Bu amaca yönelik kimlik doğrulama, bir sisteme kişinin kimliğinin tanıtılmasından sonra sistem tarafından kişinin kimliğinin tespit edilmesi işlemidir. Kimlik doğrulaması ihlalini ortadan kaldırmak ve gerekli tedbirleri almak için genellikle özetleme algoritmaları, mesaj özetleri, elektronik imzalar ve sertifikalar kullanılmaktadır (Özler, 2007).

Elektronik İmza: 5070 sayılı Elektronik İmza Kanunu'nda (EİK) yer alan şekliyle e-imza; başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veriyi tanımlar. E-imza; bir bilginin üçüncü tarafların erişimine kapalı bir ortamda, bütünlüğü bozulmadan (bilgiyi ileten tarafın oluşturduğu orijinal haliyle) ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlarla garanti eden harf, karakter veya sembollerden oluşur.

Arıkan'a (1999) göre e-imza, ıslak imzanın fonksiyonlarını da kapsayan ve bir veri mesajında bulunan veya ona eklenen ya da mesaj ile mantıksal bağlantısı kurulabilen, bireyin kimliğini tanıtan ve bireyin, mesajın içeriğini onayladığını gösteren elektronik formattaki imzadır.

1.1.4. Reddedilmezlik (Non-repudation)

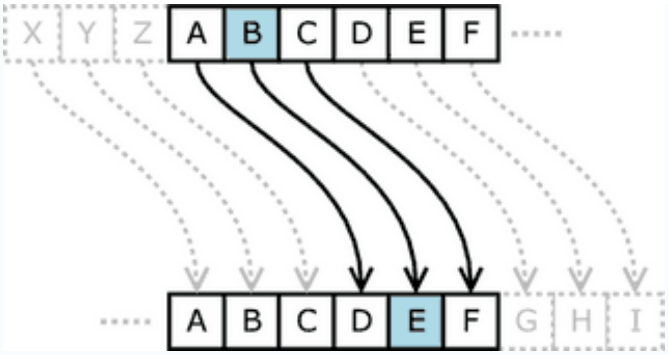
Karşılıklı haberleşmede tarafların birbirinden gelen mesajları aldığını ya da gönderdiğini inkar etmemesi gerekir. Bunu sağlamak için, mesajı gönderen ve alan kişilerin kayıtları güvenilir bir makam tarafından tutulur veya güvenli haberleşmenin yapılabilmesi için uygulanan yaklaşımlar ile inkar edemezlik sağlanır (Sağıroğlu ve Alkan, 2005).

1.2. TARİHTE KRİPTOGRAFİ

Kriptografi çok eski çağlardan beri insanoğlu tarafından kullanılmaktadır. Kripto tarihçisi David Kahn (1967), arkeolojik kazıların kriptografinin değişik tiplerinin Mezopotamya, Hindistan ve Çin'deki tarihi uygarlıklar tarafından bile kullanılmış olduğunu ortaya çıkardığından bahsetmektedir. Örneğin dört bin yıl önce Eski Mısırlılar mesajlarını gizlemek için standart dışı hiyeroglifler kullanmışlardır. Homeros tarafından M.Ö. 7. ya da 8. Yüzyılda yazıldığı düşünülen İlyada destanında da Argolis Kralı Proteus'un Lycia'ya katlanmış bir tablet üzerine kodlanmış semboller ile yazılmış bir mesaj yolladığından bahsedilmektedir (Dusek, et al., 2006).

M.Ö. 5. Yüzyılda Yunanistan'da Spartalılar harflerin yer değiştirmesi temeline dayalı "skytale" denilen kripto aletini tasarladılar. Bu alet belli kalınlıkta bir tahta silindirden ve silindirin etrafına eğik biçimde sarılmış papirüs ya da ince deri bir şeritten oluşuyordu. Gizli mesaj silindir boyunca silindire sarılı şerit üzerine yazılıyor, daha sonra şerit silindirden çözülüyordu. Birbirinden ayrılan harfler yeniden aynı kalınlıkta bir tahta silindire sarılmadıkça hiçbir anlam ifade etmiyordu (Babaoğlu, 2009). Günümüzdeki modern kripto tekniklerine bir benzetme yapılacak olunursa, silindirin çap değeri kriptografik anahtara denk gelmektedir.

Şekil 1.1 Günümüze uyarlanmış Skytale tekniğinin kullanımına dair bir örnek.



Şekil 1.2 Üç harf kaydırmalı Sezar şifresi.

Bir başka çok tutulan ve kolay yöntem de yerine kullanma yöntemidir. Bu yöntemde mesajın her harfi başka bir harf, rakam veya sembolle değiştirilir. Buna bir örnek Sezar şifresidir (Stinson, 1995). Roma İmparatorluğu'nun her yerine dağılmış olan Roma lejyonları arasında iletişim kurabilmek için Jül Sezar bir mesajın her harfinin alfabede kendisinden sonraki üçüncü harfle temsil edildiği bir şifre kullandı. Bu sistemde A, D ile, B, E ile, F, I ile yer değiştiriyordu (Şekil 1.2).

Ortaçağda çoğu kripto sistemi takdim-tehir, yerine koyma veya ikisinin birleşiminden oluşmaktaydı (Leary, 1996). Fakat bu yöntemlerin ikisi de güvenli değildir. Çünkü her ikisini de dilin bazı karakteristik özelliklerini, örneğin bazı harflerin ve onların kümelerinin sıklıklarını kullanarak çözmek mümkün olmaktadır.

Harf	Olasılık(%)	Harf	Olasılık(%)
A	11.68	N	7.23
B	2.95	O	2.45
C	0.97	Ö	0.87
Ç	1.26	P	0.79
D	4.87	R	6.95
E	9.01	S	2.95
F	0.44	Ş	1.94
G	1.34	T	3.09
Ğ	1.13	U	3.43
H	1.14	Ü	1.99
I	8.27	V	0.98
İ	5.20	Y	3.37
J	0.01	Z	1.50
K	4.71		
L	5.75		
M	3.74		

Tablo 1.1 Türk alfabesindeki harflerin kullanım sıklıkları (Arda vd., 2005).

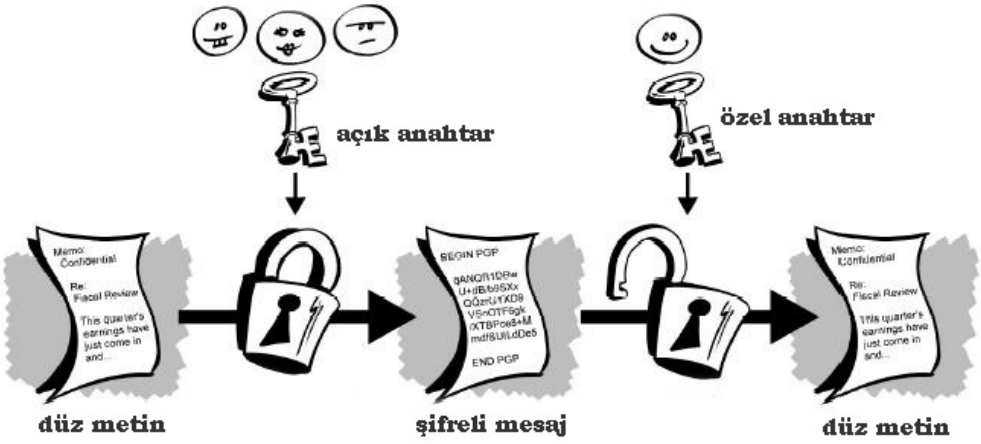
1830'larda telgrafın icadı insanlar arasındaki iletişimi ciddi ölçüde kolaylaştırdı. Buna rağmen modern iletişimin atası sayılan bu yöntem bakıldığında kriptografik açıdan önemli bir kusura sahipti; iletilen mesajın içeriği telgraf operatörünün bilgisi dahilindeydi. Bunun sonucu olarak iletişimlerini gizli tutmak isteyen kişi ve kuruluşlar tarafından çeşitli kod rehberleri tasarlandı. Bu kod rehberleri belirli kelime ve cümleleri kısa, anlamsız kelimelere dönüştürüyordu. Kodlar iki amaca hizmet ediyorlardı: İlk olarak mesajın boyutunu azaltıyorlardı ve dolayısıyla maliyeti düşürüyorlardı zira telgraflar her iletilen harf başına ücretlendiriliyordu. İkincisi eğer kod rehberi gizli tutulursa kodlar şifre haline geliyorlardı (Dusek, et al., 2006).

20. yüzyıldaki iki dünya savaşı yeni kriptografik tekniklerin gelişimini hızlandırdı. Kriptograflar şifreleme ve çözme algoritmalarının herkes tarafından bilinebileceği fakat mesajın gizliliğinin bazı gizli bilgilerle yani kullanıcılar arasında paylaşılan kriptografik anahtarla sağlanabildiği bir sistem tasarlamaya çalışıyorlardı. 1918'de bir AT&T mühendisi olan Gilbert S. Vernam'ın önerdiği tek kullanımlık şifre (one time pad) yönteminin, 1949'da başka bir AT&T mühendisi Shannon tarafından şartsız güvenlik sağladığı ispatlanmıştır (Boyacı ve Kara, 2009). Bu yöntemde tek bir kez kullanılmak üzere mesaj uzunluğuna eşit veya daha uzun, tümüyle rastsal bir anahtar seçilir. Anahtar, ikili sayı düzeninde düşünülen mesaj ile XOR'lanır. Ancak bu sistem birçok uygulama için oldukça kullanışsızdır. Çünkü her bir kullanım için en az mesaj uzunluğunda olan anahtarın haberleşme öncesi her iki tarafa da güvenli biçimde ulaştırılması gerekmektedir (Yerlikaya vd., 2006). Vernam şifresi ve anahtar dağıtım probleminden daha sonra Bölüm 1.5'te tekrar detaylı olarak bahsedilecektir.

1918'de Arthur Scherbius "Enigma" adında dahiyane bir şifre makinesi icat etti ve bir yıl sonra da icadını patent altına aldı (Deavours and Kruh, 1985). Enigma yaklaşık 10 kg ağırlığında, daktilo benzeri, rotorlu, elektromekanik bir şifreleme cihazı olmakla birlikte çok karmaşık bir yerine koyma şifresi uygulamaktaydı. Bazı geliştirmelerden sonra ilk olarak, o dönemki adı "Kriegsmarine" olan Alman donanması Enigma kullanmaya başladı. Ardından 1930'lu yılların başlarında Alman Gizli Servisi Abwehr, Alman Kara Kuvvetleri Wehrmacht ve Alman Hava Kuvvetleri Luftwaffe kendi birimlerinde gizli haberleşme için Enigma'yı kullanma kararı aldılar. Enigma II. Dünya Savaşı sırasında Alman ordusunun en yaygın kullandığı şifreleme cihazı oldu. Savaş sonunda ordunun envanterinde kayıtlı yaklaşık yüz bin Enigma vardı (Kara, 2009). Askeri Enigmanın potansiyel anahtarlarının sayıca çokluğu savaş sırasında Bletchley Parkta Enigma şifrelerini çözmekle görevli İngiliz Matematikçi Alan Turing'in ilk elektronik bilgisayarı imal etmesini sağladı. Günümüzde Pentium işlemcili bir bilgisayar Enigma tarafından şifrelenmiş bir mesajı dakikalar içerisinde çözebilmektedir.

1.3. ASİMETRİK ŞİFRELEME (AÇIK ANAHTARLI KRİPTOGRAFİ)

Whitfield Diffie ve Martin Hellman tarafından 1976 yılında geliştirilen açık anahtarlı kriptografi tek anahtar kullanan simetrik şifreleme algoritmalarının yerine iki ayrı anahtarın asimetrik kullanımını öngörmektedir. Bu anahtarlardan biri "açık anahtar" diğeri ise "özel anahtar" olarak adlandırılır. Açık anahtar ve özel anahtar bir çift oluştururlar. Alıcı açık anahtarını açık hale getirir ve özel anahtarını yalnızca kendisinde olmasını sağlamak amacıyla saklar. Algoritma öyle bir şekilde tasarlanmıştır ki herkes açık anahtarı kullanarak bir mesaj üretebilir fakat yalnız yasal alıcı kendi özel anahtarını kullanmak suretiyle mesajın şifresini çözebilir.



Şekil 1.3 Asimetrik şifreleme sistemi (Yıldırım, 2006).

Simetrik şifreleme algoritmalarının aksine asimetrik şifreleme algoritmalarında güvenli bir anahtar değişimi ihtiyacı bulunmamaktadır. Çünkü güvenlik tek yönlü fonksiyonlara dayandırılmaktadır. Bu tip fonksiyonların kendisinin hesaplanması kolay, tersinin hesaplanması imkansızdır. İmkansızdan kasıt, fonksiyonun tersinin hesaplanmasının makul bir süre içerisinde imkansız olmasıdır. Yani ne kadar büyük olurlarsa olsunlar iki asal sayıyı kağıt üzerinde olmasa bile hesap makinesi veya bilgisayar kullanarak çarpmak basittir. Fakat çok büyük bir sayıyı asal çarpanlarına ayırmak, çok güçlü bilgisayarlar ile de olsa çözülmesi güç bir matematik problemine dönüşür (Turgut, 2003a).

Ancak önemle belirtilmelidir ki, hiçbir tek yönlü fonksiyonun tek yönlü olduğu veya ters alma işlemini hızlandıracak yöntemlerin var olmadığı henüz ispatlanmış değildir.

Bugün en yaygın olarak kullanılan açık anahtar sistemi RSA kripto sistemidir. 1977 yılında Ronald Rivest, Adi Shamir ve Leonard Adleman'ın geliştirdiği bu şifreleme sistemi gücünü büyük sayıların çarpanlarına ayrılması problemindeki inanılmaz zorluktan almaktadır. Sistemin temeli ünlü matematikçi Euler'in modüler aritmetikte bulduğu çok eski bir bağıntıya dayanmaktadır (Turgut, 2003a).

Totient Fonksiyonu: Totient sayılar teorisinde, bir tam sayının o sayıdan daha küçük ve o sayı ile aralarında asal olan sayı sayısını belirten fonksiyondur. Bu fonksiyon, İsveçli matematikçi Leonhard Euler tarafından bulunmuştur. Totient fonksiyonu RSA kripto sisteminde kilit rol oynamaktadır.

Algoritma:	**Örnek:**
İki asal p ve q sayısı seçilir.	$p = 11$ ve $q = 13$.
Mod alınacak değer hesaplanır $n = p \times q$.	$n = 11 \times 13 = 143$.
Totient fonksiyonu uygulanır $t = (p-1)(q-1)$.	$t = (11-1)(13-1) = 120$.
t değeri ile en büyük ortak böleni 1 olan bir e değeri bulunur.	$e = 7$'dir. ($7 < 120$, 7 ve 120'nin en büyük ortak böleni 1'dir.)
$e \times d = 1$ Mod t olacak şekilde d değeri hesaplanır.	$7 \times d = 1$ Mod 120 $\Rightarrow$ d = 103'tür. Çünkü: $7 \times 103 = 721 = 1$ Mod 120
Açık Anahtar (e, n),	Açık Anahtar $(7, 143)$,
Özel Anahtar (d, n)'dir.	Özel Anahtar $(103, 143)$'tür.
Düz Metin Türk alfabesinin 5. harfi olan, D olsun,	Düz Metin, $D = 5$ ise,
Şifreli Metin = $C = D\text{^}e$ Mod n olur.	Şifreli Metin: $C = 5\text{^}7$ Mod $143 = 47$ olur.

Şifre çözme işlemi için,

Düz Metin, $C\text{^}d$ Mod $n = (D\text{^}e)\text{^}d$ Mod $n = D$.

Düz Metin:

$47\text{^}103$ Mod 143

$47\text{^}103 = (5\text{^}7)\text{^}103$

$= 5\text{^}721 = 5 \times [5\text{^}720]$

$= 5 \times [(5\text{^}120)\text{^}6]$

$= 5 \times [\ 1\text{^}6] = 5.$

$5\text{^}120 = 5\text{^}t = 1$ Mod 143

(Euler teoremi) veya,

daha basitçe,

$x\text{^}(e \times d) = x$; bu sebepten,

$5\text{^}721 = 5$'tir (Kodaz, 2003).

Yukarıda bir RSA kripto sistemi ile kurulacak iletişimin algoritması verilmiş ve küçük rakamlarla pratik bir uygulaması örneklenmiştir. Bu örnek, RSA sisteminin çalışma prensibini açıklamak bakımından faydalı fakat güvenliği çok zayıf bir örnektir. Gerçek hayatta bu yöntem ile şifrelenecek, önem arz eden bir mesajın güvende sayılabilmesi için p ve q sayılarının çok daha büyük seçilmesi gerekmektedir.

Bu yöntemle daha önce hiç karşılaşmamış, birbirini tanımayan kişiler bile birbirlerine gizli mesajlar gönderebilir. Örneğin İnternet'ten alışveriş yapan birisi kendisini hiçbir şekilde tanımayan bir web sitesine girerek sitenin kamuya açık anahtarını alır ve kart numarasını bu anahtarla şifreleyerek gönderir. Şifreli bilgiyi gönderen dahil hiç kimse çözemez, sadece web sitesinde bulunan gizli anahtarla gelen kart numarasını web sitesi çözebilir. Böylece kart hamili kart numarasının başkası tarafından okunmayacağından emin olacaktır (Yerlikaya vd., 2006).

425 bitlik bir RSA anahtarını (425 bitlik bir RSA anahtarı 129 basamaklı bir sayıya tekabül etmektedir) kırmak üzerine ilk yarışma Scientific American dergisinde 1977'de -ki Ronald Rivest, o tarihte bilinen en iyi algoritmalarla, iki 63 basamaklı asal sayının çarpımı olan 125 basamaklı bir sayıyı çarpanlarına ayırmak için en azından 40×10^{15} yıl gerekeceğini hesaplamıştı- yayınlandı.

N = 114, 381, 625, 757, 383, 867, 669, 235, 779, 976, 146, 612, 010, 218, 296, 721, 242, 362, 562, 561, 842, 935, 706, 935, 245, 733, 897, 830, 597, 123, 563, 958, 705, 058, 989, 075, 147, 599, 290, 026, 879, 543, 541

Martin Gardner'ın Ağustos 1977'de dergide yayınladığı düz metni "the magic words are squeamish ossifrage" olan 129 basamaklı yukarıdaki mesaj 600 kişilik bir ekibin sekiz aylık çalışması sonucunda Nisan 1996'da çözüldü (Yıldırım, 2006).

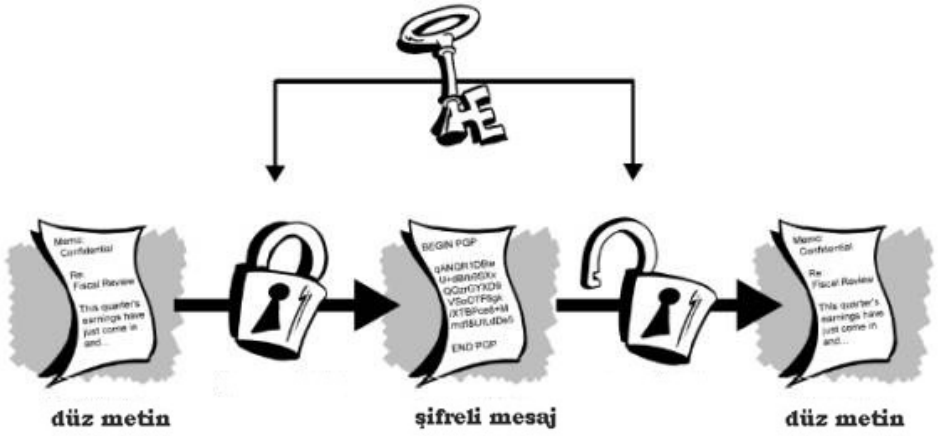
Şubat 1999'da ise 425 bitlik bir RSA modülüsünü 9 haftada çarpanlarına ayırmak için yalnızca 185 bilgisayar yetmişti. O yıllarda, internet üzerindeki e-ticaretin % 95'i 512 bitlik (155 basamaklı sayı) anahtarlarla korunmaktaydı. Ağustos 1999'da, 512 bitlik bir sayı 292 bilgisayar tarafından çarpanlarına ayrıldı. Bu, 512 bitlik anahtarların da kısa süreli güvenlik ihtiyacı dışında durumlarda güvenlik sağlayamayacağı anlamına gelmekteydi. Tüm bu saldırılar, dışarıdan çabalarla belli boyutlardaki anahtarların kırılması için ne kadar çaba harcanması gerektiğini ve bunun ne kadar bütçeyle yapılabileceğinin anlaşılmasını sağladı (Dusek, et al., 2006).

Çok büyük tam sayıları çarpanlarına ayırmak için tek yol bilgisayar ağları değildir. 1999'da Adi Shamir'in önerdiği TWINKLE aygıtı 512 ve 768 bitlik anahtarları çarpanlarına ayırmayı kolaylaştıran bir paralel optoelektronik çarpanlarına ayırma aygıtıydı (Dusek, et al., 2006). Günümüz koşullarında RSA kriptosistemi 1024-4096 bitlik anahtar uzunluklarında kullanılmaktadır (Hışıl, 2005).

Açık anahtar kriptografisine karşı bir diğer tehdit de kuantum bilgisayarlardır. Tek kuantum bilgisayar kullanılarak yapılacak olan şifre çözme işlemi, şifreleme işleminin aldığı kadar zaman alacak ve dolayısıyla açık anahtar kriptografisini değersiz kılacaktır. Bir kuantum bilgisayarının böylesi şifreleri çok kolay çözebileceğini Peter Shor'un 1994'te yayınlanan kuantum bilgisayarlar için geliştirdiği tam sayıları asal çarpanlarına ayırma algoritması göstermiş oldu. Küçük ölçekli kuantum bilgisayarlarla günümüzde yapılan ilk deneyler daha sofistike aygıtların yolunu açacak gibi görünmektedir (Vandersypen, et al., 2001).

1.4. SİMETRİK ŞİFRELEME (GİZLİ ANAHTARLI KRİPTOGRAFİ)

Simetrik şifrelemede, şifreleme ve şifre çözme için tek bir anahtar kullanılır. Gönderici mesajı bir anahtarla şifrelerken, alıcı da aynı anahtarı kullanarak şifreyi çözer. Alıcı ve göndericinin bu sistemi kullanarak güvenli bir şekilde haberleşmesi için bir anahtar üzerinde anlaşmaları ve bu anahtarı gizli tutmaları gerekmektedir. Eğer bu kişiler farklı yerlerde bulunuyorlarsa iletim kanalının, anahtarın gizliliğinin korunması açısından yeterli güvenilirlikte olması gerekmektedir. Çünkü anahtarı ele geçirecek herhangi bir kimse şifreyi kolayca çözebilir.



Şekil 1.4 Simetrik şifreleme sistemi (Yıldırım, 2006).

Anahtarların üretimi, iletimi ve saklanması "anahtar yönetimi" olarak adlandırılır. Tüm şifreleme sistemleri anahtar yönetimi sorunlarıyla uğraşmak durumundadır. Fakat anahtarın mutlaka gizli kalmasını gerektirdiğinden dolayı, simetrik şifreleme, anahtar yönetiminde kullanıcılara oldukça sıkıntı yaşatmaktadır (Aksuoğlu, 2010).

Simetrik bir algoritmanın kullanıldığı, n kullanıcılı sistemde her üyeye $n-1$ tane anahtar verilir. Buradan hareketle sistemde gizli tutulması gereken anahtar sayısı $[n.(n-1)]/2$'dir. Saklanması gereken anahtar sayısının çokluğundan dolayı çok kullanıcılı ortamlarda asimetrik şifreleme sistemleri uygun çözümdür (Aksuoğlu, 2010).

DES, Blowfish, Twofish, AES, CAST128, RC5 bazı simetrik şifreleme algoritmalardır. Bu algoritmaların en büyük avantajı kolay (hızlı) uygulanabilir ve güvenli anahtar dağıtımı problemi dışında son derece güvenli olmalarıdır.

Dünyada en yaygın gizli anahtar kripto sistemi, veri şifreleme standardı (DES) ve onun versiyonlarıdır. 1975'de IBM ve ABD hükümeti işbirliği ile geliştirilen DES, o tarihten bu yana kendisini kriptanalize karşı dikkate değer bir şekilde korumuştur. DES bir blok şifre örneğidir. Sabit uzunlukta bir metin dizinini alır ve onu bir seri uygulama ile aynı uzunlukta başka bir şifre metnine dönüştürür. DES 64 bitlik mesaj gruplarıyla çalışır. Yani mesaj 64 bitten az ise onu eklediği 0'larla 64 bite tamamlar. Eğer mesaj 64 bitten fazla ise mesaj girdisini 64 bitlik bloklara ayırır ve her birine şifreleme işlemi uygular (Yıldırım, 2006). DES algoritması şifrelenecek metni 64 bitlik bloklar halinde şifreler, kullandığı anahtar ise yine 64 bittir (Çetin, 2006).

Açık anahtar kripto sistemleri gibi DES de benzer bir takım atak dalgalarına muhatap olmuştur. DES algoritmasının en büyük zaafı 2^{56} adetlik anahtar uzayı genişliğidir. Bu gerçekten de güçlü bir şifreleme algoritması için oldukça küçük bir anahtar uzayı miktarıdır (Sakallı, 2006). 1997 yılında RSA Veri Güvenlik Şirketi, DES tarafından şifrelenmiş bir metnin çözülmesi için yarışma düzenledi. Şifreli metnin çözülmesi 96 gün sürdü. Araştırmacılar çok sayıda bilgisayar kullanarak 2^{56} muhtemel anahtarın tümünü deneyerek tabiri caizse kaba kuvvet kullandılar (Wiener, 1997). Ocak 1998'de yeni bir yarışmada 50.000 den fazla CPU birbirine bağlanmıştı. Anahtar 41 gün sonra bulundu (DES Cracker 1). Başka bir grup kod kırıcı farklı bir yaklaşım denediler. Saniyede 88 milyar anahtar hızı ile arama yaparak düz metni "it's time for those 128-, 192-, and 256-bit keys" biçiminde olan şifrelenmiş mesajı sadece 56 saatte çözecek bir tek makine imal ettiler (DES Cracker 2).

Ocak 1999'daki yarışmada önceki iki kazanan yarışmacı birlikte çalıştılar ve saniyede 245 milyar anahtarı deneyerek, anahtarı sadece 22 saat 15 dakikada buldular. Bütün olasılıkları denemeye dayalı arama sistemi DES üzerine yapılabilecek tek saldırı tipi değildir. 1990'larda şifrenin iç yapısını bozmaya yönelik başka başarılı saldırılar da yapılmıştır (Biham and Knudsen, 1998).

Kriptograflar DES'in güvenliğini arttırmaya yönelik çalışmalar yaptılar. Çalışmaların sonucunda 3DES, DESX ve diğer versiyonlar üretildi. Ekim 2000'de, yaşlanmakta olan DES'in yerine bir şey koymak için gösterilen dört yıllık çaba yeni bir standardın ortaya çıkması ile sonuçlandı: Gelişmiş Şifreleme Standardı (AES). AES 128 bitlik bloklar ile 128, 192 ve 256 bitlik anahtarlar kullanmaktadır. Bu standart Aralık 2001'de kabul gördü ve Mayıs 2002'de kullanılmaya başlandı (Dusek, et al., 2006).

Konvansiyonel kriptografik yöntemlere bir saldırı tipi de "yan kanal analizi" olarak adlandırılan saldırılardır (Rosa, 2001). Kriptografik algoritmaları gerçekleyen donanımlar bazı istemsiz çıkışlar da üretmektedirler. Bu istemsiz çıkışlar; işlem süresi, dinamik güç tüketimi, elektromanyetik radyasyon ve cihazın çıkardığı ses olabilir. Eğer böyle bir çıkış, cihaz içinde saklanan gizli bilginin tamamıyla veya bir parçasıyla ilişkiliyse "yan kanal bilgisi" olarak adlandırılır. Yan kanal analizi saldırılarında, bu yan kanal bilgileri kullanılarak gizli bilgiye ulaşılmaya çalışılır. Yan kanal analizi saldırıları kriptografik algoritmaların gerçeklendiği sistemler için büyük bir tehdit oluşturmaktadır. Bu konu üzerine artarak devam eden araştırmalarda DES, AES ve RSA'nın da içlerinde olduğu birçok algoritma gerçeklemesinin yan kanal analizi saldırılarına açık olduğu gösterilmiştir (Ordu ve Örs, 2006).

Simetrik ve asimetrik algoritmaların birbirlerine göre birtakım üstünlükleri ve zayıf yönleri vardır. Her iki algoritmanın üstünlüklerinden faydalanmak ve zayıf yönlerinden kaçınmak amacıyla hibrid (melez) kripto sistemler kullanılmaktadır (http://www.pro-g.com.tr). Hibrid sistemlerde, şifreleme için simetrik anahtarlar kullanılırken bu anahtarların iki taraf arasında paylaşılması için asimetrik yöntemler kullanılmaktadır (Yıldırım ve Demiray, 2008). Hibrid sistemler elektronik ticarette, bankacılık sektörünün finans ve ATM işlemlerinde, pin şifrelemelerinde, elektronik imzalarda, cep telefonu görüşmelerinde kimlik tespiti ve doğrulanmasında ve diğer birçok alanda yaygınlaşarak kullanılmaktadırlar.

1.5. VERNAM ŞİFRESİ VE ANAHTAR DAĞITIM PROBLEMİ

Sınırsız teknolojik gücü olan potansiyel bir rakibe karşı bile koşulsuz güvenlik sağlayabilen, bilinen tek kripto sistem 1918'de Vernam'ın geliştirdiği one time pad'tir. Başka bir deyişle, rakibin ne kadar hesaplama gücü olursa olsun, one time pad'i kırması imkansızdır. Vernam şifresi bir çeşit simetrik anahtar şifrelemesidir. Yani aynı anahtar hem şifreleme hem de çözme için kullanılır. Bir düz metine rastgele bir anahtar eklendiğinde sonuçta elde edilen dizinin bitleri de rastgele olur ve mesaj ile ilgili hiç bir bilgi içermez. Bu sistemde her harfe bir rakam verilir. Şifrelenecek metinle aynı uzunlukta olan seçilen anahtar da rakamsal olarak ifade edilir. Şifrelenecek metin ile anahtar İngilizce'de Mod 26, Türkçe'de ise Mod 29'a göre toplanır (Keskin, 2009).

A	B	C	Ç	D	E	F	G	Ğ	H	I	İ	J	K	L	M	N	O	Ö	P	R	S	Ş	T	U	Ü	V	Y	Z
00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28

Örneğin "ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ" düz metni OTP ile şifrelenecek olunursa, bu metin "05-21-13-11-22-05-09-11-20-17-21-15-00-16-07-00-28-11-25-16-11-26-5-20-21-11-23-05-21-11" şeklinde yazılır. Düz metin ile aynı uzunlukta ya da daha uzun olan rastgele bir anahtar oluşturulur. Örneğin "FEN BİLİMLERİ ENSTİTÜSÜ GENEL FİZİK BİLİM DALI" anahtarı düz metinle aynı uzunlukta kesilip kullanılabilir. Düz metin 30 harften oluşmaktadır ve anahtarın ilk 30 harfi "06-05-16-01-11-14-11-15-14-05-20-11-05-16-21-23-11-23-25-21-25-07-05-16-05-14-06-11-28-11" biçiminde yazılabilir. Şifreli metni elde etmek için düz metin ile anahtar Mod 29'a göre toplanırsa,

Düzmetin: 05-21-13-11-22-05-09-11-20-17-21-15-00-16-07-00-28-11-25-16-11-26-05-20-21-11-23-05-21-11

Anahtar : 06-05-16-01-11-14-11-15-14-05-20-11-05-16-21-23-11-23-25-21-25-07-05-16-05-14-06-11-28-11

$$5 + 6 = 11 \equiv 11\ (Mod\ 29)$$

$$21 + 5 = 26 \equiv 26\ (Mod\ 29)$$

$$13 + 16 = 29 \equiv 0\ (Mod\ 29)$$
$$11 + 1 = 12 \equiv 12\ (Mod\ 29)$$
$$\vdots$$

sonuçta "11-26-0-12-4-19-20-26-5-22-12-26-5-3-28-23-10-5-21-8-7-4-10-7-26-25-0-16-20-22" dizisi elde edilir. Bu dizinin karşılığı olan şifreli metin ise "İVAJDPRVEŞJVEÇZTIESĞGDIGVÜANRŞ" biçimindedir. Şifreyi çözmek için ise, şifrelemede yapılan işlemler tersten uygulanır. Yani şifreli metinden anahtar çıkarılır. Ancak Mod 29'da işlem yapıldığı için anahtarın çıkarılması demek, anahtarın toplamaya göre tersinin toplanması demektir. Mod 29'da bir sayının toplamaya göre tersi, o sayının 29'dan çıkarılmasıyla bulunur. Bu yüzden anahtardaki her sayı 29'dan çıkarılır ve şifre çözme anahtarı bulunur (Çimen vd., 2011).

$$29 - 6 = 23$$
$$29 - 5 = 24$$
$$\vdots$$

İşleme devam edildiği takdirde şifre çözme anahtarı "23-24-13-28-18-15-18-14-15-24-9-18-24-13-8-6-18-6-4-8-4-22-24-13-24-15-23-18-1-18" şeklinde bulunur. Şifreli metin ile şifre çözme anahtarı Mod 29'a göre toplanırsa,

Şifremetin:	**11-26-00-12-04-19-20-26-05-22-12-26-05-03-28-23-10-05-21-08-07-04-10-07-26-25-00-16-20-22**
Şifreçözme anahtarı:	**23-24-13-28-18-15-18-14-15-24-09-18-24-13-08-06-18-06-04-08-04-22-24-13-24-15-23-18-01-18**

$$11 + 23 = 34 \equiv 5\ Mod\ 29$$
$$26 + 24 = 50 \equiv 21\ Mod\ 29$$
$$\vdots$$

"ESKİŞEHİR OSMANGAZİ ÜNİVERSİTESİ" düz metinine ulaşılır. Bir farkla, elektronik veri iletiminde Vernam şifresi ile şifreleme yapılırken harfler ikilik tabandaki sayılarla ifade edilir.

Vernam sifresi, $A = \{0,1\}$ alfabesi üzerinde tanımlı bir akış şifresidir (Soyalıç, 2005). Yani düz metin ve anahtar 1 ve 0'lardan oluşur. Burada bulunan 0,1'lerin her birine "bit" adı verilir. Vernam şifresinde esas işlem XOR işlemidir. XOR işlemi vektörel olarak bitleri Mod 2'de toplama işlemidir. İlk örnekte Mod 29'da çalışıldığı için şifreleme ve şifre çözme anahtarı farklı bulunmuştu. İkilik tabanda çalışıldığında ve XOR işlemi yapıldığında şifre çözme anahtarı şifreleme anahtarının kendisidir. Şifreli metin, düz metnin anahtar ile XOR'lanmış şeklidir. Şifreli metin ile anahtar tekrar XOR'lanırsa düz metin elde edilir (Çimen vd., 2011).

Örnek:

$$
\begin{array}{rl}
 & Düz\ metin : 11010 \\
\oplus & Anahtar : 01010 \\
\hline
 & Şifreli\ Metin : 10000 \\
\oplus & Anahtar : 01010 \\
\hline
\end{array}
$$

$Düz\ metin : 11010$ (Sağıroğlu, 2011).

"One time pad" şifreleme sisteminin koşulsuz olarak güvenli olması için anahtar uzunluğu, mutlaka düz metinin uzunluğuna eşit ya da ondan daha uzun olmalıdır. Anahtar ile ilgili bir diğer önemli özellik de anahtarı oluşturan elemanların tamamen gelişi güzel olarak seçilmesidir. Sistemin adından da anlaşılabileceği üzere bir mesajın şifrelenmesi için kullanılan anahtar bir daha asla kullanılmamalıdır aksi takdirde sistemin güvenliği sekteye uğrar.

Şifreli metin, mesajın gizliliğinden emin olarak radyo yayını, internet ya da gazete vasıtasıyla açıkça yollanabilir. Ama anahtarın gönderici ve alıcı tarafından çok gizli bir kanalla paylaşılması gerekir, örneğin çok güvenilir bir telefon hattı, özel bir görüşme ya da emin bir taşıyıcı aracılığıyla. Güvenilir bir kanal genelde sadece belli zamanlarda ve belirli şartlar altında mümkündür. Böylesi bir haberleşmede tam

güvenliği sağlamak için kullanıcılar, sonradan göndermek isteyecekleri mesaja hacimce denk gizli ve anlamsız bir yığın bilgiyi yanlarında taşımak zorunda kalacaklardır. Dahası, güvenli bir kanal bulunsa bile, bu güvenliğin gerçek manada garanti olduğu söylenemez. Şöyle bir problem vardır ki: Prensip olarak, herhangi bir klasik özel kanal, kullanıcılara izlenildiklerini fark ettirmeden pasif olarak takip edilebilir. Çünkü klasik fizik, ortamın hiçbir özelliğini bozmadan bütün fiziksel özelliklerinin ölçülebilmesine fırsat verir. Şifreleme anahtarları da dahil olmak üzere her türlü bilgi bir obje ya da sinyalin ölçülebilir fiziksel özelliklerinde kodlandığından, klasik teoriler pasif takip olasılığının önüne geçememektedirler.

2. KUANTUM ANAHTAR DAĞITIMI

2.1. GİZLİ DİNLEMENİN TESPİT EDİLMESİ

Kuantum kriptografi ya da diğer adıyla kuantum anahtar dağıtımı (KAD), güvenliğinin matematikten çok fizik kanunlarına dayanması bakımından geleneksel kriptografik sistemlerden farklıdır (Toyran, 2007). Kuantum anahtar dağıtımının temeli, temel bir fizik kanunu olan Heisenberg belirsizlik ilkesine dayanmaktadır. Bu ilkeye göre kuantum fiziğinde bir nesnenin aynı anda iki özelliği (konum ve momentum) birden ölçülemez ve bu özelliklerden biri için sırayla yapılan ilk ölçüm ikinci ölçümün sonucunu belirsiz hale getirir. Bu ilke, optik hatlar üzerinden iletilen en küçük ışık parçacığı olan fotonun, polarizasyonuna bağlı olarak taşıdığı verinin arka arkaya yapılacak ölçümler ile bozulacağını öne sürmektedir. Hatasız iletim hatlarında kaynaktan hedefe iletilmekte olan verinin bozulması arada istenmeyen biri tarafından verinin okunmaya çalışıldığı anlamına gelir. Bu durumda alıcı ve gönderici taraflar hattın dinlenip dinlenmediğinden emin olabilir (Gümüş, 2011).

Kuantum mekaniğinin gizli dinlemeye engel olmadığı, yalnızca bu gibi bir durumun varlığının tespit edilmesini sağladığı unutulmamalıdır. Tutarsızlıklar görüldüğünde basitçe anahtar iptal edilir ve kullanıcılar yeni bir anahtar üretmek üzere prosedürü tekrarlarlar (Dusek, et al., 2006).

2.2. KUANTUM ÖLÇÜMÜ

Kuantum fiziğinde ölçme, klasik fizikteki ölçmeden belirgin olarak farklıdır. Kuantum teorisine göre herhangi bir ölçüm yalnızca "ölçüm tabanı" denilen tabanı oluşturan spesifik ortogonal durum vektörleri arasında kesinlikle (hata veya belirsiz sonuç olmadan) sonuç belirleyebilir. Yani ortogonal durumlar kesinlikle ayırt edilebilir fakat durumlar birbirlerine ortogonal değil ise tam olarak durumları ayırt edebilecek bir kuantum ölçümü yoktur (İpekoğlu vd., 2009). Ayrıca ölçme işlemi genel olarak sistemi etkiler. Eğer sistem, ölçüm tabanını oluşturan vektörlerden birinin katı olarak ifade edilebilen bir durumda değil de bunların lineer süperpozisyonu olan bir durumdaysa, o zaman bu durum ölçümden sonra değişir. Ölçme işlemi sırasında orijinal durum unutulur ve rastgele bir seçimle taban vektörlerden birine tekabül eden bir duruma dönüşür. İşte tam da bu, dinlemenin tespit edilebilmesini sağlayan özelliktir. Dinleme, bilgi taşıyıcısı üzerindeki bir tür ölçümlemeden başka bir şey değildir. Eğer iletim sırasında ortogonal olmayan durumlar kullanılırsa, dinlemenin bunlardan bazılarını etkilemesi gerekir yani hatalar yaratmalıdır. Uygun tasarlanmış bir protokol ile bu hatalar daha sonra kanalın yasal kullanıcıları tarafından tespit edilebilir.

2.3. BİT VE KÜBİT

Bit, klasik hesaplama ve klasik bilginin temel birimidir (Çağ, 2008). Fiziksel manada ise karşılığı aldığı değerdir. Bu değer ya 0 ya da 1'dir. Kübit ise kuantumun ilk iki harfi ile bit ifadesinin birleşiminden oluşan kuantum bitin kısa ifadesidir. Kübit klasik anlamda bitin tüm özelliklerini taşır ancak bite göre ufak bir fark vardır. Bit sıfır veya bir değerinden birini alabiliyorken, kübit sıfır, bir veya bu her iki değerin süperpozisyonunu alır. Bu manada kübit, 0 ve 1'in lineer birleşimi olarak tasvir edilebilir (Özen, 2009).

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \tag{2.1}$$

Yukarıdaki denklemde α ve β olasılık genlikleridir. Bir kübit ölçüldüğünde $|\alpha|^2$ olasılıkla 0, $|\beta|^2$ olasılıkla da 1 değeri bulunur (Şen, 2002).

Bazı kübit durumlar farklı isim ve tanımlarla betimlenmektedirler. Fotonun polarize durumlarının tanımı ve isimleri Tablo 2.1'de verilmiştir.

Kubit durumu	Polarizasyon durumu	Polarizasyon ismi
$\|0\rangle$	$\|H\rangle$	Yatay lineer
$\|1\rangle$	$\|V\rangle$	Dikey lineer
$\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+\|V\rangle)=\|+45^\circ\rangle=\|225^\circ\rangle$	+45° (225°) lineer
$\frac{1}{\sqrt{2}}(\|0\rangle-\|1\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-\|V\rangle)=\|-45^\circ\rangle=\|135^\circ\rangle$	−45° (135°) lineer
$\frac{1}{\sqrt{2}}(\|0\rangle+i\|1\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle+i\|V\rangle)=\|L\rangle$	Sol el dairesel
$\frac{1}{\sqrt{2}}(\|0\rangle-i\|1\rangle)$	$\frac{1}{\sqrt{2}}(\|H\rangle-i\|V\rangle)=\|R\rangle$	Sağ el dairesel

Tablo 2.1 Fotonun farklı polarizasyonlarına karşılık gelen bazı kübit durumları (Özen, 2009).

2.4. KUANTUM DURUMLARIN KOPYALANAMAMASI

Kuantum mekaniksel sistemlerde depolanmış bilgiye "kuantum bilgisi" denmektedir. İki seviyeli bir kuantum sistemi klasik bit kodlayabilir. Daha önce de bahsedildiği üzere "kuantum bit" ya da "kübit" olarak adlandırılan bu sistem klasik bitler gibi 0 ve 1'lerden oluşur. Ancak klasik bitlerde mümkün olmayan, $|0\rangle$ ve $|1\rangle$ durumlarının sonsuz sayıda üst üste binmesi de mümkündür. Fakat yapılacak bir ölçüm tek kübitlik sistemi $|0\rangle$, $|1\rangle$ durumlarından herhangi birine indirgeyecektir. Bu yüzden kübitteki bilgi tam olarak öğrenilemeyecek, tek kübitten tek bir klasik bilgi çıkarılabilir sonucuna zorlanılacaktır. Bu zorluğu aşmak için kübitin çok sayıda kopyasını çıkararak uygun istatistiksel ölçüm analizleri sonucu tüm bilgiye ulaşılacağı düşünülebilir. Ancak 1982 yılında Wooters ve Zurek bilinmeyen bir kuantum durumunun kopyalanamayacağını ispatlamıştır (Türkpençe, 2007).

Kuantum mekaniğinin lineerliği, isteğe bağlı bilinmeyen kuantum durumlarının kopyalanmasını engeller (Wooters and Zurek, 1982). Bunu göstermek için; $|H\rangle$ yatay polarizasyonlu bir fotonu kopyalayacak bir kopyalayıcı cihaz aşağıda verilen (2.2) işlemini gerçekleştirmelidir.

$$|kopyalayıcı_0\rangle|boşluk\rangle|H\rangle \rightarrow |kopyalıyıcı_1\rangle|H\rangle|H\rangle \tag{2.2}$$

Ve ortogonal dikey polarizasyon $|V\rangle$ için de aynı şekilde,

$$|kopyalayıcı_0\rangle|boşluk\rangle|V\rangle \rightarrow |kopyalıyıcı_2\rangle|V\rangle|V\rangle \tag{2.3}$$

işlemini yapmalıdır. Burada $|kopyalayıcı_0\rangle$, kopyalayıcının başlangıç durumudur. $|kopyalıyıcı_1\rangle$ ve $|kopyalıyıcı_2\rangle$ kopyalayıcının son durumları olup, $|boşluk\rangle$ ise bilginin yani polarizasyon durumunun kopyalanacağı, yardımcı sistemin ilk boş durumunu ifade etmektedir. Bununla birlikte $|H\rangle$ ve $|V\rangle$ durumlarının bir lineer süperpozisyonu kopyalanmak istendiğinde,

$$\begin{aligned}&|kopyalayıcı_0\rangle|boşluk\rangle(\alpha|H\rangle + \beta|V\rangle)\\&= \alpha|kopyalayıcı_0\rangle|boşluk\rangle|H\rangle + \beta|kopyalayıcı_0\rangle|boşluk\rangle|V\rangle\\&\rightarrow \alpha|kopyalıyıcı_1\rangle|H\rangle|H\rangle + \beta|kopyalıyıcı_2\rangle|V\rangle|V\rangle\end{aligned} \tag{2.4}$$

elde edilir. Bu da, $|kopyalayıcı_1\rangle$ ve $|kopyalayıcı_2\rangle$ durumlarının birbirlerine özdeş (ve bunların $|kopyalayıcı_3\rangle$'e eşit) olup olmamasına bakılmaksızın,

$$\begin{aligned}&|kopyalayıcı_3\rangle(\alpha|H\rangle + \beta|V\rangle)(\alpha|H\rangle + \beta|V\rangle)\\&= |kopyalayıcı_3\rangle(\alpha^2|H\rangle|H\rangle + \alpha\beta|H\rangle|V\rangle + \beta\alpha|V\rangle|H\rangle + B^2|V\rangle|V\rangle)\end{aligned} \tag{2.5}$$

beklenen durumundan farklıdır.

Kuantum evriminin üniterliği aşağıdaki (2.6) eşitliğini gerektirmektedir.

$$\langle H|V\rangle\langle boşluk|boşluk\rangle\langle kopyalayıcı_0|kopyalayıcı_0\rangle$$
$$= \langle H|V\rangle\langle H|V\rangle\langle kopyalayıcı_1|kopyalayıcı_2\rangle \quad (2.6)$$

Bu da ancak kopyalanacak durumlar ortogonal olduğunda sağlanır. Dolayısıyla bir kuantum nesnesinin genel durumu tam olarak kopyalanamaz. Kopyalama yalnızca takribi olarak yapılabilir. Yani sonuçta elde edilen durumlar orijinali ile tam olarak eşit değildir (Dusek, et al., 2006).

2.5. BB84 PROTOKOLÜ

Geliştirilen ilk kuantum anahtar dağıtım protokolü olan BB84, IBM araştırma bölümünden Charles Bennett ve Montreal Üniversitesinden Gilles Brassard tarafından öne sürülmüştür (Gümüş, 2011). Bennett ve Brassard'ın kuantum mekaniğinden faydalanarak rastgele bir kriptografik anahtarın güvenli bir şekilde dağıtımını sağlayabilmek için geliştirdikleri bu protokol, herhangi bir gizli dinlemeyi çok yüksek bir olasılıkla açığa çıkarabilmekte ve iki farklı konumdaki kullanıcının eşit ve tamamen rastlantısal bir bit dizisini paylaşmalarını sağlayabilmektedir.

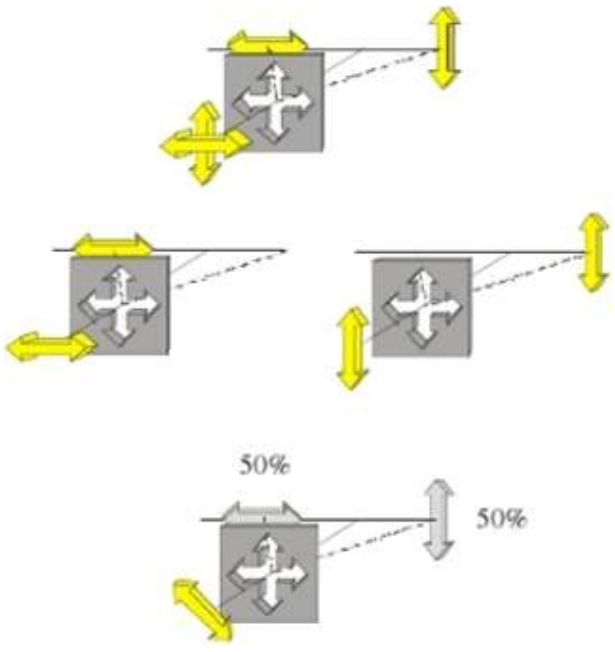
Şekil 2.1 BB84 protokolünde kullanılan polarizasyon tabanları. Sırasıyla, (a) ve (b), rektilineer ve diyagonal tabanları simgelemektedir (Toyran, 2003).

BB84 protokolünde eşlenik iki polarizasyon tabanı kullanılır (Şekil 2.1). Bu iki tabandan biri olan rektilineer taban, fotonların yatay $|H\rangle$ ve dikey $|V\rangle$ polarizasyon durumlarını hazırlayıp gönderebilir veya okuyabilir. Diyagonal taban ise 45^0 anti-diyagonal $|A\rangle$ ve 135^0 diyagonal $|D\rangle$ lineer polarizasyon durumlarını gönderebilir/okuyabilir.

Mesajın göndericisi bir kuantum sisteminin iki ortogonal durumuna mantıksal sıfır ve birleri kodlar fakat her bit için bu durum çiftini rastgele değiştirir yani iki tabandan birini seçer. Bilgilerin kodlanacağı $|H\rangle$, $|V\rangle$, $|A\rangle$ ve $|D\rangle$ polarizasyon durumları denklem (2.7)'deki bağıntılarını sağlar. Ortogonal olmayan sinyal durumları ise pratikte arada bir gizli dinleyici olup olmadığını kontrol etmek için kullanılırlar.

$$\begin{aligned} &\langle H|V\rangle = \langle A|D\rangle = 0 \\ &\langle H|H\rangle = \langle V|V\rangle = \langle A|A\rangle = \langle D|D\rangle = 1 \\ &|\langle H|A\rangle|^2 = |\langle H|D\rangle|^2 = |\langle V|A\rangle|^2 = |\langle V|D\rangle|^2 = 1/2 \end{aligned} \tag{2.7}$$

Bir tabanın her durum vektörü diğer tabanın tüm vektörlerinin üzerinde eşit uzunlukta izdüşümlere sahiptir. Bu demektir ki eğer bir tabanda hazırlanmış bir sistem üzerine diğer tabanda ölçüm uygulanırsa sonuç tümüyle rastlantısaldır ve sistem önceki durumu ile ilgili tüm hafızasını kaybeder.



Şekil 2.2 Alıcı tarafında foton polarizasyonunun doğru ve yanlış tabanlarda ölçümü. Durumların hazırlandığı tabanda gerçekleştirilen ölçümler belirleyici sonuç verir. Öte yandan, yanlış tabanda yapılanlar ise eşit olasılıkları olan rastlantısal sonuçlar elde eder (http://swissquantum.idquantique.com/?Raw-Key-Exchange).

Gönderici ve alıcı iletim sonunda açık bir kanal yoluyla iletişime geçerek her bit için sırayla kullandıkları tabanları birbirleriyle paylaşırlar. Hazırlanması ve okunması aşamasında aynı tip taban kullanılan bitler anahtarın bir elemanı olarak kaydedilir.

2.5.1. BB84 Protokolünün Uygulanması

Genelde iletişim kurmak isteyen iki kişi "Alice" ve "Bob" olarak adlandırılırlar. Protokolün uygulama aşamasında, Alice ve Bob, örneğin $|H\rangle$ ve $|A\rangle$'nın 0 bit değerinin yerine, $|V\rangle$ ve $|D\rangle$'nin ise 1 bit değerinin yerine kullanılacağı konusunda anlaşırlar. Bu seçim isteğe göre düzenlenebilir. Ancak bu eşleşme, doğru gönderim/okuma işlemi için hem gönderici hem de alıcı tarafta aynı şekilde belirlenmelidir (Gümüş, 2011). Gönderici yani Alice, iletmek istediği bitlerden oluşan bir diziyi rastgele ve bağımsız olarak, her bit için kodlama tabanını rektilineer veya diyagonal olarak seçerek oluşturur. Bu, fotonların $|H\rangle$, $|V\rangle$, $|A\rangle$ ve $|D\rangle$ olmak üzere bu dört polarizasyon durumunda eşit olasılıklarla $(p_{|H\rangle} = p_{|V\rangle} = p_{|A\rangle} = p_{|D\rangle} = 1/4)$ gönderildiği anlamına gelmektedir. Alıcı Bob ise Alice'den bağımsız ve rastlantısal olarak ölçüm tabanlarını ya rektilineer ya da diyagonal olarak seçer. İstatistiksel olarak, %50 ihtimalle Alice ve Bob'un tabanları çakışacaktır (Dusek, et al., 2006). Yani Alice ve Bob'un birbirlerinden habersiz olarak aynı tabanı seçmeleri ihtimali %50'dir.

Sonuçların ne zaman belirleyici olduğunu bilmek için Alice ve Bob birbirlerine her gönderilen ve alınan foton için hangi tabanı kullandıklarını söyleyecekleri bir açık kanala da ihtiyaç duyacaklardır. Bu kanal dinlense de fark etmeyecektir. Çünkü bu kanalla ölçümlerin sonuçları hakkında değil yalnızca kullanılan tabanlarla ilgili bilgi paylaşılmaktadır. Tabanları uyuştuğunda, Alice ve Bob biti saklarlar. Diğer yandan, farklı tabanlar seçmişlerse veya Bob'un detektöründen kaynaklı bir problem oluşmuşsa ya da foton yolda bir yerde kaybolmuşsa bit atılır. Bu görüşmeyi dinleyen herhangi bir gizli dinleyici -ki genelde "Eve" olarak adlandırılır- yalnızca ikisinin de rektilineer veya diyagonal tabanı kullanmayı seçmiş olduklarını öğrenebilir. Alice'in 0 mı yoksa 1 mi göndermiş olduğunu öğrenemez (Dusek, et al., 2006). Örnek bir BB84 protokolü uygulaması Tablo 2.1'de verilmiştir.

0	1	1	0	0	1	0	1
×	×	+	+	+	×	+	×
$\|A\rangle$	$\|D\rangle$	$\|V\rangle$	$\|H\rangle$	$\|H\rangle$	$\|D\rangle$	$\|H\rangle$	$\|D\rangle$
×	+	+	×	×	+	+	×
$\|A\rangle$	rastgele	$\|V\rangle$	rastgele	rastgele	rastgele	kayıp	$\|D\rangle$
×	+	+	×	×	+	–	×
tamam	–	tamam	–	–	–	–	tamam
0	–	1	–	–	–	–	1

Tablo 2.2 Örnek bir BB84 protokolü uygulaması. 1. satırda Alice'in rastgele oluşturduğu bitler, 2. satırda Alice'in rastgele seçtiği polarizasyon tabanları, 3. satırda gönderilen fotonların gerçek polarizasyonları, 4. satırda Bob'un rastgele seçtiği ölçüm tabanları, 5. satırda tespit edilen fotonların polarizasyonları, 6. satırda Bob'un açık kanaldan duyurduğu ölçüm tabanları, 7. satırda Bob doğru ölçüm tabanını kullandığında Alice'in açık kanaldan verdiği cevap, 8. satırda kriptografik anahtar yer almaktadır (Dusek, et al., 2006).

2.6. DURDUR-TEKRAR GÖNDER ATAĞI

İletim sırasında eğer Eve aradaysa ve kanalı gizlice dinlemek istiyorsa, iletimleri pasif olarak gözlemleyemez. Eve'in bu noktada yapabileceği iki şey vardır: Birincisi, Alice tarafından gönderilen fotonları durdurarak üzerlerinde iki taban arasından seçtiği biriyle ölçümler yapmak ve bunun sonuçlarına göre hazırladığı yeni fotonları Bob'a göndermek (Dalkılıç ve Ayhan, 2005); ikincisi ise elindeki bir sistemin, bilgi taşıyan kuantum sistemi ile etkileşmesini sağlayıp onu saklayarak daha sonra ölçmek amacıyla fotona sonda eklemektir. İlk ihtimal yani bir durdur-tekrar gönder atağı ele alındığında, Alice kodlama tabanını rastlantısal olarak değiştirdikçe, Eve hangi tabanda ölçüm yapacağını bilemez. Ölçüm tabanlarını onun da rastlantısal olarak seçmesi gerekir. Tahminlerinin yarısı doğrudur ve Bob'a doğru kutuplanmış fotonlar gönderir. Ölçümlerinin %50'sini ise yanlış tabanda yapar ve bu da hatalar üretir. Örneğin Alice'in rektilineer tabanda 1 yani $|V\rangle$ gönderdiği ve Eve'in diyagonal tabanda ölçüm

yaptığı varsayılırsa, Bob da rektilineer tabanda ölçüm yapmalıdır, aksi takdirde bit atılır. Bu noktada, Eve ne tespit ederse etsin ve gönderirse göndersin, $|A\rangle$ veya $|D\rangle$, Bob'un $|V\rangle$ yerine $|H\rangle$ yani 0 almak için %50 şansı vardır. Dolayısıyla, sürekli bir durdur-tekrar gönder atağı yapıldığında, Bob, başarıyla tespit ettiği bitlerin ortalama %25'inde hata bulacaktır. Eğer Alice ve Bob karşılaştırma amacıyla dizilerinin bir bölümünü birbirleriyle paylaşırlarsa bu hataları ortaya çıkarabilirler. Burada şuna dikkat edilmelidir: Kontrol amaçlı açık kanaldan üzerlerinde tartışılan bu bitler atılmalı, anahtara kesinlikle dahil edilmemelidirler. Sonuç olarak gönderici ve alıcı aynı tabanları seçtiklerinde, bit dizilerinin tamamen örtüşmesi gerekir. Uyumsuzluk belirlenirse bir gizli dinleyicinin fotonlara müdahale ettiğinden şüphelenilir ve kriptografik anahtar iptal edilir. Dolayısıyla gizli dinleme durumunda bile hiçbir bilgi sızıntısı oluşmaz. Diziler tamamen aynı ise, anahtarın güvenli ve gizli olduğu kabul edilir. Böylece daha önce detaylı olarak bahsedilen Vernam şifresi kullanılarak iletişim şifrelenebilir (Dusek, et al., 2006). Görüldüğü üzere durdur-tekrar gönder atağı gizli dinleme için çok başarılı ve gizli dinlemenin anlaşılamayacağı bir saldırı tipi değildir.

İkinci ihtimal olarak, Eve orijinal durumun bozulmadan kalması için bilgi taşıyıcısına (fotona) bir sonda eklemeyi ve onun bilgi taşıyıcısı ile etkileşime girmesini sağlamaya çalışabilir.

$$\begin{aligned} |a\rangle|E\rangle &\rightarrow |a\rangle|E_a\rangle \\ |b\rangle|E\rangle &\rightarrow |b\rangle|E_b\rangle \end{aligned} \tag{2.8}$$

Denklem (2.8)'de, $|a\rangle$ ve $|b\rangle$ bilgi taşıyıcısının iki muhtemel durumunu temsil etmektedir. $|E\rangle$ Eve'in sondasının ilk durumu olup, $|E_a\rangle$ ve $|E_b\rangle$ ise son durumlarıdır. Herhangi bir üniter etkileşim $\langle a|b\rangle\langle E|E\rangle = \langle a|b\rangle\langle E_a|E_b\rangle$ eşitliğini korumalıdır. Eğer $|a\rangle$ ve $|b\rangle$ durumları ortogonal değil ($\langle a|b\rangle \neq 0$) ise, bu eşitlik yalnızca $\langle E_a|E_b\rangle = 1$ iken yani Eve'in sondasının son durumları özdeş olduğunda sağlanır. Dolayısıyla Eve hiçbir bilgi elde edemez. Yani Eve ölçülen objelerin durumlarını etkilemeden ve dolayısıyla iletimde hatalara neden olmadan iki ortogonal olmayan durum arasında ayrım yapamaz (Dusek, et al., 2006).

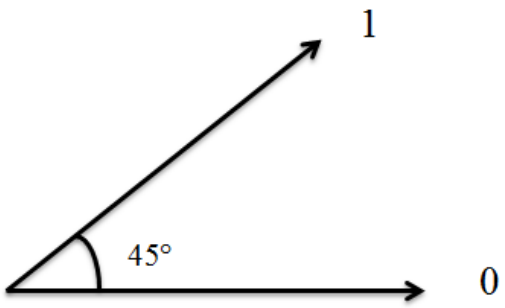
Sistemde kullanılan hiçbir fiziksel cihazın mükemmel ve parazitsiz olmadığı göz önünde bulundurulmalıdır. Şöyleki, Alice ve Bob arada Eve'in olmadığı zamanlarda bile hata tespit edebilirler. Bu duruma karşılık, iletimden sonra Alice ve Bob bit dizilerini önce bir hata düzeltmesi tekniği kullanarak tekrar bağdaştırırlar ve özdeş bir bit dizisine ulaşırlar. Fakat bu dizi tümüyle gizli değildir ve Eve bu dizinin bir kısmını biliyor olabilir. Böyle bir bilgiyi yok etmek için ise "gizlilik artırımı" denilen bir işlem uygularlar. Gizlilik artırımı Alice ve Bob'un bir bit dizisini öyle bir yöntemle süzmelerini sağlar ki Eve'in bu işlemden geçen dizinin çok küçük bir kısmını dahi bilmesi son derece küçük bir ihtimaldir. Hata düzeltme ve gizlilik artırımından daha sonra 8. Bölümde detaylı olarak bahsedilecektir.

2.7. B92 PROTOKOLÜ

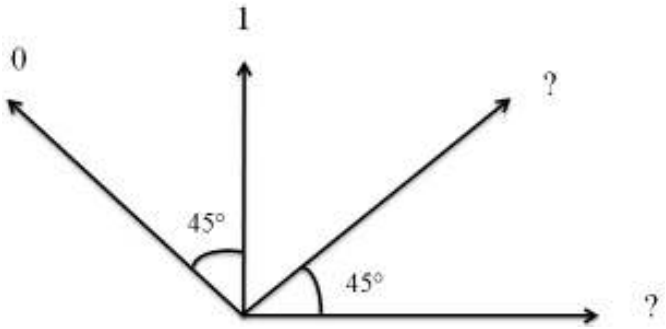
BB84'ün geliştiricilerinden olan Charles Bennett, 1992 yılında iki ortogonal olmayan durum ile de kuantum anahtar dağıtımı yapılabileceğini gösterdi. "B92 protokolü" adı verilen bu protokolde, Alice iki ortogonal olmayan durum seçer ve Bob'a rastgele gönderirse, Bob sinyal durumlarına ortogonal olan alt uzaylara izdüşümler uyguladığında ya Alice'in gönderdiği biti kesinlikle öğrenir ya da sonuç getirmeyen bir durumla karşılaşır. İletimden sonra Bob, Alice'e ne zaman bit tespit ettiğini bildirir fakat kullandığı tabanı açıklamasına gerek yoktur. Çünkü Bob fotonu tespit etmişse kullandığı taban Alice'in göndermiş olduğu biti zaten başarılı bir şekilde tanımlar (Dusek, et al., 2006).

2.7.1. B92 Protokolünün Uygulanması

B92 protokolü uygulanırken 0º polarizasyona sahip fotonlar "0" kübit anlamını, 45º polarizasyona sahip fotonlar ise "1" kübit anlamını taşımaktadır. Bob gönderilen fotonları okumak için BB84 protokolünde olduğu gibi rektilineer ve diyagonal tabanları kullanır. Ancak, polarizasyonunu 0º veya 45º olarak okuduğu fotonları eleyerek anahtara dahil etmez. 90º ve 135º açıya sahip okumaları geçerli kabul eder (Gümüş, 2011). Böylece Bob bitleri aldığı anda mesajın içeriğini öğrenir (Demirel, 2007). Bu protokolü özetleyen durumlar Şekil 2.3 ve 2.4 ile Tablo 2.2'de görülmektedir.



Şekil 2.3 B92 protokolü için polarizasyon-kübit değeri eşleşmesi (Gümüş, 2011).



Şekil 2.4 Okuma basamağında polarizasyon-kübit değeri eşleşmesi (Gümüş, 2011).

Bu durumda Tablo 2.2'de görülen polarizasyon ve taban eşleşmeleri için ilgili sonuçlar oluşacaktır.

Yollanan Kübit	Foton Polarizasyonu	Okuma Tabanı	Okunan Polarizasyon	Okunan Değer	Sonuç
1	/	×	/	?	Geçersiz
0	–	+	–	?	Geçersiz
1	/	+	|	1	Geçerli
1	/	+	–	?	Geçersiz
0	–	×	/	?	Geçersiz
0	–	×	\	0	Geçerli

Tablo 2.3 İletimleri B92 protokolü ile yapılan altı kübit için olası okuma sonuçları (Gümüş, 2011).

BB84 protokolünde alıcı ve göndericinin aynı tabanı kullanmamasına bağlı olarak bir fotonun geçerli kabul edilme olasılığı %50 iken B92 protokolünde bu oran %33'e düşmektedir. Bu da söz konusu iki protokol kıyaslandığında eşit uzunlukta anahtarların oluşturulabilmesi için B92 protokolüyle yapılan iletimin BB84 protokolüne göre daha uzun sürmesi gerektiği anlamına gelmektedir (Gümüş, 2011). Ayrıca B92 protokolü yalnızca kayıpsız veya kaybın çok düşük olduğu sistemlerde güvenlidir. Yüksek kayıplı sistemlerde, varsa, aradaki gizli dinleyici avantajlı konumdadır ve kuantum durumlarda ölçümler yapabilir. Bu gibi bir durumda gizli dinleyici eğer belirsiz bir sonuç elde ederse, sinyali bloke edebilir. Ya da gönderilen durumu tespit edebildiyse, Bob'a doğru bir kopyayı gönderebilir çünkü durumu kesinlikle bilmektedir.

2.7.2. Güçlü Referans Sinyali ile B92 Protokolü

B92 protokolünde yukarıdaki gibi bir gizli dinlemeyi önlemek için bitler zayıf bir sinyal ile klasik güçlü referans sinyali arasında bir faz farkına göre kodlanabilir (Bennett, 1992b). Şöyleki, lazer sinyali, yüksek derecede dengelenmemiş bir demet bölücü ile güçlü ve zayıf kısımlara ayrılır. Hem Alice hem de Bob bu sinyallerin arasına bir faz kayması yerleştirebilirler. Bob'un tarafında her iki sinyal dengelenmemiş demet bölücü ile giriştikleri yerde tekrar birleştirilir. Bob böylece sinyalin tamamını almış olur (Dusek, et al., 2006).

B92 protokolü güçlü referans sinyali ile uygulandığında, Eve belirsiz bir sonuç alırsa güçlü ya da zayıf sinyali yok edemez. Ya da benzer şekilde, eğer Eve kendi zayıf veya güçlü sinyalini üretmeyi ve bunları Bob'a göndermeyi denerse yine kaçınılmaz bir şekilde anlaşılabilir hatalara sebep olacaktır (Fuchs, et al., 1997).

2.8. ALTI DURUMLU PROTOKOL

BB84 protokolü ile aynı şekilde çalışan altı durumlu protokolde farklı olarak Alice ve Bob'un rastlantısal olarak değiştirdiği üç eşlenik taban kullanılır (Bruss, 1998; Bechmann, et al., 1999). Buna göre BB84 protokolünde kullanılan iki eşlenik taban, $\{|0\rangle, |1\rangle\}$ ve $\{|\bar{0}\rangle, |\bar{1}\rangle\}$ olarak ifade edilirse,

$$|\bar{0}\rangle = 1/\sqrt{2}\,(|0\rangle + |1\rangle), \quad |\bar{1}\rangle = 1/\sqrt{2}\,(|0\rangle - |1\rangle) \tag{2.9}$$

yazılabilir. O halde üçüncü taban, $\{|\bar{\bar{0}}\rangle, |\bar{\bar{1}}\rangle\}$ için de,

$$|\bar{\bar{0}}\rangle = 1/\sqrt{2}\,(|0\rangle + i|1\rangle), \quad |\bar{\bar{1}}\rangle = 1/\sqrt{2}\,(|0\rangle - i|1\rangle) \tag{2.10}$$

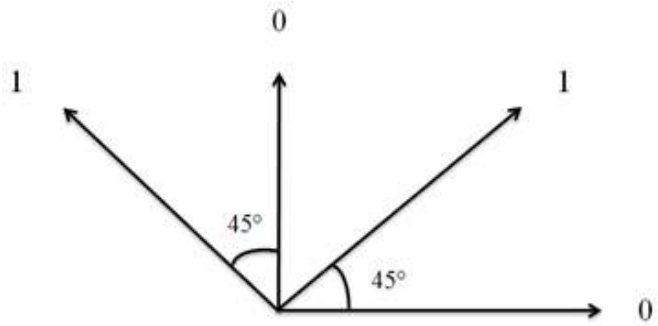
yazılabilir. Alice ve Bob'un aynı tabanı seçme ihtimali 1/3'tür. Yani elenmiş anahtar elde edilirken ham anahtarın 2/3'ü atılır (Güngördü, 2010). Fakat BB84 karşısındaki bu dezavantaj, gizli dinleme durumunda daha yüksek hata üretmesi avantajıyla önemini kaybeder. Örneğin sürekli bir durdur-tekrar gönder atağı BB84 protokolünde görülen %25'e karşı ortalama %33 hataya sebep olur. Üstelik, iki durumlu protokol yeterli, dört durumlusu ise standart iken altı durumlu protokolün sinyal durumlarının simetrisi güvenlik analizini basitleştirir (Gisin, et al., 2002; Dusek, et al., 2006).

2.9. SARG PROTOKOLÜ

SARG protokolü, PNS (photon number splitting) tipi saldırılara karşı 2004 yılında Scarani ve arkadaşları tarafından öne sürülmüştür. KAD sistemlerinde kullanılan tek foton üreteçleri dışındaki ışık kaynakları bir kübitin iletimi esnasında sadece bir adet foton üretmezler. Bunun yerine aynı polarizasyona sahip birden fazla foton üretirler. Dolayısıyla BB84 protokolünün gerçekleştirildiği hattı dinleyen bir gizli dinleyici her kübit için üretilip yollanan N adet fotondan birer tane yakalayıp okuma işleminde kullanılan tabanlar açık kanaldan açıklanana kadar kuantum belleklerde saklayabilirse anahtarı öğrenebilir. BB84'ün PNS tipi saldırılara karşı savunmasız olduğunu gören Scarani ve arkadaşları Alice ve Bob arasındaki klasik iletişimi yeniden düzenlemişlerdir (Gümüş, 2011). Dolayısıyla SARG protokolünü uygulayabilmek için BB84 ile aynı donanım kullanılabilir. Protokol uygulanırken, Alice dört kuantum durumu hazırlar ve Bob ölçümlerini aynen BB84 protokolündeki gibi yapar. Yalnız Alice kullandığı tabanı değil de durumlardan biri kendisinin gönderdiği olmak üzere ortogonal olmayan sinyal durumu çiftini açıklar. Bob, açıklanan iki ortogonal olmayan durumdan birine ortogonal bir durum bulduğu zaman biti doğru olarak öğrenebilir.

2.9.1. SARG Protokolünün Uygulanması

BB84 protokolünün aksine SARG protokolünde Alice ve Bob, okuma işleminde kullandıkları tabanları açıklamazlar. Sadece Alice gönderdiği polarizasyonu ve bu polarizasyonla 45^0 açı yapan başka bir polarizasyonu açıklar. Eğer Bob açıklanan polarizasyonlardan herhangi birine ortogonal bir okuma yaparsa ilgili okumayı geçerli saydığını Alice'e bildirir ve okuduğu kübit'in tümleyenini anahtara ekler (Gümüş, 2011). Bu protokoldeki gönderim işlemi için polarizasyon-kübit ilişkisi ve 0^0 polarizasyona sahip bir fotonun olası altı farklı iletimi için oluşan durumlar sırasıyla Şekil 2.5 ve Tablo 2.4'te görülmektedir.



Şekil 2.5 SARG protokolü için polarizasyon-kübit değeri eşleşmesi (Gümüş, 2011).

Foton Polarizasyonu	Açıklanan Pol. Çifti	Okuma Tabanı	Okunan Polarizasyon	Kabul Durumu	Kübit Değeri
–	/ –	+	–	Geçersiz	
–	/ –	×	/	Geçersiz	
–	/ –	×	\	Geçerli	0
–	\ –	+	–	Geçersiz	
–	\ –	×	/	Geçerli	0
–	\ –	×	\	Geçersiz	

Tablo 2.4 0^0 polarizasyona sahip fotonun SARG protokolüyle olası altı farklı iletimi (Gümüş, 2011).

2.10. TUZAK-DURUM PROTOKOLLERİ

Tuzak-durum metodu zayıf lazer sinyallerinin kullanıldığı KAD sistemlerinde PNS tipi saldırılara karşı geliştirilmiş başka bir yöntemdir (Hwang, 2003; Wang, 2004a; 2004b; Lo, et al., 2005b; Ma, 2004). Bu yöntem ile güvenli iletişimin mümkün olduğu mesafe kayda değer biçimde uzatılabilir ve eğer BB84 protokolü ile birlikte kullanılırsa güvenli anahtar değeri, ışık kaynağı zayıf lazer bile olsa toplam iletim ile orantılı[1] hale gelir.

Tuzak durum fikri, bazı tuzak durumlar eklenerek boş durum, tek foton ve çoklu foton durumlarının davranışlarının ayrı ayrı tahmin edilebileceği tespitine dayanmaktadır. Dolayısıyla Alice bazen ek olarak anahtar iletimi için kullanılandan farklı yoğunlukta (fakat aynı dalgaboyunda, aynı zamanlama ile v.b.) bir tuzak durum gönderir. Bu tuzak durumlar yalnızca Eve'in arada olup olmadığının kontrol edilmesine yarar. Eve, Alice'in ne zaman tuzak durumu gönderdiğini bilemez ve bunu tanımlaması da mümkün değildir. Tuzak durumlarda Eve'in PNS saldırısının yaptığı değişiklikler, Alice ve Bob'un gizli dinlemeyi tespit edebilmesini sağlar (Dusek, et al., 2006).

Bob'un Alice'in kaynağından n foton durumu yayınladığında bir sinyal tespit ettiği koşullu olasılık Y_n, hem sinyal hem de tuzak durumlar için eşit ve arada bir gizli dinleyici bulunmadığında cihaz parametrelerine bağlı olarak aşağıdaki gibi olmalıdır.

$$Y_n^{sinyal} = Y_n^{tuzak} = Y_n = [1 - (1 - \eta)^n](1 - p_{karanlık}) + p_{karanlık} \qquad (2.11)$$

Burada η toplam iletim verimi olup, $p_{karanlık}$ ise detektörün karanlık sayım yapma olasılığıdır. PNS atağı kaçınılmaz bir şekilde bazı Y_n'leri değiştirir. Y_n nicelikleri direkt olarak ölçülemezler. Burada Bob'un direkt olarak belirleyebileceği, verilen bir μ ortalama foton sayısı için Alice'in gönderdiği sinyallerin dedektördeki toplam algılanma hızıdır (Dusek, et al., 2006).

[1] Standart BB84 protokolü için güvenli anahtar değeri, iletimle ancak tek foton kaynağı kullanıldığında doğru orantılıdır. Zayıf lazer sinyalleri kullanıldığında ise iletimin karesi ile orantılıdır.

$$Q_\mu = e^{-\mu} \sum_{n=0}^{\infty} Y_n \frac{\mu^n}{n!} \tag{2.12}$$

Eğer Alice ve Bob farklı ortalama foton sayıları olan tuzak durumlar kullanırlarsa bazı n foton sayıları için Y_n'nin değerlerini tahmin edebilir ve beklenen değerlerle örtüşüp örtüşmediklerini kontrol edebilirler.

2.11. DOLANIKLIK TEMELLİ PROTOKOLLER

Diğer bir kuantum anahtar dağıtımı protokolleri sınıfı da dolanıklık temelli protokolleri (orjinal Ekert protokolü ve onun basitleştirilmiş formu) kapsar. Orijinal Ekert protokolünün güvenliği Bell eşitsizliklerine dayanmaktadır (Ekert, 1991). Protokolün basitleştirilmiş formu ise BB84 protokolüne çok benzer bir biçimde çalışmaktadır (Bennet, et al., 1992c).

2.11.1. Dolanıklık ve Bell Eşitsizlikleri

İki farklı sistemden oluşan bir toplam sistemin sahip olduğu kuantum durumlarında, alt sistemlerin durumları arasında korelasyon varsa iki sistemin dolanık olduğunu söylenir (Türkpençe, 2006). Dolanıklık, klasik mekanik ve kuantum mekaniği arasında farklılık olan konuların başında yer alır (Özen, 2009). Kuantum ışınlamanın ve kuantum hesaplamanın temelinde dolanıklık yatmaktadır (Bennett, et al., 1993; Nielsen and Chuang, 2000).

1935'te Einstein, Podolsky ve Rosen, kuantum teorisinin eksiksizliğine karşı bir iddia olarak dolanık durumda olan iki parçacıklı bir düşünce deneyini formülize ettiler. Dolanık bir çiftin bir alt sisteminde herhangi bir potansiyel ölçümün sonucunun diğer alt sistemin üzerinde yapılan doğru bir ölçüm sonucunda kesinlikle tahmin edilebileceği gerçeğinden yola çıkarak, yerellik ve gerçeklik varsayımlarını da göz önünde bulundurarak iki tamamlayıcı gözlenebilir için eş zamanlı gizli değişkenlerin olması gerektiği sonucuna vardılar (Dusek, et al., 2006).

İrlandalı fizikçi John Stewart Bell, Einstein'ın istediği gibi yerel ve gerçekçi bir kuramın mümkün olup olmadığı sorusu üzerinde yoğunlaştı. Sonunda, 1964 yılında çok önemli bir adım attı ve yerel gerçekçi kuramlarla kuantum kuramının bazı deneylerde çok farklı öngörülerde bulunduğunu gösterdi. Bell'in aslında tam olarak gösterdiği şey, bütün yerel gerçekçi kuramların deneysel sonuçlarının bugün "Bell Eşitsizlikleri" adı verilen bir takım cebirsel bağıntıları sağladığı, fakat kuantum kuramının bu bağıntılara aykırı sonuçlar ürettiğiydi (Turgut, 2010).

İki ayrı fakat bir şekilde birbirleriyle ilişkili parçacık üzerinde yapılan ölçümler sonucunda, ölçüm cihazlarının ayarları sırasıyla $n_1$ve n_2 birim vektörleriyle temsil edildiğinde ayrık ± 1 değerlerini alan $A(n_1)$ ve $B(n_2)$ -ki, yerellik şartına göre: A yalnızca n_1'e ve B de yalnızca n_2'ye bağlıdır- rastlantısal değişkenleri ele alındığında, A ve B'nin rastlantısallığının yalnızca her ikisinde de ortak olarak bulunan ve bilinmeyen bazı rastlantısal λ parametrelerinden kaynaklandığı varsayılır (gerçeklik varsayımı). Clauser ve arkadaşları tarafından 1969 yılında türetildiği formda Bell eşitsizliği,

$$|C(n_1, n_2) + C(n_1', n_2) + C(n_1, n_2') - C(n_1', n_2')| \leq 2 \tag{2.13}$$

gibidir. Burada $C(n_1, n_2)$ korelasyon fonksiyonu olup bunun için;

$$C(n_1, n_2) = \langle A(n_1)(B(n_2)\rangle = \int A(n_1, \lambda)B(n_2, \lambda)dp_\lambda \tag{2.14}$$

yazılabilir.

$$|\psi\rangle = 1/\sqrt{2}\,(|n, +\rangle_1|n, -\rangle_2 - |n, -\rangle_1|n, +\rangle_2) \tag{2.15}$$

İki yarım spinli parçacığın yukarıdaki (2.15) dolanık durumunda olduğu varsayılarak, böyle bir durum kuantum diliyle ifade edilmeye çalışıldığında; denklemdeki $|n,\pm\rangle$ durum vektörleri, n yönünde spinin iki ortogonal izdüşümüne tekabül etmektedir. Korelasyon fonksiyonu için kuantum öngörüsü aşağıdaki gibidir:

$$C(n_1, n_2) = \langle\psi|(n_1.\sigma_1)(n_2.\sigma_2)|\psi\rangle \quad (2.16)$$

Burada σ_1, σ_2 Pauli matrislerinin vektörleridir. Ölçüm cihazlarının ayarları n_1' ve n_2' arasında 135^0'lik açı varken n_2 ile n_1, n_1 ile n_2' ve n_1' ile n_2 arasında 45^0 açı olacak şekilde ayarlanırsa $|C(n_1, n_2) + C(n_1', n_2) + C(n_1, n_2') - C(n_1', n_2')| = 2\sqrt{2} > 2$ olduğu bulunur (Dusek, et al., 2006).

2.11.2. Orijinal Ekert Protokolü ve Basitleştirilmiş Formu

Ekert protokolü BB84 protokolünün aksine Heisenberg belirsizlik ilkesini kullanmaz. Bu protokolde kuantum durumları dolanık iki foton kullanılır. Dolayısıyla bir taraf diğer taraftaki kuantum durumunu tahmin edebilir. Böylece ortak bir kod anahtarı elde edilir (Şahin ve Selçuk, 2006).

1991 yılında ortaya atılan Ekert protokolüne göre, Alice ve Bob (2.15) durumundaki $-1/2$ spinli çiftten birer parçacık alırlar. Ki iki dolanık $-1/2$ spinli parçacığı veya dolanık polarizasyonlu iki fotonu paylaşıyor olmaları arasında bir fark yoktur. Daha sonra kendi parçacıkları üzerinde ölçüm cihazlarının (örneğin Stern-Gerlach aygıtları) üç yönü ile belirlenmiş üç tabanda ölçümler yaparlar. Kolay olması açısından Alice ve Bob'un yalnızca parçacıkların yayılma doğrultusuna dik düzlemde uzanan yönleri kullandıkları varsayılırsa, Alice'in tabanları dikeyle 0^0, 45^0, 90^0 ve Bob'un tabanları da 45^0, 90^0, 135^0 azimut açılarını yapmaktadır (Duran, 2011). Yani dokuz olası kombinasyon vardır. Kuantum iletimden sonra, Alice ve Bob rastlantısal ve bağımsız olarak ölçüm tabanlarını kurarlarken ayarlar açık kanaldan bildirilir. Aynı tabanlar kullanıldığında, ölçümlerinin sonuçları arasında uyum sağlanır ve kriptografik anahtar oluşur. Alice ve Bob'un aynı tabanı kullanma ihtimali 2/9'dur. Diğer tabanlardaki ölçümlerin sonuçları Bell Eşitsizliklerinin ne kadar ihlal edildiğini ölçmek için kullanılır. Eğer Bell Eşitsizlikleri yeteri kadar ihlal edilmezse ellerindeki kuantum durumun artık $|\psi\rangle$ olmadığı anlaşılır. Yani Eve, kanalı dinlemiş ve dolanıklığı yok etmiş demektir. Diğer taraftan, olabilecek en fazla ihlal olan $\pm 2\sqrt{2}$ limitine ulaşılırsa Alice ve Bob kanalın güvenli olduğundan emin olabilirler (İpekoğlu vd., 2009).

Bir yıl sonra yani 1992'de, Bennett ve arkadaşları doğrudan Bell Teoremine dayanmayan daha basit bir dolanıklık temelli protokol önerdiler. Bu yöntemde hem Alice hem de Bob BB84 protokolüne çok benzeyen bir şekilde sadece spin ölçen cihazlarının iki dik yönüne karşılık gelen iki tabandan birini seçerler. Bunun BB84'ten tek farkı Alice'in seçilmiş bir spin veya polarizasyon durumundaki parçacıkları Bob'a göndermemesi ve kendi parçacığını rastgele ve Bob'dan bağımsız olarak iki eşlenik tabandan biriyle ölçmesidir. Gerisi BB84 ile aynıdır: İletimden sonra Alice ve Bob tabanlarını karşılaştırırlar ve yalnızca aynı tabanı kullandıklarında elde edilen sonuçları saklarlar (Dusek, et al., 2006).

3. KAD SİSTEMLERİ VE YAPILAN DENEYLER

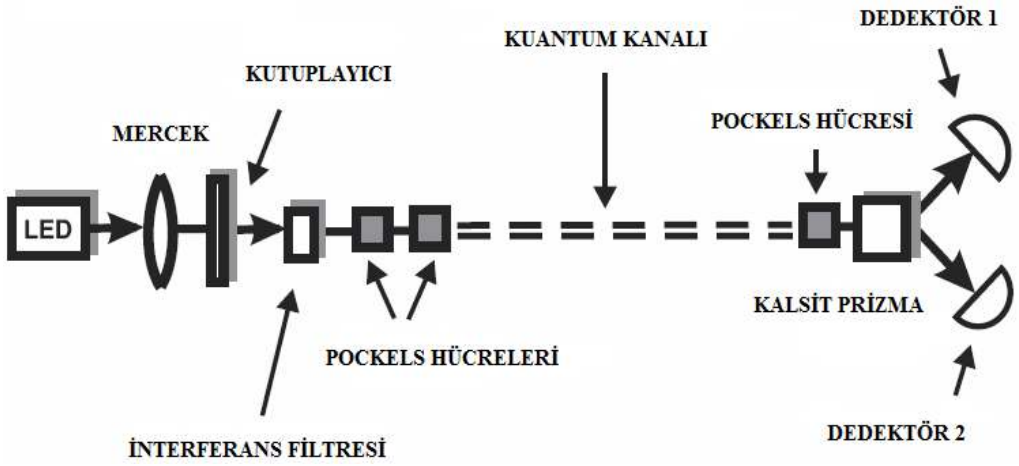
Kuantum anahtar dağıtımı elektro-optik, fiber-optik ve fotonik teknolojileri kapsar. Ayrıca deneysel çalışmalar ile araştırma geliştirme faaliyetlerinin aktif olmasını gerektirir. Laboratuvar çalışmaları ve alan uygulamaları olmaksızın KAD sistemlerinin geliştirilmesi mümkün değildir (Şahin ve Selçuk, 2006). Bu bakımdan, 1989 yılında başarıyla gerçekleştirilen ilk KAD denemesinden günümüze kadar yapılan ve bu alandaki gelişmelere öncülük eden çalışmaların genel bir değerlendirmesi faydalı olacaktır.

3.1. ZAYIF LAZERLER İLE YAPILAN KAD DENEYLERİ

3.1.1. Polarizasyon Kodlama ile Yapılan KAD Deneyleri

Herhangi bir mesaj metni, 0 ve 1'lerden oluşan bir bit dizisine dönüştürülebilir. Kuantum kriptografide bir aşama daha ileri gidilir ve mesaj bir bit dizisine indirgendikten sonra bu bitler fotonların durumları içerisine kodlanır. Fotonlar birçok ilginç özelliği olan elektromanyetik dalgalar olup fotonun bir biti kodlamak için kullanılabilecek özelliklerinden biri polarizasyon –ki günümüzde fotonların faz özelliklerini kullanan KAD teknikleri de mevcuttur- durumudur. Bir fotonu istenen bir yönde polarize etmek için polarizasyon ekseni istenen açıya ayarlanmış bir kutuplayıcı içinden geçirmek gerekir (Toyran, 2003).

Polarizasyon kodlanmış diziden mesaja ait bitleri geri elde etmek için alıcının gelen fotonların her birinin polarizasyonunu ölçebilmesi gerekir. Doğada buna hizmet edebilecek çok uygun bir madde mevcuttur: Kalsit. Kalsit, kuvartz ve turmalin gibi maddeler polarizasyon düzlemleri farklı olan ışıkları farklı şekilde kırma özelliğine sahiptirler. Bu maddelerden uygun şekil verilmiş bir prizma üzerine polarize olmamış bir ışık demeti düşürülürse bu ışığın içindeki dalgalardan sadece polarizasyon düzlemleri cisim içindeki özel bir düzleme paralel olanlar prizmanın içinden dosdoğru geçip diğer tarafından çıkarlar. Dalgaların geri kalan kısmı ya yutulur ya da saptırılır (Toyran, 2003).



Şekil 3.1 İlk KAD deneyi şeması (Bennett, et al., 1989).

Kuantum anahtar dağıtımının pratik olarak uygulanabileceğini gösteren ilk deney 1989 yılında Bennett ve arkadaşları tarafından BB84 protokolü için polarizasyon kodlama üzerine gerçekleştirildi (Şekil 3.1). İlk pratik KAD uygulaması olması açısından önemli olan bu deneyde sinyaller bir ışık yayan diyot (LED) ile üretildikten sonra interferans filtresiyle zayıflatılıp, bir kutuplayıcı ile polarize edildi. 32 santimetrelik serbest uzay kuantum kanalını katedecek kübitler fotonların polarizasyonlarına Pockels hücreleri vasıtasıyla kodlandı. Alınan polarizasyon durumları ise çıkış portları foto çoğaltıcılara bağlı bir Wollaston prizması kullanılarak analiz edildi.

Dört yıl sonra 1993'te, Cenevre Üniversitesinden Gisin ve arkadaşları serbest uzay optik yolunu 1 km'lik optik fiber ile değiştirdi (Müller, et al., 1993; Breguet, et al., 1994). Bu denemede, 800 nm'lik bir yarıiletken lazer, silikon çığ fotodiyotlar tarafından tespit edilecek ışık sinyalleri üretmek için kullanıldı. Optik fiberin kıvrımları, çift kırılmaya sebep olarak ışığın polarizasyon durumunu bozduğu için elle ayarlanabilir bir polarizasyon kontrol cihazı polarizasyonun geçici değişimlerini telafi etmek için kullanıldı.

Şekil 3.2 Cenevre Gölü altındaki 23 km'lik optik fiber hattı (Gisin, et al., 2002).

Gönderici ve alıcının iki farklı şehre (Cenevre ve Nyon) yerleştirildiği ilk deney ise Cenevre grubu tarafından gerçekleştirildi (Müller, et al., 1995). Birbirlerine Cenevre gölü altından geçen 23 km'lik bir fiberle bağlı olan iki istasyon arasında yalnızca %4'lük hata oranı tespit edildi. Fiber kayıplarını azaltmak için 1.3 μm'lik bir lazer kullanıldı ve fotonların sıvı nitrojenle soğutulan germanyum çığ fotodiyotlar ile algılanması sağlandı. Günümüzde özellikle büyük şehirlerde, erişim için kilometrelerle ifade edilen uzak mesafelere fiber hat çekebilmenin zorluğu bazen de imkansızlığı dolayısıyla alternatif bir sistem olarak hatta bazı durumlarda da tek çözüm olarak serbest uzay optik haberleşme sistemleri geliştirilmiştir. Zira atmosfer fiberlerin aksine çift kırılmaya neden olmaz dolayısıyla polarizasyon kodlamaya elverişlidir.

Şekil 3.3 Serbest uzay optik haberleşme sistemi kurulumu. Hattın diğer ucu soldaki resimde görülen büyük beyaz bloğun çatısında olup, sağda ise bu nokta optik pointer ile görüntülenmektedir (http://www.cesnet.cz/doc/techzpravy/2007/mrv-terescope-700/).

Ünlü 1989 Bennett ve Brassard deneyinden sonra serbest uzay kuantum anahtar dağıtımının uygulanabilirliği ilk kez floresan ışıkla aydınlatılmış bir koridorda 150 metrede ve gün ışığında da 75 metrede iletişimi başaran Jacobs ve Franson tarafından 1996 yılında gösterildi. Takip eden ve belli başarılara ulaşan bir dizi deneyler sonrasında 2002'de Hughes ve arkadaşları tarafından 10 km'lik mesafede serbest uzay kuantum anahtar dağıtımı gerçekleştirildi. Fakat şimdiye kadar en uzun mesafede başarıyla yapılan serbest uzay kuantum anahtar dağıtımı H. Weinfurter'in Münih grubu tarafından gerçekleştirildi (Kurtsiefer, et al., 2002a; 2002b). Bu grup, yükseklerdeki ince atmosfer tabakasının ve daha az hava türbülansının avantajından faydalanabilmek amacıyla Alplerin yüksek kısımlarına çıktı. Gönderici 2962 metre yükseklikte Zugspitze'nin zirvesinde ve alıcı da 23.4 km uzaklıktaki 2244 metre rakımlı Karwendelspitze'deydi.

3.1.2. Faz Kodlama ile Yapılan KAD Deneyleri

Faz kodlamada, polarizasyon kodlamada kullanılan farklı polarizasyonların yerine Mach-Zehnder interferometresinin (girişim ölçerinin) iki kolu arasındaki farklı faz kaymaları söz konusudur.

Mach-Zehnder interferometresinde giren fotonun aygıttan çıkarken kullanabileceği iki olası çıkış rotası vardır. Fakat burada girişim olgusu işin içine girer ve fotonun bunlardan sadece birini kullanmasına izin verir. Girişim dalgalar için geçerli bir kavramdır ve tüm temel parçacıklar gibi fotonun nerede hangi olasılıkla bulunduğunu bildiren olasılık dalgaları da aynı girişime uğrar. İşte bu nedenle Mach-Zehnder interferometresi uygun şekilde ayarlanarak fotonun sadece tek bir çıkışı kullanması sağlanabilir (Turgut, 2003b).

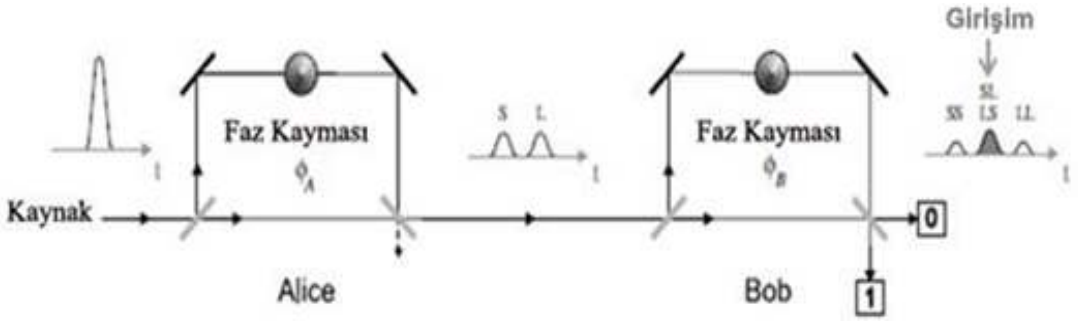
Faz kodlama yapılırken gönderici interferometrenin bir kolundaki faz kaymasını, alıcı da diğer koldaki faz kaymasını kontrol eder. Eğer gönderici ve alıcının faz kaymaları aynı veya 180^0 farklı ise bundan sonra alıcının demet bölücüsündeki fotonun davranışı çıkışlardan birindeki yapıcı girişim ve diğerindeki yıkıcı girişim dolayısıyla belirleyicidir. Kollar arasındaki toplam faz kayması 180^0'nin tam katlarından farklı ise fotonlar detektörlerde rastgele tespit edilirler. BB84 protokolü ile faz kodlama yaparken Alice interferometreye zayıf ışık sinyalleri gönderir ve $\emptyset_A$ fazını rastgele 0^0, 90^0, 180^0 veya 270^0'ye ayarlar. Bob da rastgele ve Alice'den bağımsız olarak $\emptyset_B$ fazını 0^0 veya 90^0'ye ayarlar (Dusek, et al., 2006).

Alice			Bob	
Bit value	ϕ_A	ϕ_B	$\phi_A - \phi_B$	Bit value
0	0	0	0	0
0	0	$\pi/2$	$3\pi/2$	?
1	π	0	π	1
1	π	$\pi/2$	$\pi/2$	?
0	$\pi/2$	0	$\pi/2$	?
0	$\pi/2$	$\pi/2$	0	0
1	$3\pi/2$	0	$3\pi/2$	?
1	$3\pi/2$	$\pi/2$	π	1

Tablo 3.1 BB84 protokolü ile faz kodlama (Gisin, et al., 2002).

Pratikte uzun mesafelerde eşit ve sabit faz şartlarını Mach-Zehnder interferometresinin iki farklı kolunda korumak çok zordur. Fakat bu problemin çözümü Bennett tarafından 1992 yılında sunulmuştur. Bennet'in çözümü şöyle tarif edilebilir:

İletişim kuran iki taraf bir zaman multipleksi çalıştırır ve cihazlarını birbirine bağlamak için yalnızca tek optik fiber kullanırlar (Şekil 3.4). Böylece iki dengelenmemiş Mach-Zehnder interferometresi kullanılmış olur. Her bir interferometrenin uzun ve kısa kolları arasındaki yol farkı lazer sinyalinin genişliğinden büyüktür. Fakat her iki interferometre için yol farkları aynıdır. Fotonun ilk olarak uzun koldan (L) ve ondan sonra kısa koldan (S) geçmesi durumunu, önce kısa sonra uzun koldan geçmesi durumundan ayırt etmek mümkün değildir. Süperpozisyon ilkesine göre, fotonun izleyebileceği yolların üzerinde ona iz bıraktıracak bir engel yoksa, yani iki yol birbirinden ayırdedilemezse, foton her iki yolu aynı anda alır (Kolkıran, 2010). Bu ayırt edilemezlik son demet bölücüde girişime sebep olur. Dolayısıyla merkez tepe noktası için (Şekil 3.4'te sağda) sistem aynen tek bir dengelenmiş Mach-Zehnder interferometresi gibi davranır.



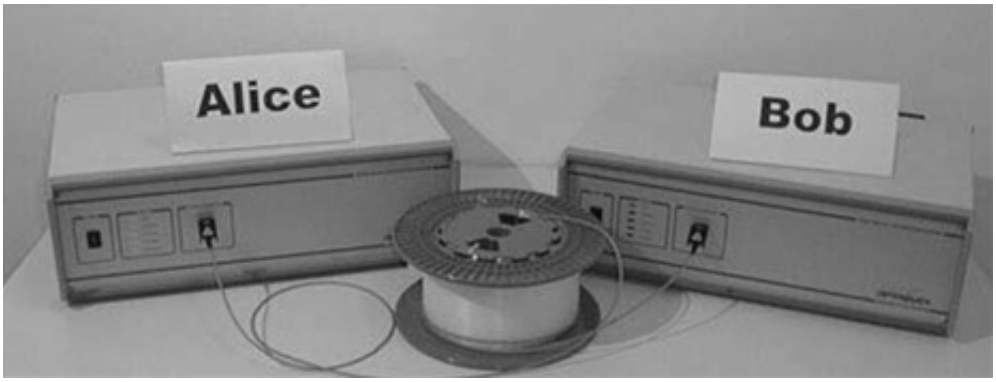
Şekil 3.4 Çift Mach-Zehnder interferometreli faz kodlama sistemi (Dusek, et al., 2006).

Faz kodlama tekniği üzerine ilk pratik sistem Townsend ve arkadaşları tarafından 1993 yılında kuruldu. Denemede, sinyal bir makaraya sarılı 10 km'lik fiber boyunca gönderildi. Daha sonra bu sistem her iki interferometredeki uzun kollarda polarizasyon 90^0 döndürülecek şekilde yeniden uyarlandı ve zaman multipleksi bir polarizasyon multipleksi ile desteklendi. Yani göndericinin interferometresinin çıktısı ve alıcının interferometresinin girdisinde polarizasyon demet bölücüler vardı. Bu teknik ile girişim yapmayan yan tepeler bastırılmış oldu (Townsend, 1994). Ayrıca, mesafe 30 km'ye çıkarıldı (Marand and Townsend, 1995). Daha sonra Townsend 1997'de hem kuantum anahtar dağıtımı hem de klasik iletişimi aynı fiber üzerinden farklı dalgaboylarında sağlamak üzere dalgaboyu bölme multipleksini test etti. Yine çift

Mach-Zehnder interferometreli bir KAD sistemi Los Alamos National Laboratory'de denendi (Hughes, et al., 1996; 2000). Bu deneme ise 48 kilometreye yakın döşenmiş bir optik fiber üzerinde yapıldı. Bir diğer fiber kullanımına dayalı sistem de 830 nm'de Dusek ve arkadaşları tarafından kuruldu. 500 metrelik mesafede kuantum kimlik tanımlama sistemi olarak kullanılan sistemde interferometrelerin aktif stabilizasyonu sağlandı ve pratik kuantum anahtar dağıtımı için tüm destek prosedürleri programlandı. Kimura ve arkadaşları tarafından 2004'te silika tabanlı entegre optik interferometreli sistem geliştirildi ve 150 km'lik bir mesafede denendi. Toshiba Avrupa Araştırma Birimi aktif interferometre stabilizasyonu için yeni bir yöntem uygulayarak 1550 nm'de otomatik bir sistem geliştirdi ve bu sistemi 122 km'ye kadar mesafelerde denedi (Gobby, et al., 2004; Yuan and Shields, 2005).

Polarizasyon kodlama veya çift Mach-Zehnder interferometre kullanan sistemlerin ikisi de polarizasyonların ve/veya fazların dalgalanma ve kaymalarını telafi etmek için aktif bir stabilizasyon gerektirir. Müller ve arkadaşları 1997'de, Martinelli'nin 1989'da ortaya attığı bir fikirden ilham alarak optik ve mekanik dalgalanmaların otomatik olarak pasif bir yöntemle telafi edildiği faz kodlamalı KAD aygıtının nasıl uygulanacağına dair ilginç bir yöntem önerdi. Bu yöntemde: Ortogonal lineer polarizasyonların karşılıklı geciktirilen iki güçlü sinyali Bob'dan Alice'e gider. Bu sinyaller -ki bir kısmı aynı zamanda senkronizasyon amaçlı kullanılır- Alice'in tarafında zayıflatılır. İlk sinyal faz kaymalıdır çünkü Alice bu yolla bilgiyi kodlar ve her iki sinyal bir Faraday aynasından yansıtılır. Daha sonra, bu zayıf sinyaller Bob'a geri döner. Aynı hattan fakat değişmiş polarizasyonlarla geri döndüklerinden, sinyallerin ilk yolculuklarındaki polarizasyon bozuklukları dönüş yolunda telafi edilir. Bob'un tarafında ilk sinyal dengelenmemiş Mach-Zehnder interferometresinin uzun kolundan geçerken, ikinci sinyal kısa koldan geçer. Bob kollardan birinde kendi faz kaymasını uygular. Sinyaller arasındaki orijinal gecikme aynı dengelenmemiş interferometre tarafından sağlandığından bu interferometrenin stabilizasyonu gerekmemektedir. Çalıştırılması için herhangi bir özel optik ayarlama gerekli olmadığı için bu sistem genellikle "tak ve kullan" olarak adlandırılır. Tak kullan sisteminin aynı zamanda bazı eksiklikleri de vardır: Sinyallerin ilk önce Bob'dan Alice'e gitmesi ve sonra da geri gelmesi durumu tüm işlemin zamanlamasını karmaşıklaştırır ve iletim hızını etkili bir

şekilde azaltabilir. Sorun, özellikle kendini Rayleigh geri saçılımı ile gösterir. Hata oranını arttırmamak için Bob'dan gelen kuvvetli sinyaller diğer yönden yayılan zayıf sinyaller ile karşılaşmamalıdır. Ayrıca, zayıflatılıp bilgi kodlanmadan önce güçlü sinyallerin Bob'dan Alice'e tüm yolu geçmeleri gerektiğinden, Eve'in örneğin foton istatistikleri gibi bazı özellikleri değiştirme fırsatı vardır. Sistem ayrıca bazı Truva atı saldırılarına karşı daha hassastır (Dusek, et al., 2006).



Şekil 3.5 Ticari bir tak kullan KAD sistemi (Sergienko, 2006).

Tak ve kullan tekniği ile ilgili ilk deneysel gerçekleştirme 1997 yılında Cenevre gölü altından geçen 23 km uzunluğundaki optik fiber üzerinde Zbinden ve arkadaşları tarafından yapıldı. Daha sonra, tamamen otomatik sistem aynı fiber üzerinde denendi (Ribordy, et al., 2000). Bu otomatik sistem 1300 nm'de BB84 protokolü uygulanarak çalıştırıldı. 1300 nm'de çalışan benzer bir otomatik dengeleyicili sistem de IBM'de bağımsız olarak geliştirildi (Bethune and Risk, 2000). Bu sistem ise makaraya sarılı 10 km uzunluğundaki bir fiber üzerinde denendi. Burada Bob tarafından gönderilen sinyaller Rayleigh geri saçılımından kaçınmak için düşük bir yoğunlukta tutuldu. Senkronizasyon, bir dalgaboyu bölme multipleksi kullanılarak, 1550 nm'de klasik sinyaller ile sağlandı. Nielsen ve arkadaşları 2001'de 1310 nm'de çalışan bir sistem kurdu ve bu sistemle 20 km'lik fiber üzerinden bir anahtarı iletti. A. Karlsson'un grubu tak ve kullan tekniğinin fiberlerde 1550 nm'de de uyarlanabileceğini gösterdi (Bourennane, et al., 1999). Daha sonra, geliştirilmiş bir Cenevre tak ve kullan sistemi 1550 nm'de Cenevre ile Lozan arasında 67 km uzunluğunda bir optik fiber üzerinde çalıştırıldı (Stucki, et al., 2002).

Daha önce Bölüm 2.10'da bahsedilen tuzak durum yönteminin ilk deneysel uygulaması Zhao ve arkadaşları tarafından 2005'te yapıldı. Grup bunun için id Quantique tarafından üretilmiş ticari bir tak ve kullan KAD sistemi kullandı. Anahtar dağıtımı 15 km'lik bir mesafede denendi. Protokol olarak, BB84 protokolü ile birlikte pratik olması açısından tek tuzak durum içeren tuzak-durum protokolü kullanıldı. Sinyal ve tuzak durumların ortalama yoğunlukları sırasıyla 0.8 ve 0.12 foton olarak seçildi.

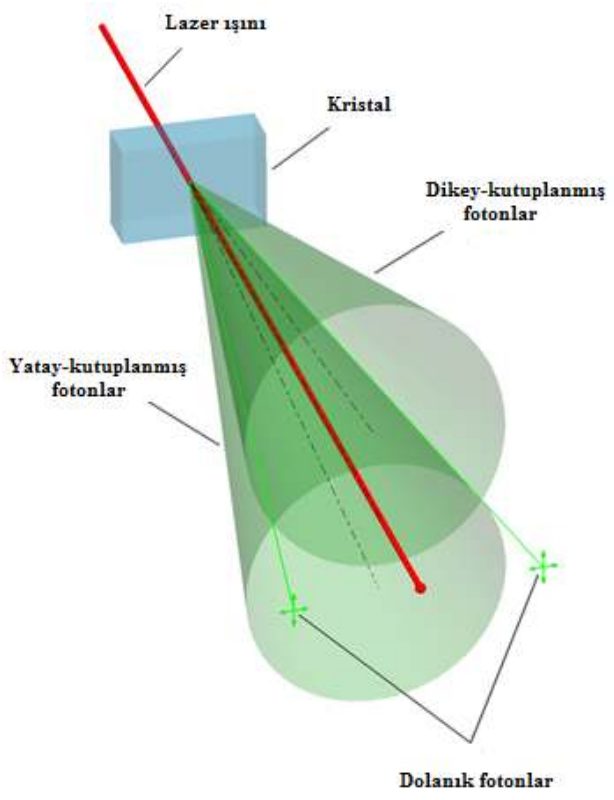
Gisin ve arkadaşları 2004'te spesifik bir protokole dayanan ve zayıf lazer sinyali kullanılan uygulamalar için yeni bir pratik KAD tekniği önerdi. Bu teknikte anahtar, Bob'a gelen sinyallerin geliş sürelerinin basit bir ölçümü ile elde edilir. Bir gizli dinleyicinin olup olmadığı ek bir gözlem hattı üzerinde kurulu bir interferometre tarafından kontrol edilir. Her bir bit iki sinyalin bir dizisi içerisine kodlanır: Bir boş ve bir boş olmayan veya tam tersi. Herhangi iki boş olmayan sinyal arasında kaynak olarak bir mod-kilitli lazer kullanıldığından bir faz bağdaşıklığı vardır. Bazı sinyaller Bob'un demet bölücüsünde yansıtılır ve dengelenmemiş Mach-Zehnder interferometresine (gözlem hattı) gider. Kuantum bağdaşıklığın rol oynadığı yer burasıdır. Eğer bağdaşıklık bozulmazsa yalnızca interferometrenin belirli bir çıktısındaki detektör bazı anlarda sinyal gönderebilir. Bu durum bir gizli dinlemenin tespit edilmesini sağlar. Bununla ilgili ilk deneysel gerçekleştirme ise Stucki ve arkadaşları tarafından 2005 yılında yapıldı (Dusek, et al., 2006).

3.2. KUANTUM DOLANIKLIK İLE YAPILAN KAD DENEYLERİ

Kuantum dolanıklık modern bilgi teknolojilerinin üretilmesi ve geliştirilmesi için önemli bir kaynaktır ve özellikle kuantum anahtar dağıtımı konusunda dolanık durumların incelenmesi oldukça önemlidir. Dolanıklık temelli KAD protokollerinin çalışma prensibinden teorik olarak daha önce Bölüm 2.11'de bahsedilmişti. Bu protokollerin pratik uygulamalarında ise sadece fotonların dolanık durumları kullanılır. Buna rağmen, örneğin fotonların polarizasyonlarındaki dolanıklık, enerji ve zaman dolanıklığı veya enerji-zaman dolanıklığının özel bir şekli olan zaman kayıtlı dolanıklık gibi dolanıklığın farklı türleri kullanılabilir.

3.2.1. Polarizasyon Dolanıklığı ile Yapılan KAD Deneyleri

Kuantum dolanıklık, kuantum ışınlama, kuantum bilgisayarlar ve kuantum kriptografi gibi merak uyandıran günümüz biliminin en önemli uğraşları üzerine araştırmalarını içeren fiziğin en ilginç çalışma alanlarından biri olup bu terim, ışığın parçacıkları olan fotonlar gibi çok çok küçük kuantum niceliklerin nasıl birlikte olduğundan, birbirlerine nasıl bağlandığından ve bilginin kuantum bitlerini nasıl paylaştığından bahseder. Dolanıklık atom altı parçacıklar arasındaki etkileşmelerle oluşturulur. Böyle etkileşmelerin sayısız şekilde olabileceği söylenebilir. Diğer taraftan en yaygın kullanılan yöntemlerden biri polarizasyon dolanık bir foton çifti üreten kendiliğinden parametrik alt dönüştürme (KPAD) yöntemidir.



Şekil 3.6 KPAD ile polarizasyon polarizasyon dolanık çiftler üretilmesi. Eğer işlem sonunda üretilen dolanık fotonlar aynı polarizasyondalarsa buna "tip 1 ilişki", birbirlerine dik polarizasyondalarsa da "tip 2 ilişki" denir (http://en.wikipedia.org/wiki /Spontaneous_parametric_down-conversion).

Polarizasyon dolanıklığı kullanılarak yapılan kuantum anahtar dağıtımında gönderici ve alıcının her birine aşağıda verilen durumlardan birindeki dolanık çiftin bir fotonu verilir (Dusek, et al., 2006).

$$1/\sqrt{2}\,(|V\rangle_A|V\rangle_B \pm |H\rangle_A|H\rangle_B),\;\; 1/\sqrt{2}\,(|V\rangle_A|H\rangle_B \pm |H\rangle_A|V\rangle_B) \qquad (3.1)$$

Burada $|V\rangle$ ve $|H\rangle$ sırasıyla dikey ve yatay lineer polarizasyonlu tek foton durumlarını simgelemektedir. Çiftler lineer olmayan optik kristallerde bir parametrik alt dönüştürme işlemi ile hazırlanır. Polarizasyon dolanıklığı ya tip 2 faz çakışmalı bir kristal ile veya birbirine yakın ve optik eksenleri birbirlerine dik olarak yerleştirilmiş tip 1 faz çakışmalı iki kristal ile sağlanır. Ayrıca gönderici ve alıcı polarizasyon ölçüm tabanlarını hızla değiştirebilen polarizasyon analizcilerine sahip olmalıdır (Dusek, et al., 2006).

Polarizasyon dolanıklığı kullanılarak gerçekleştirilen ilk iki deney 2000 yılında kayıtlara geçmiştir. İlk deneyde Zeilinger'in grubu 702 nm'de foton çiftleri üretmek üzere tip 2 faz çakışmalı bir BBO kristalini, üzerine argon iyon lazer pompalayarak kullandı. Grubun analizcilerinde hızlı modülatörler, kutuplayıcı demet bölücüler ve silikon çığ fotodiyot detektörler vardı. Böylece döşenmiş tek modlu fiberlerde 360 metrelik uzaklıkta kuantum anahatar dağıtımı gerçekleştirdiler. İkinci deneyde ise Los Alamos'daki Kwiat'ın grubu üzerine argon iyon lazer pompalanan tip 1 faz çakışmalı iki BBO kristali ile çalışarak 702 nm'lik yarılmış dalgaboylarında foton çiftleri ürettiler. Protokol olarak orijinal Ekert protokolünü kullandılar ve serbest uzayda bir kaç metrelik bir uzaklıkta anahtar dağıtımını sağladılar. Ayrıca, deneme sırasında deneysel farklı gizli dinleme stratejilerini de simüle ettiler. Daha sonraki bir tarihte, 2004 yılında bir deney de Poppe ve arkadaşları tarafından Viyana'da gerçekleştirildi. Bu denemede ise 810 nm'deki polarizasyon dolanık çiftler, yarıiletken lazer ve BBO kristali kullanılarak tip 2 parametrik alt dönüştürme ile üretildi ve gizli anahtar 1.45 km uzunluğundaki fiber üzerinden dağıtıldı.

3.2.2. Enerji-Zaman Dolanıklığı ile Yapılan Faz Kodlama Deneyleri

Enerji-zaman dolanıklığı ile yapılan faz kodlamada kullanılan çift fotonlu dolanık durumlar takribi olarak aşağıdaki formdadır.

$$\int d\omega \xi(\omega) \, |\omega\rangle_A |\omega_0 - \omega\rangle_B \tag{3.2}$$

Yukarıdaki ifadede $|\omega\rangle$, ω frekansındaki bir tek foton durumunu simgelemektedir. ω_0 pompalanan lazerin optik bir frekansı olup, $\xi(\omega)$ her bir frekans bileşenlerinin dağılımını ifade eder. Çiftler yine lineer olmayan optik kristallerdeki parametrik alt dönüştürme ile üretilir. Denklem (3.2)'de verilen eşitliğe yakın durumlardaki fotonlar geniş bağdaşıklık zamanlı bir lazer, kristale pompalandığında üretilirler (Dusek, et al., 2006).

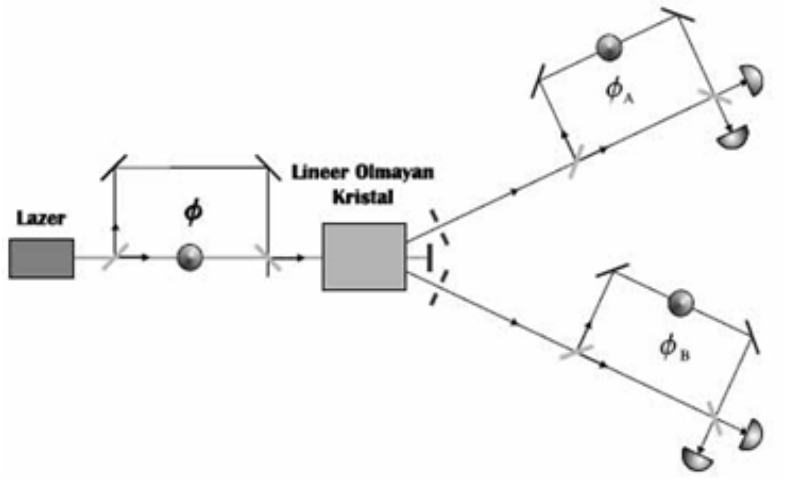
Uygulama aşamasında, Alice ve Bob birer foton edinirler ve bir interforemetre Bob'un tarafında, diğeri ise Alice'in tarafında olmak koşuluyla eşit şekilde dengesiz Mach-Zehnder interferometrelerinden geçmelerini sağlarlar. Her interferometrenin uzun ve kısa kolları arasındaki yol farkı üretilen fotonların bağdaşıklık uzunluğundan daha uzun fakat pompalanan lazerin bağdaşıklık uzunluğundan daha kısa olmalıdır. Yol farkları ise her iki interferometre için aynı olmalıdır. Bir çiftten iki fotonun tespit anları çok sıkı bir şekilde ilişkilidir. Fakat bu çakışık tespitlerin tam zamanları belirsiz ve rastlantısaldır. Dolayısıyla Alice ve Bob, fotonların ikisinin de interferometrelerin uzun kollarından geçtiği ve ikisinin de kısa kollardan geçtiği durumları ayırt edemezler. Bu durum dördüncü mertebeden bir girişime yol açar. Alice ve Bob ölçüm tabanlarını interferometrelerinin kolları arasındaki faz kaymalarını değiştirerek seçerler. Örneğin kaymaları 0^0 ve 90^0 olarak rastgele ve bağımsız olarak düzenlerler. Bir fotonun kısa koldan diğerinin ise uzun koldan geçtiği durumlar yok sayılır (Dusek, et al., 2006).

Orijinal olarak 1989 yılında Franson tarafından farklı sebeplerle tasarlanan bu sistemin fiberlerde kuantum anahtar dağıtımı için kullanılabileceği fikri Ekert ve arkadaşları tarafından 1992'de ortaya atıldı. Pratik sistem ise ilk olarak Cenevre Üniversitesinden Ribordy ve arkadaşları tarafından 2001 yılında denendi. Grup, 810

nm ve 1550 nm'lik asimetrik dalgaboylarına sahip dolanık çiftler üretebilmek için frekansı ikiye katlanmış bir Nd-YAG lazeri ve $KNbO_3$ kristali kullandı. Kullanılan 810 nm'lik dalgaboyu, Alice'in tarafında verimli ve düşük gürültülü Si-APD foton sayaçları kullanabilme avantajı sağladı. Burada kaynak ve Alice'in analizcisi arasındaki mesafe oldukça kısaydı. Diğer fotonun 1550 nm'lik dalgaboyu, optik fiberlerin düşük kayıp aralığına uyum sağladı ve dolayısıyla bu foton kaynak ile Bob arasındaki daha uzun olan yolu kat etti. Bob burada kaynağa bir makaraya sarılı 8.5 km. uzunluğunda optik fiber ile bağlıydı. Pasif kurulum kullanıldı. Her istasyonda birer adet olmak üzere iki ölçüm tabanı kutuplayıcı bir demet bölücü kullanılarak pasif ve rastlantısal olarak seçildi. Bir fiziksel interferometre, ışığın iki farklı polarizasyonu için farklı faz ayarları ile iki interferometre gibi davrandı.

3.2.3. Zaman Kayıtlı Dolanıklık ile Yapılan Faz-Zaman Kodlama Deneyleri

Bu yöntem yukarıda anlatılan faz kodlama ile benzer biçimde çalışmaktadır. Fakat burada pompa demetine yerleştirilmiş bir tane daha dengelenmemiş Mach-Zehnder interferometresi vardır ve darbeli bir kaynak kullanılmaktadır. Cihaza ait şema Şekil 3.7'de verilmiştir.



Şekil 3.7 Zaman kayıtlı dolanıklık ile KAD için şematik kurulum (Dusek, et al., 2006).

Üretilen çift ise aşağıdaki durumla tanımlanabilir:

$$1/\sqrt{2}\,(e^{i\emptyset}|S\rangle_A|S\rangle_B - |L\rangle_A|L\rangle_B \quad (3.3)$$

Burada S ve L sırasıyla interferometrenin kısa ve uzun kollarından geçen pompa sinyallerinin katkılarını simgelemektedirler. Her üç interferometrenin yol farkları aynı olmalıdır. Alice her lazer sinyalinden sonra bir fotonu üç farklı zaman aralığında tespit edebilir: Birincisi hem pompalanan sinyalin hem de Alice'in fotonunun kısa kollardan geçtiği duruma (SS); ikincisi kısa ve uzun kollardan geçtikleri duruma veya tersine (SL veya LS) ve üçüncüsü de hem pompalanan sinyalin hem de Alice'in fotonunun uzun kollardan geçtiği duruma(LL) tekabül eder. Bob'un tespitleri için de aynı şey geçerlidir. Bir gizli anahtar elde etmek için, Alice ve Bob, her ikisinin de birinci ya da üçüncü zaman aralığında fakat bunu açıklamadan ve hangi detektörde olduğu fark etmeksizin bir foton tespit ettiği zamanki olaylar ve her ikisinin de hangi detektörde olduğunu açıklamadan ikinci zaman aralığında detektör sinyalleri tespit ettiği zamanki olaylar üzerinde açık kanal yoluyla anlaşırlar. İlk olayda Alice ve Bob, birbirleriyle uyumlu tespit zamanları olmak koşuluyla, birinci ve üçüncü zaman aralığına farklı bit değerleri atarlar. İkinci olay, yani her iki fotonun da ikinci zaman aralığında tespit edilmesi durumu, yukarıda tarif edilen faz kodlama yöntemine denktir (Dusek, et al., 2006).

Bu teknik Brendal ve arkadaşları tarafından 1999 yılında ortaya atıldı. Deneysel gerçekleştirmesi ise Tittel ve arkadaşları tarafından 2000 yılında yapıldı. Yalnızca laboratuarda test edilen sistemde $KNbO_3$ kristali ve darbeli bir yarıiletken lazer diyot kullanıldı. Alt dönüştürülmüş fotonların dalgaboyu 1310 nm'di. Daha sonra, zaman kayıtlı dolanık kübitlerin dağıtımı 50 km'lik optik fiber üzerinden uygulamalı olarak gösterildi (Marcikic, et al., 2004).

4. IŞIK KAYNAKLARI

Kuantum anahtar dağıtımı protokolleri türüne özgü olarak ışık fotonunu alarak kuantum dolanıklık veya Heisenberg belirsizlik ilkesinden faydalanırlar. Pratik kuantum anahtar dağıtımı gerçekleştirmelerinde en sık kullanılan ışık kaynakları lazerlerdir. Fakat bir kuantum hattında kullanılan sinyal içindeki iki veya daha fazla

foton, PNS tipi bir saldırıya fırsat sunacağından bir gizli dinleyici için bulunmaz fırsattır. Dolayısıyla anahtar dağıtımının güvenliğinin önemli bir bölümünü tek fotonlar üretmek oluşturur. Bu talep üzerine tek fotonlar üretmek için çeşitli yöntemler ortaya konmuştur.

4.1. ZAYIF LAZERLER

Lazerin temeli, atom veya molekül enerji düzeyleri arasındaki elektron geçişleri ile oluşan ışık fotonlarına dayanır. Bir atomun iki enerji düzeyi E_2 ve E_3 olsun, $E_3 > E_2$ olduğu farzedilirse, minimum enerji ilkesine göre atom veya moleküller düşük enerji seviyesinde olmak istediklerinden E_3 seviyesindeki elektron kendiliğinden E_2 seviyesine inecektir. Ama bu sırada enerjisi $E_3 - E_2 = h\gamma$ olan bir foton salar. Burada γ fotonun frekansıdır. Eğer elektron bu salınımı kendiliğinden yaparsa salınan fotonun yönü tamamen rastgeledir. Ancak eğer E_3 düzeyindeki elektron $E_3 - E_2$ enerjisindeki başka bir fotonla etkileşerek E_2 düzeyine inerse bu şekilde salınan fotonun yönü ve fazı geçişe etki eden fotonla aynı olacaktır. Bu ikinci geçiş biçimine "uyarılmış salınım" denir ve lazerin çalışmasının ana ilkesidir (http://tr.wikipedia.org/wiki/Lazer). Pratik KAD sistemlerinde lazerler en sık kullanılan kaynaklardır. Lazer ışımasında Poisson olasılık dağılımına göre n foton bulunma ihtimali aşağıdaki gibidir (Güngördü, 2010).

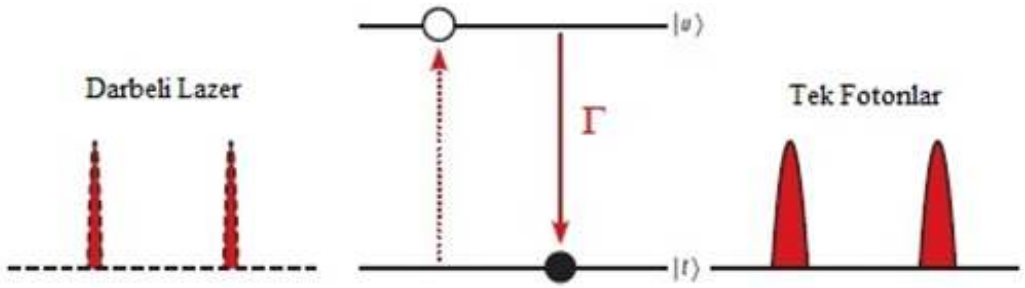
$$p(n) = e^{-\mu}\frac{\mu^n}{n!} \tag{4.1}$$

Burada μ ortalama foton sayısı olup, görülmektedir ki çok küçük μ'ye sahip yüksek derecede zayıflatılmış lazer sinyali iyi bir tek foton Fock durumuna karşılık gelir. Çünkü birden fazla fotonun $p_{multi}/p(1)$ olasılığı $\mu \to 0$ iken sıfıra yaklaşır. Burada problem artan $n = 0$ boş durumlarıdır. Örneğin $\mu = 0.1$ seçilirse, $p(0) = 0.905$, $p(1) = 0.090$ ve $p_{multi} = 0.005$ olur. Boş sinyaller iletim hızını düşürür. Bu da detektörün karanlık sayımlarından daha önemli bir sorundur. Çünkü detektörlerin boş olanlar da dahil her sinyal için aktif olmaları gerektiğinden dolayı boş sinyallerin oranı azalan μ ile artar fakat karanlık sayım oranı sabit kalır. Bu durum, keyfi olarak düşük ortalama foton sayılarının kullanımını engeller (Dusek, et al., 2006).

Detektör karanlık sayımlarının varlığı ve sistemdeki kayıplar, yasal kullanıcıları mümkün olan en yüksek ortalama foton sayısını kullanmaya yöneltir. Diğer yandan, çoklu foton sinyallerinden dolayı sızabilecek potansiyel bilgi ihtimali ise kullanıcıları ortalama foton sayısını mümkün olduğu kadar düşük tutmaya zorlar. Uygun ortalama foton sayısı verilen şartlarda güvenli anahtar değerini en üst seviyeye çıkarır.

4.2. TEK FOTON KAYNAKLARI

Günlük hayatta karşılaşılan ışık kaynakları belli bir spektral aralıkta birçok fotonun üretilmesi ile elde edilir. Fotonları tek tek üreten bir üreteç doğada bulunmamaktadır. Dolayısıyla, bir tek foton üretecini ancak yapay olarak elde etmek mümkündür (Küçükkara ve Kiraz, 2010).



Şekil 4.1 Tek foton üreteci şeması (Küçükkara ve Kiraz, 2010).

Tek foton üreteci tek bir atomun darbeli bir lazer ile uyarılmasını temel alır. Her lazer darbesi atomun temel enerji seviyesinden uyarılmış enerji seviyesine geçişini sağlar. Kendiliğinden ışıma etkisi sayesinde atom bir foton yayarak temel enerji seviyesine geri döner. Böylece her uyarıcı lazer darbesi ile tek foton üretilir. Tek foton üreteci için gerekli en önemli koşul atomların tek tek tuzaklanabilmesidir. Bu bakımdan tek iyon, tek kuantum nokta veya tek molekül gibi tuzaklanması daha kolay olan yapılar da tek foton üreteci uygulamaları için tercih edilir. Son 10 yıldır bu yapılar kullanılarak değişik tek foton üreteçleri geliştirildi ve tek foton üreteci kuantum optik araştırmalarında ihtiyaç duyulan temel bir ışık kaynağı olarak literatürdeki yerini aldı (Küçükkara ve Kiraz, 2010).

4.2.1. Parametrik Alt Dönüştürme

KPAD ile üretilmiş foton çiftleri kullanılarak tek foton benzeri durumlar hazırlanabilir (Hong and Mandel, 1986). Burada önemli olan çiftin fotonları arasında sıkı bir zaman korelasyonu olmasıdır. Yani, ideal durumda eğer yan sinyalin yoluna bir foton sayısı detektörü yerleştirilir ve bu dedektör bir foton tespit ederse, aynı anda yani femtosaniyeler mertebesinde bir zaman aralığında sinyal demetinde de bir foton bulunmalıdır. Fakat şunu da eklemek gerekir ki gerçekte fibere yapılan verimsiz bir eklemeden kaynaklanan sinyal demetindeki kayıplara bağlı olarak ve kısmen de tetik detektörünün karanlık sayımları yüzünden, tetik detektörü sinyal gönderse bile bazen düşük bir olasılıkla da olsa sinyal ışınında foton olmayabilir. Ayrıca pratik olarak uygulanabilir hemen hemen tüm detektörler foton sayılarını ayırt edemezler ve kuantum verimlilikleri %100'ün ciddi şekilde altındadır. Dolayısıyla, aynı zamanda bir tetik tespitinden sonra sinyal ışınında birden fazla foton olması olasılığı da sıfır değildir. Diğer taraftan, bir pompa fotonunun alt frekans fotonları çiftine dönüşümünün verimliliği çok düşüktür. Dolayısıyla çoklu foton durumlarının üretilmesi ihtimali de yine düşüktür. Bu durum gerçekleşse bile çoklu foton durumlarını elemek için tetikleme için kullanılan yan sinyal demetinin birkaç detektöre bölünmesi esasına dayanan teknikler mevcuttur. Birden fazla detektör sinyalinin alındığı durumlar elenir.

KPAD tek foton benzeri kaynağının, zayıflatılmış lazerlere kıyasla en önemli avantajı boşluk katkılarını yani boş sinyallerin yüzdesini önemli ölçüde azaltmasıdır. Teknolojik açıdan bu kaynakların kullanılması mümkün görünmekle birlikte, diyot lazer pompalanmış kızılötesine yakın bölgede yayım yapan KPAD kaynakları kompakt ve sağlam biçimde imal edilebilirler (Volz, et al., 2001).

4.2.2. Renk Merkezleri

Elmasın renk merkezleri tek foton kaynakları araştırması kapsamında çalışılan bir alandır. Renk merkezleri bir kristal örgüsündeki safsızlıklara ve boşluklara bağlı kusurlardır. Bu tür kusurları olan kristaller göreceli olarak daha kolay hazırlanabilirler. Renk merkezleri temelli kaynakların en büyük avantajı oda sıcaklığında çalışmalarıdır.

Sentetik elmastaki nitrojen-boşluğu merkezleri özellikle yoğun bir şekilde incelenmiştir (Kurtsiefer, et al., 2000; Brouri, et al., 2000; Beveratos, et al., 2001). Bu merkezler yedek bir nitrojen atomu ve komşu örgü pozisyonundaki bir boşluktan oluşur. Her bir nitrojen atomu 532 nm'de odaklanmış bir lazer demeti ile uyarılır. Floresans sebebiyle, atom sonuç olarak 690 nm civarında merkezlenmiş bir spektrumla bir foton yayar. Güçlü bir ayrışma gözlemlenir. Bu kaynakların zayıf noktası üretilen sinyallerin yaklaşık 100 nm'lik geniş spektrumudur. İletim ortamının optik özellikleri (soğurma, kırılma indisi, v.b.) dalgaboylarının bu geniş aralığında değişirler. Fakat, son yıllarda fotonları oda sıcaklığında 802 nm'de yalnızca 1 nm civarında bir spektral genişlikte yayabilen yeni bir tür kristal kusuru bulunmuştur. Bu renk merkezi gerçek bir elmas içerisinde dört nitrojen atomu tarafından çevrelenmiş bir nikel iyonundan oluşmaktadır (Gaebel, et al., 2004).

Renk merkezleri üzerine kurulu tek foton kaynaklarının temel problemleri hali hazırda hacimli kristallerde aşağı yukarı %0.1 olan çok düşük toplama verimliliğidir. Bu, elmas nano kristallerde % 2'nin üzerinde olup durum biraz daha iyidir (Beveratos, et al., 2002). Toplanma verimliliğini arttırmanın yolu ise: Kristali, istenilenin dışındaki tüm uzaysal modlara yayılımın önlendiği optik bir kovuğa koymaktır.

4.2.3. Kuantum Noktalar

Kuantum noktalar yarıiletken nanoyapılardır (Santori, et al., 2001; Moreau, et al., 2001; Zwiller, et al., 2001; Hours, et al., 2003; Baier, et al., 2004). Uygun bir hazırlıkla iki veya daha fazla seviyeli elektronik bir sistem elde edilebilir. Foton yayılımı bir elektron-delik çiftinin yeniden birleşimi ile meydana gelir. Elektron-delik çiftleri, darbeli veya sürekli dalgalı lazerin optik pompalaması ile ya da elektrik akımı ile üretilebilir (Yuan, et al., 2002). Kuantum noktalar hazırlamak için farklı teknikler mevcuttur ve en sık kullanılan malzemeler GaAs, GaAlAs veya InP'dir. Yayınlanan ışığın dalgaboyu temel olarak kullanılan malzeme ile alakalı olup telekom dalgaboylarında çalışan kaynaklar yapmak mümkündür (Takemoto, et al., 2004). Üretilen bir sinyalin spektral genişliği uyarılan enerji seviyeleri sayısına ve üretilen elektron-delik çiftlerinin ortalama sayısına bağlıdır.

Kuantum nokta foton kaynaklarının pratikteki en büyük handikapı sıvı helyum sıcaklığına soğutulmaları ihtiyacıdır. Fakat son araştırmalar bu kaynakların 100 K sıcaklığa kadar çalışılabileceklerini göstermektedir (Mirin, 2004). Fakat bu denli yüksek sıcaklıktaki kaynakların foton sayısı dağılımı kötüdür. Bir diğer problem de genellikle 10^{-4}'den 10^{-3}'e kadar olan düşük toplanma verimliliğidir. Bu da, boş bir sinyal elde etme olasılığının oldukça yüksek olduğu anlamına gelmektedir. Verimlilik, kuantum nokta tümleşik katı hal mikro kovuğa yerleştirerek 10^{-1}'e kadar arttırılabilir (Gerard, et al., 1998). Kuantum nokta tek foton tabancası ile gerçekleştirilen ilk kuantum anahtar dağıtımı uygulaması serbest uzayda 1 m gibi sembolik bir mesafede Waks ve arkadaşları tarafından 2002'de yapıldı.

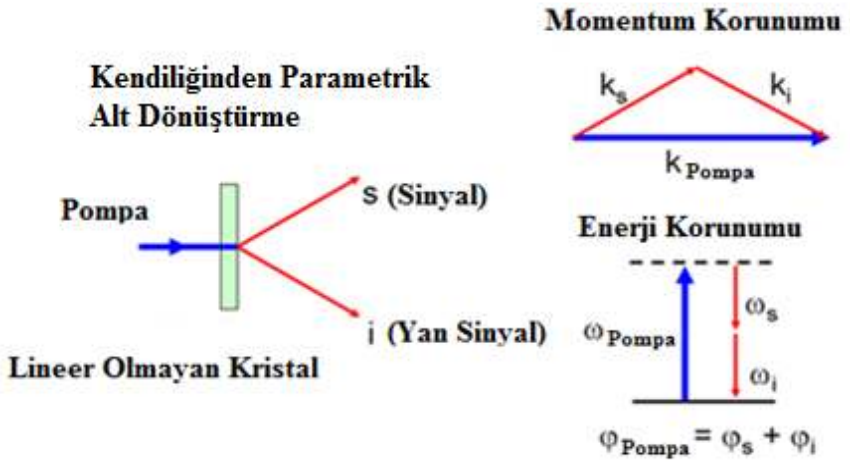
4.2.4. Tek Atomlar ve Moleküller

Tek foton benzeri durumlar üretmek için bir başka alternatif yol da bir tek atomun veya molekülün elektronik düzeyleri arasındaki ışınımlı geçişleri kullanmaktır. Bir tuzakla yakalanan ve burada hem uyarıcı lazer ışınıyla hem de kovuğun boşluk alanıyla etkileştikleri optik bir boşluğa yerleştirilen tek iyonlar, dar spektrumlu ve yüksek toplama verimlilikli iyi bir tek foton kaynağı örneği olabilirler (Kuhn, et al., 2002; Keller, et al., 2004). Fakat bu tür kaynakların pratik kullanılabilirliği, teknolojik karmaşıklıkları yüzünden düşüktür.

4.3. DOLANIKLIK KAYNAĞI

4.3.1. Kendiliğinden Parametrik Alt Dönüştürme

Kendiliğinden parametrik alt dönüştürme işlemi ile enerji, momentum ve polarizasyon dolanık fotonlar hazırlanabilir ve bunlardan herhangi biri Ekert tipi protokollerle KAD amacıyla kullanılabilir. İşlemde, lazer pompasından bir foton belirli bir olasılıkla iki alt frekans fotonuna dönüştürülür. Yalnız bu olasılığın yaklaşık olarak 10^{-10} civarında düşük bir olasılık olduğunu da eklemek gerekir. Lineer olmayan optik ortam gerektiren işlemde toplam enerji ve momentum korunur. Gerekli ortam için $KNbO_3$, $LiIO_3$, $LiNbO_3$, β-BaB_2O_4 gibi kristaller kullanılabilir.



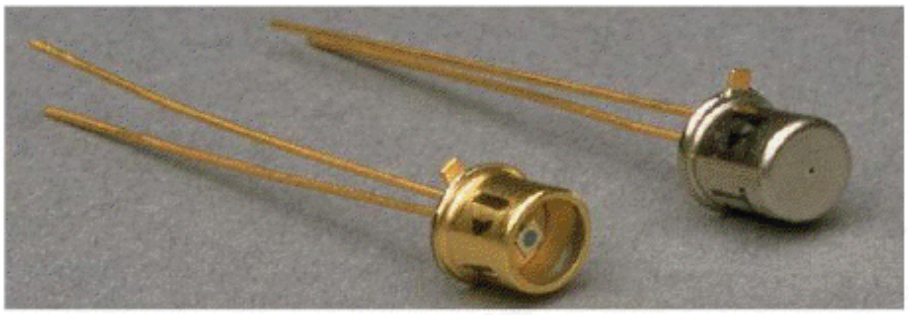
Şekil 4.2 KPAD işlemi. Fotonları foton çiftlerine bölmek için lineer olmayan bir kristal kullanılır. Enerjinin korunumu yasasına göre çifti oluşturan fotonlar orijinal fotonun enerji ve momentumuna eşit toplam enerji ve momentuma sahiptirler (http://en.wikipedia.org/wiki/Spontaneous_parametric_down-conversion).

5. DETEKTÖRLER

Dedektörler, elektromanyetik dalga formundaki enerji akısını ölçülebilir niceliklere çeviren ve kayıt edilmesini sağlayan cihazlardır. Bir dedektörün en önemli karakteristikleri verim, hız, gürültü ve fiziksel uyumdur (Demirburan ve Yazgan, 1987). Bunlardan kuantum verimliliği, dedektörün üzerine düşen ışınım miktarının ne kadarına yanıt verdiğini ifade eder ve "ölçülen foton sayısı/gelen foton sayısı" ile tanımlanır. İdeal olarak, çıktı sinyali gelen foton sayısı ile doğru orantılı olmalıdır. Ancak çıktı sinyalinde daima belirsizlikler olacaktır. Bu belirsizlikler genelde "gürültü" olarak adlandırılır. Temel gürültü kaynakları: Gözlenen kaynaktan gelen foton gürültüsü, arka alan foton gürültüsü ve aletsel gürültü olarak verilebilir.

5.1. ÇIĞ FOTODİYOTLAR

Çığ fotodiyot, impatt, avalanş veya 1958 yılında Read tarafından geliştirildikleri için "Read diyodu" olarak da bilinen APD'ler fotoelektrik etkiyi kullanarak ışığı elektrik sinyaline çeviren oldukça hassas yarıiletken elektronik aygıtlardır.



Şekil 5.1 Sıradan bir APD kesiti (Kışoğlu, 2008).

APD'ler kuantum anahtar dağıtımı sistemlerinde en yaygın olarak kullanılan dedektörlerdir. APD'de çarpan bir foton tarafından üretilen bir tek fotoelektron çarpışma iyonlaşmasıyla çoğaltılır. Bunun sebebi APD tek foton detektörlerinin "Geiger modu" denilen bir modda çalıştırılmalarıdır. Bu modda, eklemde kırılma voltajını aşan bir ters voltaj uygulanır. Dolayısıyla çarpan foton binlerce taşıyıcıdan oluşan bir çığı tetikler. Detektörü resetlemek için çığın söndürülmesi gereklidir. Bu da pasif veya aktif bir şekilde yapılabilir. Pasif söndürmede detektör devresine büyük bir direnç yerleştirilir. Bu, APD'de çığın başlamasından sonra voltajda bir azalmaya sebep olur. Aktif söndürme durumunda ise geri besleme voltajı aktif bir kontrol devresi ile düşürülür. Bu çözüm daha hızlıdır ve dolayısıyla daha hızlı yinelenme değerlerine ulaşılabilir. Günümüzde sıkça kullanılan bir diğer yöntem de geri besleme voltajınının bozulma voltajının üzerine çıkarıldığı kısa ve iyi tanımlanmış bir zaman periyodunda "geçitli mod" denilen modda çalışmaktır (Dusek, et al., 2006).

Spesifik dalgaboylarındaki fotonları tespit etmek için farklı materyallerden yapılmış detektör çipleri gereklidir. Görünür ve infrarede yakın bölge için silikon APD kullanılabilir. Düşük karanlık sayım oranları, %70'e varan yüksek kuantum verimliliği ve 10 MHz'e ulaşan maksimum sayım hızları sunan entegre Peltier soğutmalı ve aktif yatıştırmalı kompakt sayma modülleri de günümüzde ticari olarak bulunmaktadır. Isıl gürültü yüzünden meydana gelen karanlık sayım sayılarını makul bir düzeyde tutmak için -20 ^{0}C'ye kadar soğutma gerekli olup karanlık sayımların yani detektörün foton algılamadığı halde sinyal gönderdiği durumların kuantum anahtar dağıtımını kısıtlayan önemli bir faktör olduğu unutulmamalıdır (Dusek, et al., 2006).

Fiber komünikasyonlarda kullanılan 1300 nm ve 1550 nm'lik telekom dalgaboyları için silikon detektörler uygulanamaz. Bunun yerine 1300 nm'de germanyum ve InGaAs/InP detektörler kullanılabilir. Germanyum detektörleri 77 K'e (sıvı nitrojen sıcaklığı) kadar soğutmak gerekir. Bu dedektörlerin tipik kuantum verimlilikleri %15 dolaylarındadır. Karanlık sayım oranları ise 77 K sıcaklıkta saniyede 25×10^3 sinyaldir. Germanyum detektörler 1550 nm'de kullanılamazlar. Hali hazırda bu dalgaboyu aralığı için genel olarak bulunabilen tek detektörler InGaAs (InP substrat üzerinde) dedektörlerdir. Bu detektörler genel olarak her iki telekom dalgaboyu için kullanılmaktadır. InGaAs detektörler de düşük sıcaklıklara kadar soğutulmalıdır. Pratikte bu soğutma işlemi ya -60 ^{0}C'ye yani 213 K'e kadar üç aşamalı Peltier termoelektrik soğutucularla ya da -100 ^{0}C'ye yani 173 K'e kadar kompakt Stirling motorlar ile yapılır. Günümüzde 1550 nm'de InGaAs APD'nin bir Peltier soğutucu ile kuantum verimliliği %5-10 civarlarında, karanlık sayım oranı geçitli modda $10^4 s^{-1}$ civarında, maksimal yineleme frekansı ise 100 kHz ile 1MHz arasındadır. Bir Stirling soğutucu ile ise 100 K'de kuantum verimliliği %10'un üzerinde olup, geçitli modda saniyede yüzlerce karanlık sayım meydana gelmektedir ve maksimal yineleme frekansı yine 100 kHz ile 1 MHz arasındadır. Burada artan algılama verimliliği ile birlikte karanlık sayım oranının da arttığı görülmektedir. Sıcaklıkla birlikte karanlık sayım oranı arttığından, düşük sıcaklıklarda daha iyi toplam performans elde edilebilir.

Kuantum anahtar dağıtımı üzerinde olumsuz bir etki ile çığ söndürüldüğünde tüm şarj taşıyıcılar tekrar birleşince görülür. Bu durum diyotu tekrar yalıtıcı bir duruma getirir. Tam bir foto algılama döngüsü biter ve diyot bir sonraki algılama için hazır olur. Fakat, bazı tekrar birleşimler "backflashes" olarak tabir edilen geri parıldama olayını doğuracak şekilde ışınımlıdır. Bu zayıf ışık sinyalleri iletim kanalına doğru geriye yayılırlar ve Bob'un taban ayarlarının bir rakibin eline geçmesine fırsat verebilirler. Yani, önemli bir yan kanal oluştururlar. Bu yüzden uygun filtrelerle dikkatle yok edilmelidirler (Kurtsiefer, et al., 2001). Son olarak, telekom dalgaboylarında KAD'nın performansını ve mesafeyi karanlık sayımları azaltarak arttırmak için InGaAs APD'leri direkt kullanmak yerine, verimli Si-APD'ler ile parametrik frekans üst dönüşüm birlikte kullanılabilir. Periyodik kutuplanmış lityum niyobat içerisindeki üst dönüşüm nispeten düşük gürültülü olduğu gibi oldukça verimli olabilir (Diamanti, et al., 2005).

5.2. KUANTUM NOKTA DEDEKTÖRLER

Kuantum nokta rezonans tünelleme diyotu, rezonans tünelleme diyotunun yapısı içerisine kuantum nokta katman yerleştirilmiş, yarıiletken bir aygıttır (Blakesley, et al., 2005). Bu diyotun içerisinde iki n-katkılı GaAs katmanı çift bariyerli AlGaAs yalıtım katmanları ile ayrılır ve sonra kendini kuran bir InAs kuantum nokta katmanı ilave olur. Bu çift bariyerli yapının içerisinden akan rezonans tünel akımı bitişik nokta katmanının içerisindeki kuantum noktalarından bir foton tarafından uyarılmış deliğe duyarlıdır. Bir deliğin nokta tarafından yakalanması aygıttan geçen akımın büyüklüğünü değiştirebilir. Kuantum nokta dedektörlerin 550 nm'de ölçülen maksimum algılama verimliliği %12'dir. Fakat, makul olan 4000 s^{-1}'lik karanlık sayım oranı yalnızca %5'lik algılama verimliliği ile elde edilmiştir. 77 K'de bu değerleri veren örnek her 150 ns'de yeni bir foton tespit edebilir. Bu da takribi olarak 6 MHz'lik yineleme hızına tekabül etmektedir (Blakesley, et al., 2005). Fakat bu dış elektroniklerle sınırlanmış bir değerdir ve yakın bir gelecekte 100 MHz'lik oranlar umulmaktadır. GaAs'ten yapılmış detektörün telekom dalgaboylarında kullanılamadığı da eklenmeli ve bu dalgaboyları için detektörlerin InP gibi maddelerden yapılması gerektiği not edilmelidir.

5.3. GÖRÜNÜR IŞIK FOTON SAYAÇLARI

Görünür ışık foton sayaçları, bir iç silikon katman ve az katkılanmış bir arsenik kazanç katmanından oluşan iki ana katmanlı yarıiletken detektörlerdir (Waks, et al., 2003; Kim, et al., 1999). Bir tek foton soğurulduğunda bir tek elektron-delik çifti üretilmiş olur. Aygıt üzerinden uygulanan küçük bir geri besleme voltajına bağlı olarak, elektron bir kenardaki şeffaf bağlantıya doğru hızlandırılır bu arada delik de diğer yandaki kazanç alanına doğru hızlandırılır. Bu alandaki verici elektronlar etkili bir şekilde safsızlık durumlarında dondurulur çünkü aygıt 6 K civarında bir çalışma sıcaklığına kadar soğutulur. Buna rağmen, bir delik kazanç bölgesine doğru hızlandırıldığında verici elektronları darbe iyonizasyonuyla iletim bandına kolayca iter. Dağılmış elektronlar takip eden darbe iyonizasyon olguları yaratabilirler ve bunlar da çığın çoğalmasına yol açar (Dusek, et al., 2006).

Bir foton tespit edildiğinde, detektör yüzeyinde birkaç mikron çapında bir kör nokta oluşur. Detektörün geri kalanı sonraki algılamalar için müsait durumdadır. Eğer detektörde birden fazla foton bulunursa, çoklu fotonların aynı konuma gelmesi olasılığı zayıf olduğundan dedektör bütün fotonları tespit eder. Dolayısıyla bu dedektörler verimli foton sayısı durumu tespiti yapabilirler. Görünür ışık foton sayaçlarının kuantum verimliliği %90 civarında olup karanlık sayım oranı 6 K sıcaklıkta 543 nm'de 2.10^4 s^{-1}'dir (Dusek, et al., 2006).

5.4. SÜPERİLETKEN DEDEKTÖRLER

Tek fotonları tespit etmek için süperiletken dedektörlerden yararlanılabilir. Tüm süperiletken detektör türleri için çok soğuk ortam gereklidir. Genellikle "süperiletken tek foton detektörü" olarak adlandırılan ilk detektör tipi, niyobyum nitrat gibi süperiletken malzemeden yapılmış kendi aralarında bağlanarak kıvrımlı bir tel formu oluşturan ince şeritlerden oluşur (Verevkin, et al., 2002). Bu telde maddenin kritik akımının altındaki geri besleme akımı korunur. Çarpan bir foton bir Cooper çiftini kırar ve direnç potansiyeli yaratan bir sıcak nokta üretir. Şeritlerin genişliği öyle tasarlanır ki sıcak noktanın etrafında zorlanan akım kritik akımı aşar. Bu durum, direnç artışı ve fotonun tespit edildiğini gösteren bir voltaj sinyali ile sonuçlanır. Bu dedektör tipi üzerinde yapılan çalışmalar, bu dedektörlerin 2.5 K'lik sıvı helyum sıcaklığında 1300-1550 nm'de %10'a kadar kuantum verimliliğine, 0.01 s^{-1} civarında bir karanlık sayım oranına ve 2 GHz.'in üzerinde bir sayma hızına sahip olduklarını göstermektedir (Verevkin, et al., 2004).

İkinci süperiletken detektör tipi de "geçiş kenar sensörü" denilen dedektörlerdir. Bu sensörler dirençli geçiş sırasında elektriksel olarak geri beslenmiş olan süperiletken ince filmlerden oluşur. Aygıt, fotonun soğurulması ile ortaya çıkan ısıyla orantılı bir elektrik sinyali üretir. Bu detektörler çarpan fotonların sayısını dahi belirleyebilir. Üzerlerinde yapılan en son çalışmaların sonuçlarına göre 1550 nm'de %80'i aşan kuantum verimlilikleri ile çok iyi performans göstermektedirler (Rosenberg, et al., 2005). Fakat ne var ki bu detektörler çok yavaştırlar. Çünkü her foton tarafından ortaya çıkan ısının önce yok edilmesi gerekir (Miller, et al., 2003).

Bir diğer süperiletken dedektör tipi de süperileken tünel eklem detektörüdür (Fraser, et al., 2003). Birlikte bir Josephson eklemi oluşturan, bir yalıtıcı katman tarafından ayrılmış iki süperiletken elektrottan oluşur. Eklemden geçen tünellenen akımı bastırmak için, elektrotlara paralel bir manyetik alan uygulanır. Gelen fotonlar Cooper çiftlerini kırarlar. Bu alan soğurulan enerjiye bağlı olarak tünelleme hızını değiştirir. Çalışma sıcaklığı yüzlerce milikelvin düzeyindedir. Bu detektörler fotonları kızılötesi ve morötesi bölgeler arasında tanımlayabilirler.

6. KUANTUM KANALLAR

6.1. OPTİK FİBERLER

Optik fiberler diğer iletişim malzemelerine oranla uzun mesafelerdeki veri iletişiminin daha hızlı ve yüksek değerlerde yapılabilmesine olanak verdikleri için haberleşme sistemlerinde sıklıkla kullanılmaktadırlar. Optik fiberler, verileri elektrik sinyali yerine ışık olarak gönderirler. Dolayısıyla manyetik alanlardan, radyo dalgalarından, elektriksel alanlardan etkilenme olasılıkları yoktur. Optik fiberlerde ışık, iç yansımalar aracılığıyla optik fiberin merkezinde tutulmaktadır. Bu sayede fiber bir dalga kılavuzu gibi hareket etmektedir. Çoklu yayınma hatlarını ya da çapraz modları destekleyen fiberlere "çok modlu fiberler", sadece tek bir modu destekleyen fiberlere ise "tek modlu fiberler" denmektedir. Çok modlu fiberler genellikle geniş çaplı bir merkeze sahiptir ve kısa mesafeli iletişim hatlarında kullanılırlar. Tek modlu fiberler ise 200 metrenin üzerindeki iletişim hatlarında kullanılmaktadırlar. Bu bakımdan karasal kuantum anahtar dağıtımı için en fazla gelecek vaat eden kanallar şüphesiz tek modlu optik fiberlerdir. Standart telekom fiberlerde en düşük zayıflatmalara 1300 nm'de (0.35 dB/km civarı) ve 1550 nm'de (0.2 dB/km civarı) rastlanır. Fakat ne yazık ki bu dalgaboyları için standart silikon bazlı yarıiletken fotodetektörler kullanılamazlar. Özel fiberler kullanmak ve 800 nm civarında çalışmak koşuluyla verimli detektörlerden yararlanılabilir. Fakat bu dalgaboylarında da bu tip fiberlerin zayıflatmaları 2 dB/km civarındadır ve bu değer nispeten yüksektir. Dolayısıyla yine standart telekom fiberlere yoğunlaşılmakta ve 1300 nm ve 1550 nm dalgaboylarında düşük gürültülü ve verimli detektörler yapılmaya çalışılmaktadır.

Fiberlerde görülen kayıplar KAD sistemlerinin çalışma alanını kısıtlayan iki ana faktörden birisidir. Örneğin bir fiberdeki 0.20 dB/km'lik bir zayıflama 100 km sonra %99 kayıp demektir. Diğer sorunlar ise fiberlerin bazı optik özelliklerinin sıkı ısı bağımlılığı olması ve ışığın polarizasyon durumlarının geometrik faz, çift kırılma ve dağılmaya bağlı olarak bozulmasıdır (Dusek, et al., 2006).

Polarizasyonun bozulması bilginin kodlanması için her hangi bir tür polarizasyon kodlaması kullanılmasının önünde ciddi bir engeldir. Bu yüzden, fiber kullanılan KAD sistemlerinde genellikle faz kodlama yöntemi kullanılır.

6.2. SERBEST UZAY

Serbest uzay optik haberleşme yaklaşımı ile hassas olarak yönlendirilebilen lazerler aracılığıyla, birbirini gören iki nokta arasında araya girme, karıştırma ve dinlenme riski olmadan veri transferi sağlanabilir. Dolayısıyla kuantum anahtar dağıtımı, optik fiberlerde olduğu gibi serbest uzayda da başarıyla gerçekleştirilebilir. Ayrıca 770 nm ve 860 nm civarlarında atmosferin çok düşük soğurmaya sahip olması sebebiyle nispeten verimli ve düşük gürültülü yarıiletken detektörler kullanılabilir. Bu tür bir iletişim için herhangi bir kablo döşeme işlemi gerekmez. Üstelik bu dalgaboylarında atmosfer çift kırıcı değildir. Yalnızca zayıf bir dispersiyonu vardır. Serbest uzay optik iletişiminin dezavantajı ise yalnızca görülebilen mesafelerde iletişim kurulabilmesidir. Yani iletişim kuran tarafların arasında engel olmaması gerekir. Ayrıca iletişimin verimi hava kirliliğine ve diğer atmosferik şartlara yüksek derecede bağlıdır. Değişik hava şartlarında zayıflamada büyük değişiklikler gözlenebilir. Örneğin, 860 nm civarındaki dalgaboylarında hava açıkken zayıflama 0.2 dB/km'nin altındadır. Hafif yağmurlu havada zayıflama 2-10 dB/km iken, yoğun sisli havada ise 20dB/km'yi geçer. Ayrıca, 15-20 km'lik yüksekliklere kadar hatırı sayılır atmosferik türbülanslar vardır. Bunların dışında çevredeki gün ışığı gibi arka plandaki bir ışığın sahte etkisi de bir sorundur. Serbest uzay optik iletişiminin karşılaştığı başka bir sorun da ışın ıraksamasıdır. Kırılmalara bağlı olarak ışığın çapı uzun mesafelerde epeyce genişler. Bu etki alıcı tarafından ışığın bir kısmının yakalandığı durumlarda ilave kayıplara sebep olabilir.

7. ENGELLER

Günümüzde kuantum anahtar dağıtımının yaygın olarak kullanımını engelleyen iki ana teknolojik engel vardır. Bunlar: Düşük iletim hızı ve sınırlı uygulama mesafesi olarak verilebilir.

7.1. İLETİM HIZI

Ham anahtar değerini sınırlayan faktörlerden en temel olanı detektörün ölü zamanı yani yenilenme süresidir. Çığ fotodiyotların bir foton algıladıktan sonra yeni bir algılamaya hazır hale gelebilmesi için önce, şarj taşıyıcılarının çığı söndürülmelidir. Tipik bir APD'nin ölü zamanı yaklaşık bir mikro saniye civarındadır. İletim hızını azaltan bir diğer durumla da, kaynak olarak zayıf lazerler kullanıldığında karşılaşılır. Çünkü güvenlik açısından çoklu foton sinyallerinden kaçınmak amacıyla seçilen küçük ortalama foton sayısı, iletim hızını azaltan boş sinyallerin sayısını arttırır. İletim hızındaki azalma aynı zamanda büyük ölçüde kanaldaki kayıplara bağlıdır. Bu faktörlerin dışında elenmiş anahtar değeri hata düzeltme ve gizlilik artırımı işlemleri ile daha da azalır. Hata oranı ne kadar yüksekse, aynı miktardaki ham anahtardan süzülen anahtar o kadar kısalır (Dusek, et al., 2006).

7.2. MESAFE KISITLAMASI

Güvenli kuantum anahtar dağıtımının yapılabileceği maksimal uzaklık artan kayıplar ve detektör gürültüsü ile birlikte azalır. Belirli bir detektör ve ayarı için detektörün karanlık sayım oranı sabittir. Fakat anahtar değeri toplam kayıplara bağlı olarak uzayan mesafe ile birlikte azalır. Dolayısıyla karanlık sayımlar yüzünden oluşan hatalı bitlerin göreceli sayısı o şekilde artar ki güvenli bir anahtar dağıtımı imkansız hale gelir. Standart yükselticiler de fotonların durumlarını gizli dinleme ile benzer şekilde etkilediklerinden kullanılamazlar. Günümüz teknolojisi ile 100 km'ye kadar güvenli kuantum anahtar dağıtımı yapılabilmektedir (Dusek, et al., 2006). Bu mesafe duruma göre bazen yeterli olabilip daha uzak mesafelerdeki istasyonlar arasında iletişim için ise yetersiz kalabilmektedir.

7.2.1. Kuantum Yineleyiciler

Kuantum anahtar dağıtımında dolanık çiftlerin kullanımı önemli bir avantaj sağlar. Güvenli iletişimin menzilini en azından teoride isteğe bağlı bir uzaklığa genişletmeyi taahhüt eder. Buna kuantum yineleyicilerle ulaşılabilir (Dür, et al., 1999). Kuantum yineleyiciler, anahtar üzerinde herhangi bir bilgi sunmadan hata düzelmesi yapabilirler. İletim kanalı her biri bir dolanık çift kaynağı taşıyan daha kısa segmentlere bölünür ve her segmentin sonunda bir dolanıklık arıtması uygulanır (Bennett, et al., 1996). Böylece orijinal olarak daha çok sayıda olan ve iletim sırasında zarar gören dolanık çiftlerden daha az sayıda fakat onarılmış yüksek derecede dolanık çiftler üretilir. Bağımsız segmentler dolanıklık değiş tokuşu ile birbirlerine bağlanırlar (Bennett, et al., 1993; Zukowski, et al., 1993). Dolayısıyla sonuçta Alice ve Bob yüksek derecede dolanık çiftlere sahip olurlar.

8. DESTEKLEYİCİ İŞLEMLER

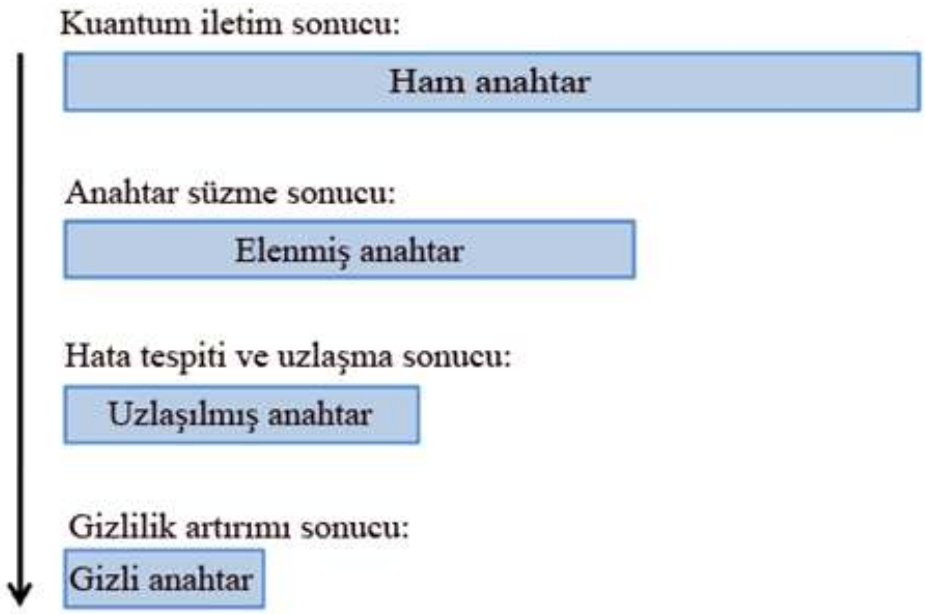
8.1. HATA ORANI TESPİTİ

Kutuplayıcılar, fiberler, detektörler vb. gibi gerçek aygıtlar hiç bir zaman mükemmel ve gürültüsüz değildirler. Dolayısıyla, optik hatlarda hatalı kübit iletimi sadece hattı dinleyen bir gizli dinleyiciden değil aynı zamanda hattaki fiziksel gürültüden de kaynaklanabilir. Hata oranı tespiti işleminde hat gürültüsünün ardına saklanan bir saldırganın tespit edilmesi ön görülmektedir. Bunun için Alice ve Bob önceden hattın dinlenmediğinden emin oldukları bir anda anahtar iletimi gerçekleştirip bu iletimde hat gürültüsü nedeniyle hatalı iletilen kübitlerin sayısından bir R_{max} hata oranı belirlerler. Daha sonraki iletimlerde de elde ettikleri ham anahtardan rastgele seçilen bit pozisyonlarındaki bitleri karşılaştırıp –ki karşılaştırılan bitlerin sayısı ne kadar fazla olursa dizideki gerçek hata oranı tespit edilen değere o denli yakın olur- R hata değerini belirler ve $R < R_{max}$ için hattın dinlenmediğinden emin olurlar (Gümüş, 2011). Ya da $R > R_{max}$ için bunun tam tersini düşünerek anahtar dağıtımını iptal eder/erteler veya bazı iletim sonrası işlemler uygulayarak hala bir güvenli anahtar elde etmeyi umabilirler.

8.2. SIZAN BİLGİNİN HESAPLANMASI

Kuantum fiziğinin kanunları tarafından izin verilen atağa ve bu ataktan dolayı ortaya çıkacak hata oranına dayanarak, bir gizli dinleyicinin eline geçebilecek bilgi miktarının sınırları belirlenebilir. Eve daha önce üzerinde durulan en basit sürekli bir durdur tekrar-gönder atağı için, ortalama olarak bit başına $I = 2\epsilon$ oranında bilgi elde eder. Burada ϵ bit-hata oranıdır. Tabi, bu atak ideal bir atak değildir ve $I(\epsilon)$'nin sınırlayıcı değerleri seçilen protokole ve uygulamaya bağlıdır (Dusek, et al., 2006).

8.3. KLASİK BİT DİZİLERİ İÇİN HATA DÜZELTME



Şekil 8.1 Anahtar süzme basamakları ve anahtar uzunluğu (Calver, 2011).

Kuantum iletim Alice ve Bob'un bir ham anahtar paylaşmasını sağlar (Calver, 2011). Alice ve Bob, Bob'un yanlış tabanlar kullandığı sinyalleri ayırarak elenmiş bir anahtar elde ettiğinde, sahip oldukları bit dizilerinin tamamen eşit olması gerekmez. Bu durum ya bir gizli dinleyici ya da teknolojik gürültü yüzünden meydana gelebilir. Dolayısıyla sonuçta tamamen paylaşılan gizli bir anahtar üretebilmek için önce bir hata düzeltme işlemi yaparak hatalı bitleri düzeltmeli ya da elemelidirler.

Açıklanacak olandan başka yöntemlerin de varolduğu belirtilerek, uygulanması kolay bir hata düzeltme işlemine göz atılacak olunursa, Alice ve Bob önce hataların yerlerini rastlantısal hale getirmek için dizilerindeki bit pozisyonlarının rastlantısal bir permütasyonu üzerinde açık kanaldan anlaşarak bunu dizilerine uygularlar. Sonra değiştirdikleri dizilerini belli uzunlukta (örneğin k-bit'lik) bloklara ayırırlar. Öyleki, her blokta birden fazla hata bulunmasının ihtimal dahilinde olmadığı düşünülür. Yani blok boyutu beklenen bit-hata oranının bir fonksiyonudur. Sonra her blok için, bloktaki bitlerin Mod 2'ye göre toplamına tekabül eden, bloğun paritesini karşılaştırırlar. Uyumlu pariteleri olan bloklar geçici olarak doğru kabul edilirler. Eğer pariteler uyuşmazsa, blok kabaca eşit uzunlukta iki alt bloğa bölünür ve birinci alt blokların pariteleri karşılaştırılır. Bu, Alice ve Bob'un hatanın hangi alt blokta olduğunu anlayabilmelerini sağlar. İçinde hata bulunduğu anlaşılan alt blok tekrar kendi içinde iki alt bloğa ayrılır. Bu işleme hatalı bitin pozisyonu tespit edilene kadar devam edilir. İçinde çift sayıda hata bulunan blok veya alt bloklardan kaynaklanan, tespit edilemeden kalmış hataları ortadan kaldırmak için rastlantısal permütasyon ve blok parite karşılaştırma işlemi artan blok boyutlarıyla bir kaç kez daha tekrarlanır. Alice ve Bob blok uzunluğu dizinin uzunluğu ile karşılaştırılabilecek kadar arttığında yani verinin içerisinde toplam olarak en fazla birkaç hata kaldığını tahmin ettiklerinde stratejilerini değiştirirler. Bu noktada blokları kullanmak yerine dizilerinden rastgele bir alt küme seçerek, bu alt kümelerin paritelerini karşılaştırırlar. Eğer uyuşmazlık tespit edilirse yine yukarıdaki yöntemle bu alt kümenin alt blokları içinde hatalı bit bulunup düzeltilene kadar ikili arama işlemine devam edilir. Örneğin Alice ve Bob, pariteleri uyuşmadığı için içinde hata bulunduğunu tespit ettikleri $\vec{a}$ = 1101100$\underline{0}$1 ve $\vec{b}$ = 1101101$\underline{1}$ şeklinde olan k=8 bit'lik bloklarını karşılaştırırlarsa, ilk dört bitlerinin pariteleri uyuştuğundan hatanın bloklarının ikinci dört bitlik kısmında olduğunu anlayacaklardır. a_5a_6 ve b_5b_6 bitlerinin pariteleri kontrol edildiğinde bunların içinde de hata olmadığı görülecektir. Dolayısıyla hatanın artık son iki bitten birinde olduğu kesindir. Bunlardan a_7 ve b_7 kıyaslandığında, 7. sıradaki bitte hata olduğu bulunacaktır (Loepp and Wooters, 2006). Böylece bu bit atılabilir ya da istenilirse düzeltilebilir. Bu işlem sonunda artık Alice ve Bob tamamen paylaşılan fakat yalnızca kısmen sır olan bir diziye sahiptirler.

8.4. KLASİK BİT DİZİLERİ İÇİN GİZLİLİK ARTIRIMI

İletim sırasında hem Bob hem de Eve ölçüm yapmışsa, ikisi de Alice'in gönderdiği anahtar bitleri üzerinde bir miktar klasik bilgiye sahiptirler. Eğer Bob, Alice tarafından gönderilen anahtar ile ilgili olarak Eve'den daha fazla bilgiye sahipse yani $\left[I(B;A > I(E;A))\right]$ ise, Alice ve Bob tek yönlü iletişim kurarak Eve'in üzerinde kayda değecek kadar bilgi sahibi olamayacağı yeni bir gizli anahtar oluşturabilirler. Bunun için ilk olarak Alice ve Bob tamamen eşit bit dizine sahip olabilmek için bir hata düzeltme işlemi uygulamak zorundadırlar. Bunu yaparak Alice ve Bob eşit dizilere sahip olurlar. Fakat bu diziler tam olarak gizli olmayacaktır. Bundan sonra, gizlilik artırımı için aşağıdaki gibi bir algoritma uygularlar (Bennett, et al., 1988; 1992a; 1995).

Alice, elenmiş anahtardan rastgele N tane biti ($[X_1, X_2, \dots, X_N]$) seçer ve bunlar üzerinde $\oplus$ ile ifade edilen XOR işlemini uygular. Yani Mod 2'ye göre toplama işlemi yapar. Aslında bir parite biti hesaplar: $[X_1 \oplus X_2 \oplus \dots \oplus X_N]$ ve sonucu saklar. Daha sonra Bob'a hangi bitler üzerinde çalışma yaptığını söyler, fakat sonucu paylaşmaz. Bob bundan sonra aynı pozisyondaki kendi bitleri üzerinde aynı çalışmayı yapar: $[Y_1 \oplus Y_2 \oplus \dots \oplus Y_N]$ ve o da sonucu saklar. Alice ve Bob'un dizileri tamamen aynı, yani $X_i = Y_i$ ise Bob'un sonucu Alice'inkiyle aynı olmalıdır. Alice ve Bob bundan sonra her bir N'li anahtar bitlerini hesaplanan XOR değeri ile değiştirirler. Böylece yeni bir anahtar oluşur. Bu arada eğer anahtarında birçok hata bulunan Eve, aynı işlemi denerse, bu yalnızca hatalarını arttırır. Dolayısıyla bilgisi azalır. Örneğin, Eve'in her bir bitin değerini doğru bilme ihtimali $p = 1/2\ (1 + \varepsilon)$ ise, $\varepsilon < 1$ iken parite bitini de $p' = 1/2\ (1 + \varepsilon^N\ ) < p$ ihtimaliyle bilecektir (Dusek, et al., 2006).

8.5. KLASİK BİT DİZİLERİ İÇİN AVANTAJ ARITMASI

Bob ve Alice'in anahtar üzerindeki ortak bilgisi Eve ve Alice'in ortak bilgisinden az bile olsa, $\left[I(B;A \leq I(E;A))\right]$, Alice ve Bob için iki yönlü bir klasik iletişim kurarak, paylaşılan gizli bir anahtar oluşturmak hala mümkündür (Dusek, et al., 2006). Bunu yapabilmek için aşağıdaki gibi bir yol izlenebilir.

Alice elenmiş anahtar bitlerinden N bit'lik ($[X_1, X_2, \dots, X_N]$) bir blok alır. Daha sonra rastgele bir C biti üretir ve bloğun tüm bitlerini aynı C biti ile XOR işlemine sokar: $[X_1 \oplus C, X_2 \oplus C, \dots, X_N \oplus C\ ]$. Son olarak da bu kodlanmış bloğu Bob'a gönderir. Bob ise Alice'in bloğuna karşılık gelen kendi elenmiş anahtar bloğu $[Y_1, Y_2, \dots, Y_N]$ olmak koşuluyla,$[(X_1 \oplus C) \oplus Y_1, (X_2 \oplus C) \oplus Y_2, \dots, (X_N \oplus C) \oplus Y_N]$'i hesaplar. Bob sadece $[0, 0, \dots, 0]$ veya [1, 1, . . . , 1] gibi eşit bitlerden oluşan sonucu kabul eder. Bunu yakaladığında yeni anahtarı, her bir elemanını sırayla ya $C' = 0$ veya $C' = 1$ olarak kabul ederek oluşturur. Eğer $X_i = Y_i$ ise, $(X_i \oplus C) \oplus Y_i = C$ olmalıdır. Eğer Bob'un hesaplaması farklı bitlerden oluşmuşsa, Bob bloğu reddeder.

Bu işlem elenmiş anahtarın diğer blokları ve diğer C rastgele bitleriyle de tekrar edilir. Alice tarafından gönderilip, Bob tarafından kabul edilen rastgele C bitlerinin dizisi Alice tarafından üretilen yeni bir anahtara ve Bob tarafından kabul edilen C' bitlerinin dizisi de Bob tarafından alınan yeni bir anahtara karşılık gelir. Bu yolla, Bob'un Alice tarafından gönderilen yanlış C bitini kabul etmesi ihtimali, ϵ^N olduğundan artan N ile birlikte azalır. Burada ϵ, orijinal elenmiş anahtardaki bit-hata oranıdır. Eve, kendi tarafında C bitini tahmin etmek için bir tercih kullanmak zorundadır. Böylece, Bob'un Alice'in $[X_1, X_2, \dots, X_N\ ]$ bitleri üzerindeki bilgisi Eve'inkinden az olsa bile C hakkındaki bilgisi Eve'den fazla olabilir. Yeni anahtar üzerinde hata düzeltme ve gizlilik artırımı sırasıyla uygulanabilir (Dusek, et al., 2006).

8.6. AÇIK GÖRÜŞMENİN DOĞRULANMASI

Pratikte fiziksel olarak müdahale edilemeyen açık bir kanal mümkün olmadığından, kuantum anahtar dağıtımı yapılırken açık kanaldan gönderilen ek bilgi değiştirilebilir. Örneğin Eve hem kuantum hem de klasik kanalı kesebilir ve Alice'in karşısında Bob'muş gibi davranabilir. Bunun önüne geçebilmek için açık kanaldan gönderilen mesajların doğru göndericiden geldiğinin ve değiştirilmediğinin doğrulanması gereklidir. Buna yönelik bir işlem ilave anahtar materyalinin depolanması ve gönderilmesini gerektirir. Kuantum kriptografinin koşulsuz güvenlik sağlaması için açık görüşmeyi doğrulamak için kullanılan işlemin de aynı zamanda koşulsuz olarak

güvenli olması gerekir. Bu amaca uygun doğrulama algoritmaları mevcuttur (Wegman and Carter, 1981; Stinson, 1995). Doğrulama şifresi her zaman doğrulanan metinden daha uzun olmalıdır fakat doğrulama etiketi yani mesajla birlikte mesajın kaynağını ve gerçekliğini doğrulamak için gönderilen bilgi nispeten daha kısadır. Doğrulama etiketi doğrulama şifresi hakkında Eve'e bilgi sızmasını engellemek için OTP ile şifrelenir. Dolayısıyla doğrulama etiketi ile aynı uzunlukta rastlantısal bir dizinin, her KAD iletiminden sonra yenilenmesi gerekir (Dusek, et al., 2006).

9. KUANTUM ANAHTAR DAĞITIMININ GÜVENLİĞİ

Kuantum anahtar dağıtımının hedefi kullanıcılara gizli anahtarlar ulaştırmaktır. Fakat deneysel bir uygulamada direkt olarak güvenli kuantum anahtar dağıtımı gösterilemez. Çünkü güvenlik teorik bir ifadedir ve deneyden elde edilecek veriden süzülen gizli anahtarı elde etmek için kullanılan belirgin protokollere dayanır. Bu protokoller de hata oranı, kaynağın ortalama foton sayısı ve sinyallerin kayıp oranı gibi gözlenebilir parametrelere dayanır. Dolayısıyla bir deneyde teorik güvenlik analizinin model varsayımları doğrulanır ve aygıtın gözlenen parametrelere ve seçilen protokole göre gizli bir anahtar üretebilecek şekilde nasıl çalıştırılabileceği gösterilir.

Kuantum anahtar dağıtımı sistemlerinin gerçek hayattaki pratik uygulamaları sorununa daha yakından bakılacak olunursa, kullanılmakta olan tüm aygıtların bir dereceye kadar kusurları olduğu göz önüne alınmalıdır. İlaveten tüm aygıtlar gibi kuantum kanallar da bazı kusurlar gösterir. Temel KAD protokolleri bir gizli dinleyicinin varlığını kuantum mekanik sinyallerdeki değişikliklere bakarak kontrol eder. Kusurlar neticesinde, Alice ve Bob'un ellerinde ideal olanlardan sapmış veriler kalacağı gerçeği söz konusudur. Dolayısıyla, yalnızca bir gizli dinleyicinin varlığını kontrol eden ideal bir basit protokolde Alice ve Bob'un iletişimlerini iptal etmeleri gerekecektir. Çünkü veri bozulmalarının aygıt veya kanal kusurlarından değil de aktif bir gizli dinleyiciden kaynaklandığına dair en kötü senaryo ilk olarak akla gelir. Yani gizli dinleyici Alice ve Bob'un verisiyle ilgili bilgiye sahip olmuş olabilir. İşin kötüsü Alice ve Bob genelde tamamen hatasız bir dizisi de paylaşmamaktadırlar (Dusek, et al., 2006).

Eve'in bir gizli dinleme aktivitesini nasıl uygulayabileceğine bakılacak olunursa; kuantum mekaniği ölçüm teorisinden bilinmektedir ki, gizli dinleme sonda ile sinyaller arasında bir etkileşim olarak düşünülebilir. Eve bundan sonra sondayı ölçerek sinyaller hakkında bilgi sahibi olabilir. Gizli dinleme saldırıları üç'e ayrılır: Eğer Eve her bir kübitten bağımsız yoklamalar alır ve birbiri ardına bu yoklamaları ölçümlerse, bu çeşit ataklara "münferit" ya da "tutarsız ataklar" denir. Eğer Eve çeşitli kübitleri birbiriyle tutarlı şekilde işlerse, bu da "tutarlı atak" olarak adlandırılır. Bir de Eve her kübit başına bir yoklama alır fakat bunları tutarlı atakta olduğu gibi ölçümleyebilir. Bunlar da "kollektif ataklar" olarak adlandırılırlar (Dalkılıç ve Ayhan, 2005).

9.1. GÜVENLİK İSPATLARI

Kuşkusuz ki, bu çalışmada bahsedilen anahtar dağıtım prosedürleri biraz idealleştirilmiş olup sorun şudur ki, prensipte çevreyle istenmeyen etkileşimlerin sonucunda ortaya çıkan masum gürültülerle, genelde orada bulundukları varsayılan gizli dinleyicilerden kaynaklanan gürültüleri ayırt etmenin yolu yoktur. Tüm işlevsel kuantum anahtar dağıtım protokolleri, gizli dinlemeden kaynaklı olan veya olmayan gürültüyle çalışabilir olmalıdır. Aynı zamanda Alice ve Bob'un, ölçülebilir parametrelerin hangi değerleri için gizli bir anahtar üretebileceğini açıkça belirtmeli ve bu tarz bir anahtar oluşturan fiziksel olarak uygulanabilir bir prosedür sağlamalıdır. Ayrıca prosedür tasarlanırken gizli dinleyicinin sınırsız kuantum hesaplama gücüne erişebileceği göz önünde bulundurulmalıdır.

Eve'in Alice ve Bob'un üzerinde kıyaslanamaz derecede teknolojik avantajı olduğunu varsaymak makul olur. Eve kuantum bilgisayarlar da dahil olmak üzere sınırsız hesaplama gücüne sahip olabilir; Alice ve Bob'un ölçüm tabanlarını açıkladıkları ve ortak anahtarlarındaki hataları düzeltmek için daha detaylı bilgi paylaşımında bulundukları tüm açık mesajları dinleyebilir. Alice ve Bob ise sadece her bir kübite ölçümler uygulayabilir ve klasik kanaldan iletişime geçerler. Bir kuantum kanalıyla iletişime geçebilmek dışında kuantum bilgisayarları ya da ileri kuantum teknolojileri yoktur.

Uygun güvenlik kriterleri için bu tip engelleyici koşullar altında yapılan araştırmalar ilk kuantum gizli dinleme çalışmalarına yol açtı ve finalde de anahtar dağıtımının güvenliğinin ilk ispatını getirdi. Orijinal ispat, Alice ve Bob kuantum gizlilik artırımı uygulayabildiği sürece dolanıklık temelli anahtar dağıtımlarının, sonsuz hesaplama gücüne sahip bir rakibe karşı gerçekten güvenli ve gürültüye toleranslı olduğunu gösterdi. Prensipte kuantum gizlilik artırımı, bir kuantum yineleyiciler zincirinde dolanıklık değiş tokuşu yapılan herhangi bir uzaklıkta güvenli bir anahtar üretilmesine izin verir. Ancak iki kübitin bozuk karışık durumlarından saf dolanık durumları süzen bu prosedür küçük ölçekli bir kuantum hesaplama gerektirir. Inamori ve Ben-Or'un takip eden ispatları Alice ve Bob'un sadece klasik hata düzeltme ve klasik gizlilik artırımı uygulayarak da gizli bir anahtarı kısmen dolanık parçacıklardan süzebileceğini gösterdi. Kuantum gizlilik artırımı, güvenlik ispatı için Lo ve Chau tarafından da kullanılmıştır. Mayers'in eş zamanlı ispatı, protokolün Alice ve Bob'un kuantum bilgisayarlar kullanmaya güvenmek zorunda kalmadıklarında güvenli olabileceğini göstermiştir. Aynı sonuca farklı yöntemler kullanan Biham ve arkadaşları tarafından da varılmıştır. İki ispat da kuantum gizlilik artırımı gerektirmese de oldukça karışıktır. Kuantum gizlilik artırımı ve hata düzeltmenin iyi bir birleşimi, sanal kuantum hata düzeltmeye dayalı BB84 protokolünün güvenliğinin nispeten daha basit bir ispatını formülize eden Shor ve Preskill tarafından öne sürülmüştür. Bu ispat daha detaylı olarak Gottesman ve Lo tarafından BB84 protokolünde daha yüksek bir bit-hata oranına izin vermek amacıyla iki yönlü açık iletişim için; ve Tamaki ve arkadaşları tarafından B92 protokolünün güvenliğini kanıtlamak amacıyla genişletilmiştir. Daha yakın bir zamanda kuantum iletişimin karmaşıklığından kaynaklanan sonuçları kullanan BB84'ün başka bir basit ispatı Ben-Or tarafından ortaya atılmış ve kuantum hafızaların performansıyla ilgili sınırlara dayalı genel bir ispat da Christlandl ve arkadaşları tarafından öne sürülmüştür (Sergienko, 2006).

Son olarak, Eve'in lehine olan Alice ve Bob kuantum bilgisayarlara erişemezken Eve'in erişebildiği senaryonun dışında, yani Alice, Bob ve Eve'nin klasik veya kuantum olsun aynı teknolojiye erişebildikleri eşit durumlarda anahtar süzmek için kriterlerle ilgili ilginç bağlantılar bulunmaktadır (Sergienko, 2006).

9.2. SPESİFİK SALDIRILAR

Bölüm 2'de tanıtılan protokollerin güvenlik sonuçlarına değinmeden önce, spesifik bir kaç atağa göz atılması faydalı olacaktır.

9.2.1. Durdur-Tekrar Gönder Atağı

Bu tip bir saldırıdan söz edildiğinde, Alice'in gönderdiği sinyaller üzerinde Eve'in uyguladığı tam bir ölçüm anlaşılmaktadır. Daha önce Bölüm 2.6'da bahsedildiği üzere, sonuçta oluşan bağıntılar Alice ve Bob'un gizli bir anahtar oluşturmasına izin vermez.

Bu tip bir saldırıya en basit örnek olarak BB84 protokolüne yapılan bir durdur-tekrar gönder atağı verilebilir. Eve sinyal tabanlarından birinde BB84 sinyallerini ölçer ve ölçüm sonucuna uyan bir durum hazırlar. Böyle bir saldırı %25'lik bir hata oranına neden olur. Bu hata oranı Eve'in, Alice ve Bob ile aynı tabanı kullandığında ortaya çıkan %0 ve tabanı onlardan her farklı olduğunda ortaya çıkan %50 hata oranlarının ortalamasından oluşur. Sonuçta, %25'ten fazla ortalama hata oranı olan bir iletim için kuantum anahtar dağıtımı tamamlanamaz (Dusek, et al., 2006).

9.2.2. Kesin Durum Ayırma Atağı

Bu atak, durdur-tekrar gönder saldırısının özel bir şeklidir. Alice tarafından gönderilen sinyal durumları lineer bağımsız olduğunda uygulanabilir. Böyle bir durumda Eve sinyalleri kesin bir durum ayrımı (KDA) ölçümü ile ölçebilir. Böylece bir olasılıkla hatasız olarak tam sinyali öğrenebilir (Dusek, et al., 2000). Sonra, seçimler yaparak sinyalin tam nerede olduğunu kesinlikle bildiği yerlerde Bob'a yeni bir sinyal çıkarıp diğer durumlarda boş durum gönderebilir. Bu strateji ile kayıplı bir kanalı taklit edebilir. Sonuç olarak Alice ve Bob tarafından elde edilen veri, gizli dinlemeye ait hiçbir belli işaret göstermez. Fakat sinyalin serbestlik derecesinde görünür bir bozulma olmamasına rağmen, güvenli bir anahtar da üretilemez. Bu problem, B92 protokolünde ortogonal olmayan polarizasyon durumlarındaki tek fotonların, tek foton tespiti ile

birlikte kullanıldığı durumda tipik olarak gözlenir. Bu protokol, kanalın geçirgenliği sinyal durumlarının ortogonal olmamasına dayanan bir eşiğin altına düştüğünde güvensiz hale gelir. Eşik, KDA ölçümünün başarı olasılığının Bob'un kayıplı kanalda tespit olasılığına eşit olduğu durumda geçirgenlik olarak tanımlanır. Örnekte, KDA ölçümünün başarı olasılığı $P_{USD}^{SUCC} = 1 - |\langle\varphi_0|\varphi_1\rangle|$ olarak verilir ve Bob sinyallerin η kadarını elde eder. Burada η kanalın geçirgenliğidir. O halde geçirgenlik eşiği için $\eta_{thresh} = 1 - |\langle\varphi_0|\varphi_1\rangle|$ ifadesi yazılabilir (Tamaki, et al., 2003a).

9.2.3. Demet Bölme Atağı

Demet bölme atağı kuantum anahtar dağıtımının herhangi bir optik uygulaması için çok doğal bir saldırıdır. Sebebi kayıplı bir optik iletim hattının, içine hattın kayıplarını temsil eden bir demet bölücü eklenmiş ideal bir hattan oluşan bir modelle gayet iyi betimlenebilmesidir. Böyle bir durumda Bob gönderilen sinyali alırken, Eve de demet bölücünün ikinci çıktısından yayılan bir sinyal yakalar. Bazı protokollerde, Eve bu gibi bir durumda sinyalin bir kısmını belirleyici olarak öğrenebilir (Bennett, et al., 1992a; Dusek, et al., 2000). Bununla örneğin BB84 protokolünde tek fotonlar yerine zayıf lazer sinyallerinin kullanıldığı durumda karşılaşılabilir. Alice burada BB84 polarizasyonlarında zayıf lazer sinyalleri hazırlar. Bu sinyaller aynı zamanda çoklu foton sinyalleri de içerir. Eve'in saldırısındaki demet bölücü Eve'e bazı sinyaller için sinyalin bazı, hatta tüm fotonlarını verir. Eve, Alice ve Bob sinyallerin polarizasyon tabanlarını ve ölçüm sonuçlarını açık kanaldan iletene kadar bekler, ondan sonra fotonlarını doğru tabanda ölçer ve Alice'in sinyallerini belirleyici olarak elde eder. Eğer Bob'da en az bir foton elde ettiyse, o zaman Eve de elenmiş anahtarın bir bitini belirleyici olarak bilmektedir (Inamori, et al., 2001). Buna bağlı olarak gizli anahtar değerinin $R \leq p_{exp} - p_{split}$ ile sınırlı olduğu gösterilebilir. Burada p_{exp} elenmiş anahtarın içerisine bir sinyalin girme olasılığıdır. p_{split} ise Eve'in sinyalin en azından bir fotonunu elde etmesinin ve bu sinyalin elenmiş anahtara girmesinin ortak olasılığıdır. Ortalama foton sayısı μ olan zayıf lazer sinyallerinin kullanıldığı durumda, $R \leq (1 - e^{-\mu\eta})\left(1 - e^{-\mu(1-\eta)}\right)$ bulunur.

Aslında bu üst sınır, ortalama foton sayısı μ'nün ve toplam geçirgenlik η'in tüm değerleri için pozitiftir. Bu saldırının, Alice ve Bob tarafından engellenmesinin kanalı ek bir teste tabi tutarak mümkün olmadığı açıktır.

9.2.4. Foton Sayısı Bölme Atağı

Demet bölme atağında gelen sinyal durumlarının fotonları Eve ve Bob arasında istatistiki olarak dağıtılır. Prensipte, Eve daha etkili bir yöntem kullanabilir (Dusek, et al., 1999; Lütkenhaus, 2000; Brassard, et al., 2000). Eve ve Bob en az birer foton elde ettiklerinde, Eve'in elenmiş anahtarın bir elemanını bilebileceği bilinmektedir. Bununla beraber demet bölücü, bazen çoklu foton sinyallerinin tüm fotonlarını Eve'e veya Bob'a gönderir.

"Foton sayısı bölme atağı" denilen gelişmiş gizli dinleme saldırısı, Eve'in sinyallerin toplam foton sayısı üzerinde yıkıcı olmayan bir kuantum ölçüm yapmasıyla başlar. Eve ne zaman bir çoklu foton sinyali yakalarsa, belirleyici bir şekilde bir fotonu ayırır, diğer fotonları Bob'a gönderir. Ayrıca, ne zaman bir tek foton yakalarsa ya sinyali bloke eder ya da üzerinde bir standart gizli dinleme yöntemi uygular ve Bob'a gönderir. Tahmin edileceği üzere, sinyalin polarizasyonundaki hatalar yalnızca tek foton sinyallerindeki gizli dinleme ile oluşur. Bu etki bir an için görmemezlikten gelinirse, yine demet bölme atağındakine benzer şekilde mümkün olan gizli anahtar değerindeki üst sınır $R \leq p_{exp} - p_{multi}$ şeklinde bulunur (Brassard, et al., 2000). Denklemde p_{multi} Alice'in bir çoklu foton sinyali göndermesinin ve bu sinyalin elenmiş anahtara girmesinin ortak olasılığı olup, p_{exp} bir sinyalin elenmiş anahtara girmesinin toplam olasılığıdır. Bu sınır, μ ortalama foton sayılı ve kanal için η tek foton geçirgenlikli bir poisson foton sayısı dağılımı için değerlendirilebilir. Bu durumda, $R \leq (1+\mu)e^{-\mu} - e^{-\mu\eta}$ bulunur. Bu da μ ve η'in sadece belli kombinasyonları için pozitiftir. Genellikle, verilen belli bir μ için, altında hiç bir güvenli anahtar üretilemeyen geçirgenlik kesme düzeyi vardır. Eve'in bu saldırıyı başarıyla gerçekleştirilebilmesi için hata oranının artmasına sebep olmamak amacıyla bazı tek foton sinyallerini yok etmesi gerektiği not edilmelidir.

9.3. GÜVENLİK ANALİZLERİNİN SONUÇLARI

Buraya kadar spesifik saldırılar tartışıldı. Bundan sonra, şu ana kadar bilinen tam güvenlik analizlerinin sonuçları özetlenecektir. Sonuçlar tipik olarak sadece büyük sayıda sinyal sayılarıyla sınırlı olarak verilir, dolayısıyla sinyallerin sınırlı dizilerinin istatistiki etkileri ihmal edilebilir.

9.3.1. Tek Fotonlarla B92 Protokolü

B92 protokolü yalnızca ortogonal olmayan iki sinyal durumu kullanır. Bu protokol KDA saldırısına müsaittir. Buna rağmen, giren sinyal durumlarının örtüşmesi ile kayıplı kanallar üzerinden koşulsuz güvenli anahtar dağıtımı elde etmek mümkündür. Bu protokol kayıplı ve kayıpsız kanallar için analiz edilmiştir (Tamaki, et al., 2003b). Anahtar değeri için bir kesin formül yoktur.

9.3.2. Tek Fotonlarla BB84 Protokolü

BB84 protokolünün güvenliği üzerinde Mayers, Shor ve Preskill tarafından çok çalışılmıştır. Mayers ispatında sinyallerin rastlantısal permutasyonlarını kullanmamış ve $R = 1 - h(\epsilon) - h(2\epsilon)$ ile verilen güvenli anahtar değerini elde etmiştir. Burada ϵ gözlenen hata oranı olup $h(x)$ ise $h(x) = -xlog_2 x - (1-x)log_2(1-x)$ ile verilen ikili entropi fonksiyonudur. Sinyallerin bir rastgele permutasyonunu da dahil ettiklerinden Shor ve Preskill tarafından verilen güvenlik değeri $R = 1 - 2h(\in)$ şeklinde olup daha yüksektir.

Bu senaryoda kesme hata oranı %11 civarındadır. Ancak kuantum ilintilerinin %25'e kadar doğrulanabildiği bilinmektedir. Gottesman ve Lo 2003 yılında protokolün açık görüşme fazında bu üst sınıra daha fazla yaklaşabilen iki yönlü bir iletişim protokolü sundular. Bu protokol, Chau tarafından 2002 yılında %20'yi tolere edecek kadar geliştirildi. Bu değer günümüzde BB84 protokolü için bilinen en yüksek hata oranı eşiğidir (Dusek, et al., 2006).

Bu protokol için kanaldaki herhangi bir kayıp, değerleri sadece tek foton geçirgenliğine tekabül eden bir ön katsayı kadar azaltabilir. Buradaki anahtar değerleri beklenen 1/2 ön katsayısı olmadan verilmiştir. Zira Alice ve Bob'un sinyal tabanları yalnızca vakaların yarısında örtüşür. Lo ve arkadaşlarının (2005a) işaret ettiği biçimde Alice ve Bob iki sinyal tabanı için olasılıkları asimetrik olarak seçebilirler. Limit dahilinde, temel olarak yalnızca bir taban kullanırlar ve diğer tabandaki sinyallerin yalnızca küçük bir bölümünü kontrol ederler. Bu durum, daha büyük bir örnekleme boyutu gerektirse de değer formüllerinde 1/2 çarpanı atılabilir.

9.3.3. Altı Durumlu Protokol

Altı durumlu protokol BB84 protokolüne benzer bir şekilde analiz edilebilir. Bu analiz üzerinde Lo tarafından çalışılmış ve Lo aşağıdaki anahtar değerini bulmuştur.

$$R = 1 + \left(1 - \frac{3\epsilon}{2}\right) log_2 \left(1 - \frac{3\epsilon}{2}\right) + \frac{3\epsilon}{2} log_2 \frac{\epsilon}{2} \quad (9.1)$$

Burada 1/3 ön çarpanını elde etmemek için yine protokolün üç tabanının asimetrik olarak kullanabileceği fikrinden yararlanılmıştır. Aynı zamanda, bu protokol için geliştirilmiş iki yönlü protokoller vardır. Şimdiye kadar bulunan en iyi hata eşiği Chau tarafından 2002'de % 27.6 olarak verilmiştir.

9.3.4. Zayıf Lazer Sinyalleriyle BB84 Protokolü

Pratik uygulamalarında zayıf lazer sinyalleri kullanılan BB84 protokolü özel bir önem taşımakta olup bu protokolün güvenliği üzerinde 2001 yılında Inamori ve arkadaşları tarafından çalışılmıştır. Bu protokol için sadece uzun dizilerin anahtar değerine değil, aynı zamanda sonlu anahtar boyutları için de tamamlanmış analizlere ulaşılmıştır. Burada Mayers'in tek fotonlu BB84 protokolü sonuçları genişletilir ve dolayısıyla sinyallerin rastlantısal permutasyonu kullanılmaz. Bu rastlantısal permutasyon Gottesman ve arkadaşları tarafından 2004 yılında ortaya atılmıştır. Uzun anahtar limitinde son anahtar değeri aşağıdaki gibi verilir (Dusek, et al., 2006).

$$R = (1 - \Delta) - h(\epsilon) - (1 - \Delta)h\left(\frac{\epsilon}{1-\Delta}\right) \quad (9.2)$$

Denklem (9.2)'de Δ, Bob tarafından alınan sinyallerin bir çoklu foton işlemi durumunda tüm sinyal bilgisinin Eve'e sızmış olabilecek kısmıdır. Bu kesir, kaynağın çoklu foton olasılığı p_{multi} ve Bob için toplam sinyal tespit olasılığı p_{exp}'e bağlı olarak $\Delta = p_{multi}/p_{exp}$ şeklinde verilebilir.

Bu sonuç Eve'in en genel atağı olan, ölçümlerini geciktirebildiği tutarlı atağa dayanır ve Bob'un tüm tespit kusurlarının Eve'e mal edildiği paranoyak bir tabloda bile mantıklı gizli anahtar değerlerinin verilebilmesini mümkün kılar. Şüphesiz, deneysel sistemin parametreleri optimize edilebilir. Sinyallerin μ ortalama foton sayısı değiştirilerek, η toplam geçirgenlik olmak üzere anahtar değerinin $R \sim \eta^2$ olması için aşağı yukarı $\mu \approx \eta$ seçilmesi gerektiğini görülebilir.

9.3.5. Zayıf Lazer Sinyalleriyle Tuzak Durumlu BB84 Protokolü

Zayıf lazer sinyalleriyle gerçekleştirilen BB84 protokolü, çoğunlukla foton sayısı bölme atağıyla verilen $R \sim \eta^2$ değerini verir. Bu saldırıdan kaçınmak için yapılabilecek, tuzak durumların kullanılmasıdır (Hwang, 2003; Lo, et al., 2005b; Wang, 2004a; Wang, 2004b). Burada Alice kanalı sadece tek bir ortalama foton sayısı olan sinyallerle ölçmez. Bunun yerine, ortalama foton sayısını rastgele değiştirir; bunu iki, üç veya daha fazla yoğunluk ayarıyla yapar. Buradaki fikir Eve'in tam PNS saldırısını artık tamamlayamayacak olmasıdır. Eve hala her çoklu foton sinyalinden bir fotonu ayırabilir fakat aynı ortalama foton sayılı herbir sinyal alt kümesinin doğru sayıda tek foton sinyallerini bloke edemez. Etki açısından bu, Eve'i yalnızca demet bölme atağını kullanmaya zorlar.

Bu temel fikir tam güvenlik analizi ile desteklenir (Lo, et al., 2005b). Burada son anahtar değerinin $R \sim \eta$ olduğu görülür ki bu da açıkça bu şemaların performansı üzerinde büyük bir gelişmedir. Şimdilerde güvenlikten feragat etmeden 100 km'nin üstündeki mesafelerde iletim mümkün olabilmektedir.

9.3.6. Güçlü Referans Sinyali ile B92 Protokolü

KAD protokollerinin değerini iyileştirmek için bir başka yaklaşım da faz referanslı tutarlı durumların kullanımıdır. Buradaki fikir yine, Eve'in belli etmeden sinyalleri bastırmasını imkansız hale getirmektir. Tam da bunun yapılabilmesi, KDA ve PNS saldırısını bu kadar güçlü yapar. Bu şema, bu durumda güvenli anahtar değerinin yine $R \sim \eta$ olduğunu teyit eden Koashi tarafından analiz edilmiştir (Dusek, et al., 2006).

9.4. YAN KANALLAR VE DİĞER KUSURLAR

Kriptografik cihazların fiziksel işleyişleri farkında olunmadan kötü niyetli kişilerin gizli bilgilere ulaşmasına yol açabilir. Yan kanal analizi, elektronik cihazların fiziksel özellikleri yoluyla, gizli tutulması gereken iç işleyişleri hakkında bilgi edinilmesidir. Matematiksel veya fiziksel olarak tam güvenlik sağlamak, bir cihazın fiziksel işleyişinin de güvenli olduğu anlamına gelmeyebilir. Yani güvenli olduğu düşünülen bir cihaz, iç işleyişi hakkında bilgi sızdırıyor olabilir. Yan kanallar yolu ile edinilen bilgi kriptografik cihazın güvenlik tanımını tamamıyla geçersiz kılabileceği gibi, kısmi bilgi sağlayarak imkan dahilinde olmayan saldırıları da olası hale getirebilir. Yan kanal yolu ile elde edilen bilgiler, sistem güvenliğini sadece %1 oranında azaltsa bile, bu sistemin kullanılamaz hale gelmesi demektir. Bir elektronik cihazın %99 oranında çalışması performans değerlendirmesi açısından kabul edilebilir olabilir. Oysa bir kriptografik cihazın %99 oranında güvenli olması güvensiz olduğu anlamına gelir. Bu nedenle, kriptografik cihazların her koşulda %100 güvenlik sağladıklarından emin olabilmek için fiziksel işleyiş sırasında sızdırılan bilgileri de dikkate almak gerekir (Karakoyunlu, 2009).

Şimdiye kadar, güvenlik tartışılırken sinyallerin protokolde tarif edildiği şekle tam uygun biçimde hazırlandığı varsayıldı. Halbuki, fiziksel gerçekleştirmelerde bir çok kusurlar olabilir. Örneğin, farklı sinyal polarizasyonlarının hazırlanması, sinyallerin zamanlamaları ve spektrumları gibi diğer serbestlik derecelerini de etkileyebilir. Dolayısıyla, istenenin dışındaki serbestlik derecelerini gözlemleyerek Eve sinyal ile ilgili olarak tipik güvenlik analizinde yakalanamayacak bilgiler elde edebilir.

Ayrıca başka kusurlar da göz ardı edilmemelidir. Tespit işlemi sırasında tipik olarak sinyal seçimlerinin rastlantısal olduğunu varsayılır. Ya Eve taban veya seçilen sinyal hakkında önceden bilgi sahibi olabilirse? Ya da eğer detektörler seçilen sinyal tabanına bir bağımlılık gösterirlerse veya Eve detektörleri bir dereceye kadar manipüle edebilirse? Dahası, Bob'un ölçüm tabanı ayarları detektör geri parıldamaları tarafından açık edilebilir. Bunun yanında Eve Alice'in aygıtından yansıyan ışığı ölçerek ayarlarını elde etmeyi umabilir. Bütün benzer olasılıklar dikkatle göz önüne alınmalı ve bertaraf edilmelidir. Şunu da eklemek gerekir ki çoğu kusur üzerlerinde kantitatif bir sınır koyulduğunda halledilebilir (Gottesman, et al., 2004). Ve bunlar küçük oldukları sürece, sonuçta elde edilen anahtar oranları üzerindeki etkileri de küçüktür.

10. BEKLENTİLER

Kuantum kriptografinin yüksek güvenlik seviyesi sağlayan verimli ve kullanıcı dostu sistemler sunmaya hazır olduğu açıktır. Klasik yöntemler hala kısa süreli güvenlik ihtiyacı olan şifrelemeler için güvenli olmakla birlikte, daha uzun süreli beklentiler ile bakıldığında kuantum kriptografinin daha değerli olduğu söylenebilir. Kuantum bilgisayarların geliştirilmesindeki ilerleme bilgi teknolojileri pazarında kuantum anahtar dağıtımı gereksinimini hızlandıracak belirgin bir rol oynayabilir. Kuantum anahtar dağıtımı ayrıca mevcut altyapı ile de gayet iyi birleştirilebilir. Çok düşük bit oranlı (saniyede yüzlerce bit) kuantum anahtar dağıtımı bile çağdaş kripto sistemleri belirgin bir şekilde geliştirebilir. Örneğin AES gibi simetrik şifreler için gizli anahtarların saniyede bir kaç kez değiştirilmesini sağlar.

Kuantum anahtar dağıtımının yaygın kullanımı 100 km'ye kadar olan sınırlı operasyon menzili yüzünden bir miktar kısıtlanmıştır. Bu durumu iyileştirmeye yönelik aşılması gereken üç ana teknolojik zorluk olup bunlar; 1) fiber komünikasyona uygun dalgaboylarında (1550 nm) çalışan detektörlerin gürültülerinin önemli biçimde azaltılması, 2) ultra düşük seviyede zayıflatıcı fiberlerin geliştirilmesi ve 3) kuantum yineleyicilerin geliştirilmesi olarak verilebilir.

Konuya ülkemiz açısından bakıldığında, kuantum kriptografiyi çeşitli optik hatların güvenliğini sağlamada tercih eden birçok ülke haklı olarak yüksek gizlilik içeren bu alandaki uygulamalardan elde edilen tecrübelerin en azından bir kısmının bilimsel ortamda açıklanmasını istememektedir. Ticari birkaç firmanın ürettiği kuantum kriptografi cihazları ise her link veya ağ yapısı ile uyumlu olmamakla birlikte buradan çıkan sonuç: Türkiye'deki gizlilik gerektiren çeşitli fiber ve optik hatlarda kullanılması muhtemel kuantum kriptografi sistemlerinin, ülkenin kendi imkanları ile tasarlanıp üretilmesi şarttır. Bunun için ise; 1) değişen fiber altyapısına uyum sağlayabilecek kuantum kriptografi tekniklerinin tasarlayabilecek, 2) teorik ve simulatif ortamda yapılacak analizlerden sonra deneysel ortamda sistem örneklerinin kurulum ve testini yapabilecek ve 3) endüstriyel uygulamalı mühendislik bilgisi çerçevesinde prototip sistem imalat ve gösterimini başarabilecek bilgi ve tecrübe birikiminin oluşması şarttır (Şahin ve Selçuk, 2006).

KAYNAKLAR DİZİNİ

Aksuoğlu, A., 2010, RSA Algoritmasının iyileştirilmesi için yeni bir yaklaşım, Yüksek lisans tezi, Anadolu Üniversitesi Fen Bilimleri Enstitüsü, 73 s.

Arda, D., Buluş, C. ve Yerlikaya, T. "Simetrik kriptosistemlerden çok alfabeli yerine koyma metodunun Türkiye Türkçesinin yapısal özelliklerini kullanarak kriptanalitik incelenmesi." Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, 2005, İstanbul, Türkiye.

Arıkan, S. A., 1999, Dünyada ve Türkiye'de elektronik ticaret çalışmalarına hukuki bir yaklaşım, Ankara: İGEME raporu.

Babaoğlu, A., 2009, Kriptolojinin geçmişi bir şifreleme algoritması kullanmadan önce son kullanma tarihine bakın!. Bilim ve Teknik Dergisi, 500, 24-27.

Baier, M. H., Pelucchi, E., Kapon, E., Varoutsis, S., Gallart, M., Robert-Philip I. and Abram, I., 2004, Single photon emission from site-controlled pyramidal quantum dots, Appl. Phys. Lett., 84, 648.

Bechmann-Pasquinucci, H. and Gisin, N., 1999, Incoherent and Coherent Eavesdropping in the 6-state Protocol of Quantum Cryptography, Phys. Rev. A, 59, 4238.

Bennett, C. H., Brassard, G. and Robert, J.-M., 1988, Privacy Amplification by Public Discussion, SIAM J. Comput. 17(2), 210.

Bennett, C. H. and Brassard, G., 1989, The Dawn of a New Era for Quantum Cryptography: The Experimental Prototype Is Working!, Sigact News 20(4), 78.

Bennett, C. H., Bessette, F., Brassard, G., Salvail, L. and Smolin, J., 1992a, Experimental Quantum Cryptography, J. Cryptology, 5, 3.

Bennett, C. H., 1992b, Quantum cryptography using any two nonorthogonal states, Phys. Rev. Lett., 68, 3121.

KAYNAKLAR DİZİNİ (devam)

Bennett, C. H., Brassard, G. and Mermin, N. D., 1992c, Quantum cryptography without Bell's theorem, Phys. Rev. Lett., 68, 557.

Bennett, C. H., Brassard, G., Crepeau, C., Jozsa, R., Peres, A. and Wootters, W. K., 1993, Teleporting an unknown quantum state via dual classical and Einstein-Podolsky-Rosen channels, Phys. Rev. Lett., 70, 1895.

Bennett, C. H., Brassard, G., Crepeau, C. and U. M. Maurer, 1995, Generalized Privacy Amplification, IEEE Transactions on Information Theory, 41, 1915.

Bennett, C. H., Brassard, G., Schumacher, B., Popescu, S., Smolin, J. and Wootters, W. K., 1996, Purification of Noisy Entanglement and Faithful Teleportation via Noisy Channels, Phys. Rev. Lett., 76, 722.

Bethune, D., and Risk, W., 2000, An autocompensating fiber-optic quantum cryptography system based on polarization splitting of light, IEEE J. Quantum Electron, 36, 340.

Beveratos, A., Brouri, R., Gacoin, T., Poizat, J.-P. and Grangier, P., 2001, Nonclassical radiation from diamond nanocrystals, Phys. Rev. A, 64 061802.

Beveratos, A., Brouri, R., Gacoin, T., Villing, A., Poizat, J.-P. and Grangier, P., 2002, Single Photon Quantum Cryptography, Phys. Rev. Lett., 89 187901.

Biham, E. and Knudsen, L. R., 1998, DES, Triple-DES and AES, RSA Laboratories' Cryptobytes, 4(1), 18.

Blakesley, J. C., See, P., Shields, A. J., Kardyna B. E., Atkinson, P., Farrer, I. and Ritchie, D. A., 2005, Efficient Single Photon Detection by Quantum Dot Resonant Tunneling Diodes, Phys. Rev. Lett., 94, 067401.

Bourennane, M., Gibson, F., Karlsson, A., Hening, A., Jonsson, P., Tsegaye, T., Ljunggren, D. and Sundberg, E., 1999, Experiments on long wavelength (1550 nm) plug and play quantum cryptography system, Opt. Express, 4, 383.

KAYNAKLAR DİZİNİ (devam)

Brassard G., Lütkenhaus, N., Mor, T. and Sanders, B. C., 2000, Limitations on Practical Quantum Cryptography, Phys. Rev. Lett., 85, 1330.

Breguet, J., Müller, A. and Gisin, N., 1994, Quantum Cryptography with Polarized Photons in Optical Fibers: Experimental and Practical Limits, J. Mod. Opt., 41, 2405.

Brendel, J., Gisin, N., Tittel, W. and Zbinden, H., 1999, Pulsed energy-time entangled twin-photon source for quantum communication, Phys. Rev. Lett., 82, 2594.

Boyacı, U. K. ve Kara, O., 2009. Bilgi güvenliği problemlerine matematiksel yaklaşım getiren bir bilim dalı: kriptoloji. Bilim ve Teknik Dergisi, 500, 42-48.

Brouri, R., Beveratos, A., Poizat, J.-P. and Grangier, P., 2000, Photon antibunching in the fluorescence of individual color centers in diamond, Opt. Lett., 25, 1294.

Bruss, D., 1998, Optimal Eavesdropping in Quantum Cryptography with Six States, Phys. Rev. Lett., 81, 3018.

Calver, T.I., 2011. An empirical analysis of the cascade secret key reconciliation protocol for quantum key distribution. Thesis, Air University, 85 p.

Chau, H. F., 2002, Practical scheme to share a secret key through a quantum channel with a 27.6% bit error rate, Phys. Rev. A, 66, 60302.

Clauser, J. F., Horne, M. A., Shimony, A. and Holt, R. A., 1969, Proposed Experiment to Test Local Hidden-Variable Theories, Phys. Rev. Lett., 23, 880.

Çağ, M. A., 2008. Negatiflik ve konkurus ölçümleri aracılığıyla kuantum dolaşık durumların betimlenmesi, Yüksek lisan tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, 72 s.

Çetin, Ö., 2006. Eliptik eğri kriptografisi, Yüksek lisans tezi, Gazi Üniversitesi Fen Bilimleri Enstitüsü, 111 s.

KAYNAKLAR DİZİNİ (devam)

Çimen, C., Akleylek, S. ve Akyıldız, E., 2011. Şifrelerin matematiği: kriptografi, ODTÜ Yayıncılık, Ankara.

Dalkılıç, G. ve Ayhan, E. "Kuantum kriptografide dinlenme (Eavesdropping) ve optik açıklar (Loopholes) kullanılarak gerçekleştirilen ataklar." Akademik Bilişim Konferansı, 2-4 Şubat 2005, Gaziantep Üniversitesi, Gaziantep.

Deavours, C. A. and Kruh, L., 1985, Machine Cryptography and Modern Cryptanalysis (Artech House, Dedham MA).

Demirburan, Y. ve Yazgan, E., 1987. Optik fiber ve optik iletişim. Hacettepe Üniversitesi Elektrik Mühendisliği Dergisi, 343, 104-109.

Demirel, Ö., 2007, Kuantum şifreleme sanatı. Bilim ve Teknik, 64-66.

Dereli, T., 2009, İletişimde mutlak güvenlik için kuantum kriptografi. Bilim ve Teknik Dergisi, 500, 54-57.

DES cracker 1 accessed.
http://www.distributed.net/index.html.en.

DES cracker 2 accessed.
http://www.eff.org/Privacy/Crypto/Crypto misc/DESCracker.

Diamanti, E., Takesue, H., Honjo, T., Inoue, K. and Yamamoto, Y., 2005, Performance of various quantum key distribution systems using 1.55 μm up-conversion single-photon detectors, Los Alamos e-print archive: quant-ph/0506036.

Duran, D., 2011, Kuantum dolanıklık ve kuantum bilişim kuramındaki uygulamaları, Yüksek lisans tezi, Ankara Üniversitesi Fen Bilimleri Ensitüsü, 113 s.

Dusek, M., Haderka, O. and Hendrych, M., 1999, Generalized Beam-Splitting Attack in Quantum Cryptography with Dim Coherent States, Opt. Commun., 169, 103.

KAYNAKLAR DİZİNİ (devam)

Dusek, M., Jahma, M. and Lütkenhaus, N., 2000, Unambiguous state discrimination in quantum cryptography with weak coherent states, Phys. Rev. A, 62, 022306.

Dusek, M., Lütkenhaus,N. and Hendrych, M., 2006, Quantum cryptography. accessed. http://arxiv.org/abs/quant-ph/0601207, 25 November 2011.

Dür, W., Briegel, H.-J., Cirac, J. I., Zoller, P., 1999, Quantum repeaters based on entanglement purification, Phys. Rev. A, 59, 169.

Ekert, A., 1991, Quantum cryptography based on Bell's theorem, Phys. Rev. Lett., 67, 661 p.

Ekert, A. K., Rarity, J. G., Tapster, P. R. and Palma, G. M., 1992, Practical quantum cryptography based on two-photon interferometry, Phys. Rev. Lett., 69, 1293.

Franson, J. D., 1989, Bell inequality for position and time, Phys. Rev. Lett., 62, 2205.

Fraser, G. W., Heslop-Harrison, J. S., Schwarzacher, T., Holland, A. D., Verhoeve, P. and Peacock, A., 2003, Detection of multiple fluorescent labels using superconducting tunnel junction detectors, Review of Scientific Instruments, 74, 4140.

Fuchs, C., Gisin, N., Griffits, R. B., Niu, C.-S. and Peres, A., 1997, Optimal Eavesdropping in Quantum Cryptography, I. Information Bound and Optimal Strategy, Phys. Rev. A, 56, 1163.

Gaebel, T., Popa, I., Gruber, A., Domhan, M., Jelezko, F. and Wrachtrup, J., 2004, Stable single-photon source in the near infrared, New Journal of Physics, 6, 98.

Gerard, J.-M., Sermage, B., Gayral, B., Legrand, B., Costrad, E. and Thierry-Mieg, V., 1998, Enhanced Spontaneous Emission by Quantum Boxes in a Monolitic Optical Microcavity, Phys. Rev. Lett., 81, 1110.

Gisin, N., Ribordy, G., Tittel, W. and Zbinden, H., 2002, Quantum cryptography, Rev. Mod. Phys., 74, 145.

KAYNAKLAR DİZİNİ (devam)

Gisin, N., Ribordy, G., Zbinden, H., Stucki, D., Brunner, N. and Scarani, V., 2004, Towards practical and fast Quantum Cryptography, Los Alamos e-print archive: quant-ph/0411022.

Gobby, C., Yuan, Z. L. and Shields, A. J., 2004, Quantum key distribution over 122 km of standard telecom fiber, Appl. Phys. Lett., 84, 3762.

Gottesman, D., H.-K. Lo, N. Lütkenhaus, and Preskill, J., 2004, Security of quantum key distribution with imperfect devices, Quant. Inf. Comp., 4, 325.

Gümüş, E. "Kuantum kriptografi ve anahtar dağıtım protokolleri". Akademik Bilişim Konferansı, 2-4 Şubat 2011, İnönü Üniversitesi, Malatya.

Güngördü, U., 2010, Quantum key distribution protocols, Master of science thesis, Koç University Graduate School of Sciences and Engineering, 79 p.

Hışıl, H. "Crympıx: kriptografik çok-basamaklı kütüphane". 1. Ağ ve Bilgi Güvenliği Sempozyumu, 9-11 Haziran 2005, İstanbul Teknik Üniversitesi, İstanbul.

Hours, J., Varoutsis, S., Gallart, M., Bloch, J., Robert-Philip, I., Cavanna, A., Abram, I., Laruelle, F. and Gerard, J.M., 2003, Single photon emission from individual GaAs quantum dots, Appl. Phys. Lett., 82 2206.

http://www.cesnet.cz/doc/techzpravy/2007/mrv-terescope-700/.

http://swissquantum.idquantique.com/?Raw-Key-Exchange.

http://en.wikipedia.org/wiki/Spontaneous_parametric_down-conversion.

http://tr.wikipedia.org/wiki/Lazer.

KAYNAKLAR DİZİNİ (devam)

Hughes, R., Luther, G. G., Morgan, G. L. and Simmons, C., 1996, Quantum cryptography over underground optical fibers, Lecture Notes in Computer Science, 1109, 329.

Hughes, R., Morgan, G. and Peterson, C., 2000, Quantum key distribution over a 48-km optical fiber network, J. Mod. Opt., 47, 533.

Hughes R. J., Nordholt, J.E., Derkacs, D. and Peterson, C.G., 2002, Practical freespace quantum key distribution over 10 km in daylight and at night, New J. Phys., 4, 43.

Hwang, W.-Y., 2003, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett., 91, 057901.

Inamori, H., Lütkenhaus, N., and Mayers, D., 2001, Unconditional security of practical quantum key distribution, Los Alamos e-print archive: quant-ph/0107017.

İpekoğlu, Y., 2009. IARS kuantum bilgi kuramının temel kavramları, ODTÜ Fizik Bölümü, Ders notu, 94 s.

Jacobs, B. C. and Franson, J.D., 1996, Quantum Cryptography in Free Space, Opt. Lett., 21, 1854.

Kahn, D., 1967, The Codebreakers: The Story of Secret Writing (Macmillan, New York).

Karakoyunlu, D., 2009. Kara kutu mu, şeffaf kutu mu?. Bilim ve Teknik Dergisi, 500, 50-53.

Keller, M., Lange, B., Hayasaka, K., Lange, W. and Walther, H., 2004, A calcium ion in a cavity as a controlled single-photon source, New J. Phys., 6, 95.

Keren, S., 2011, Kriptoloji ile gelişen teknolojiler, Bitirme Tezi (yayımlanmamış), Yıldız Teknik Üniversitesi Kimya-Metalürji Fakültesi, 81 s.

KAYNAKLAR DİZİNİ (devam)

Keskin, B., 2008, Bilişim sistemlerinin stratejik yönetim açısından önemi, Yüksek lisans tezi, Gebze İleri teknoloji Enstitüsü Fen Bilimler Enstitüsü, 414 s.

Kışoğlu, H. F., 2008, CMS HCAL Hadronik Kapak Kalorimetresindeki hibrid foto-diyotların enerji kazanç kararlılığı çalışmaları, Yüksek lisans tezi, Çukurova Üniversitesi Fen Bilimleri Enstitüsü, 75 s.

Kim, J., Takeuchi, S., Yamamoto, Y. and Hogue, H., 1999, Development of a high quantum-efficiency single-photon counting system App. Phys. Lett., 74, 902.

Kimura, T., Nambu, Y., Hatanaka, T., Tomita, A., Kosaka, H. and Nakamura, K., 2004, Single-photon interference over 150-km transmission using silicabased integrated-optic interferometers for quantum cryptography, Jpn. J. Appl. Phys., 43, L1217.

Kodaz, H. "RSA şifreleme algoritmasının uygulaması". Akademik Bilişim Konferansı, 3-5 Şubat 2003, Çukurova Üniversitesi, Adana.

Kolkıran, A., 2010, Bakmadan görmek mümkün mü?. NTV Bilim Dergisi, 21, 40-43.

Kurtsiefer, C., Zarda, P., Mayer, S. and Weinfurter, H., 2001, The breakdown flash of silicon avalanche photodiodes-back door for eavesdropper attacks, J. Mod. Opt., 48, 2039.

Kurtsiefer, C., Zarda, P., Halder, M., Gorman, P. M., Tapster, P. R., Rarity, J. G. and Weinfurter, H., 2002a, Long distance free-space quantum cryptography, in: Quantum optics in computing and communications, Eds. S. Liu, G. Guo, H.-K. Lo, N. Imoto, Proceedings SPIE, 4917, 25.

Kurtsiefer, C., Zarda, P., Halder, M., Weinfurter, H., Gorman, P. M., Tapster, P. R., Rarity, J. G., 2002b, Quantum cryptography: A step towards global key distribution, Nature 419 450.

Küçükkara, İ. ve Kiraz, A., 2010, Kuantum optiği ve elektromanyetik etkili saydamlık ve tek foton üretimi. Bilim ve Teknik Dergisi, 510, 62-65.

KAYNAKLAR DİZİNİ (devam)

Leary, T. P., 1996, Cryptology in the 15th and 16th Century, Cryptologia, 20(3), 223.

Lo, H.-K., Chau, H. F. and Ardehali, M., 2005a, Efficient Quantum Key Distribution Scheme And Proof of Its Unconditional Security, Journal of Cryptology, 18, 133.

Lo, H.-K., Ma, X. and Chen, K., 2005b, Decoy state quantum key distribution, Phys. Rev. Lett., 94, 230504.

Loepp, S. and Wootters, W. K., 2006, Protecting information: from classical error correction to quantum cryptography, Cambridge University Press, 305 p.

Lütkenhaus, N., 2000, Security against individual attacks for realistic quantum key distribution, Phys. Rev. A, 61, 052304.

Ma, X., 2004, Security of Quantum Key Distribution with Realistic Devices, Los Alamos e-print archive: quant-ph/0503057.

Marand, C., and Townsend, P. D., 1995, Quantum key distribution over distances as long as 30 km, Opt. Lett., 20, 1695.

Marcikic, I., Riedmatten, H. de., Tittel, W., Zbinden, H., Legre, M., Gisin, N., 2004, Distribution of time-bin qubits over 50 km of optical fiber Los Alamos e-print archive: quant-ph/0404124.

Miller, A. J., Nam, S. W., Martinis, J. M. and Sergienko, A. V., 2003, Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination, Appl. Phys. Let., 83, 791.

Mirin, R. P., 2004, Photon antibunching at high temperature from a single In-GaAs/GaAs quantum dot, Appl. Phys. Lett., 84, 1260.

Moreau, E., Robert, I., Manin, L., Thierry-Mieg, V., Gerard, J.M. and Abram, I., 2001, Quantum Cascade of Photons in Semiconductor Quantum Dots, Phys. Rev. Lett., 87, 183601.

KAYNAKLAR DİZİNİ (devam)

Müller, A., Breguet, J. and Gisin, N., 1993, Experimental Demonstration of Quantum Cryptography Using Polarized Photons in Optical Fibre over More than 1 km, Europhys. Lett., 23, 383.

Müller, A., Herzog, T., Huttner, B., Tittel, W., Zbinden, H. and Gisin, N., 1997, Plug and play systems for quantum cryptography, Appl. Phys. Lett., 70, 793.

Nabiyev, V. V. ve Günay, A. Şifreleme yönteminin tespiti amacıyla çeşitli şifreleme algoritmalarının araştırılması, 1. Ulusal Elektronik İmza Sempozyumu Bildiri Kitabı, 7-8 Aralık 2006, Gazi Üniversitesi, Ankara.

Nielsen, M. A., and Chuang, I. L., 2000, Quantum Computation and Quantum Information (Cambridge Univ. Press, Cambridge).

Ordu, L. ve Örs Yalçın, S.B. "Yan kanal analizlerine genel bakış". 5. Ulusal Elektronik İmza Sempozyumu Bildiri Kitabı, 7-8 Aralık 2006, Gazi Üniversitesi, Ankara.

Özen, S., 2009, Tuzaklanmış iyonda negativity ve konkurus hesaplarıyla kuantum dolaşıklık, Yüksek lisans tezi, Afyon Kocatepe Üniversitesi Fen Bilimleri Enstitüsü, 74 s.

Özler, İ., 2007, Bilgi güvenliği ve elektronik imza kavramları, ekonomik boyutlarının incelenmesi ve elektronik imza uygulamaları, Yüksek lisans tezi, Dicle Üniversitesi Sosyal Bilimler Enstitüsü, 125 s.

Poppe, A., Fedrizzi, A., Lorünser, T., Maurhadt, O., Ursin, R., Böhm, H. R., Peev, M., Suda, M., Kurtsiefer, C., Weinfurter, H., Jennewein, T. and Zeilinger, A., 2004, Practical Quantum Key Distribution with Polarization Entangled Photons, Opt. Express,12, 3865.

Proje Bilişim Güvenliği ve Araştırma Ltd Şti, 2003. Bilişim güvenliği, 66 s. erişim. http://www.pro-g.com.tr/

Ribordy, G., Gautier, J.-D., Gisin, N., Guinnard, O. and H. Zbinden, 2000, Fast and user-friendly quantum key distribution, J. Mod. Opt., 47, 517.

KAYNAKLAR DİZİNİ (devam)

Ribordy, G., Brendel, J., Gautier, J. D., Gisin, N. and Zbinden, H., 2001, Long distance entanglement based quantum key distribution, Phys. Rev., A 63, 012309.

Rosa, T., 2001, Future Cryptography: Standards Are Not Enough, in: Proc. Of Security and Protection of Information, NATO - IDET (Military Academy in Brno, Brno) 237.

Rosenberg, D., Lita, A. E., Miller, A. J. and S. W. Nam, 2005, Noise-free highefficiency photon-number-resolving detectors, Phys. Rev. A, 71, 061803(R).t

Sağıroğlu, Ş. ve Mustafa A., 2005, Her yönüyle elektronik imza, Grafiker Yayınları, 17 s.

Sağıroğlu, Ş., 2011, Şifreleme bilimi. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi, Ders notu, 61 s.

Sakallı, M.T., 2006, Modern şifreleme yöntemlerinin gücünün incelenmesi, Yüksek lisans tezi, Trakya Üniversitesi Fen Bilimleri Enstitüsü, 203 s.

Santori, C., Pelton, M., Solomon, G., Dale, Y. and Yamamoto, Y., 2001, Triggered Single Photons from a Quantum Dot, Phys. Rev. Lett., 86, 1502.

Sergienko, A. V., (Ed.) 2006, Quantum communications and cryptography. accessed. http://vnuki.org/library/book/211002

Soyalıç, S., 2005, Kriptografik hash fonksiyonları ve uygulamaları, Erciyes Üniversitesi Fen Bilimleri Enstitüsü, 92 s.

Stinson, D. R., 1995, Cryptography, Theory and Practice (CRC Press, Boca Raton).

Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. and H. Zbinden, 2002, Quantum key distribution over 67 km with a plug&play system, New J. Phys., 4, 41.

KAYNAKLAR DİZİNİ (devam)

Şahin, A. B., Selçuk, G. "İletişim ağ güvenliğinde son aşama: kuantum kriptografi ve fiber optik ortamda kuantum temelli rastsal sayı üretimi". Ulusal Elektronik İmza Sempozyumu, 7-8 Aralık 2006, Gazi Üniversitesi, Ankara.

Şen, G.A., 2002, Kuantum bilgi-işlem algoritmaları üzerine bir inceleme, Yüksek lisans tezi, Ege Üniversitesi Fen Bilimleri Enstitüsü, 142 s.

Takemoto, K., Sakuma, Y., Hirose, S., Usuki, T., Yokoyama, N., Miyazawa, T., Takatsu, M. and Arakawa, Y., 2004, Non-classical Photon Emission from a Single InAs/InP Quantum Dot in the 1.3-μm Optical-Fiber Band, Japan. J. App. Phys., 43, L993.

Tamaki, K., Koashi, M., and Imoto, N., 2003a, Security of the Bennett 1992 quantum key distribution protocol against individual attack over a realistic channel, Phys. Rev. A, 67, 032310.

Tamaki, K., Koashi, M. and Imoto, N., 2003b, Unconditionally secure key distribution based on two nonorthogonal states, Phys. Rev. Lett., 90, 167904.

Tittel, W., Brendel, J., Zbinden, H. and Gisin, N., 2000, Quantum cryptography using entangled photons in energy-time Bell states, Phys. Rev. Lett., 84, 4737.

Townsend, P., Rarity, J. G. and Tapster, P. R., 1993, Single photon interference in a 10 km long optical fiber interferometer, Electron. Lett., 29, 634.

Townsend, P., 1994, Secure key distribution system based on quantum cryptography, Electron. Lett., 30, 809.

Townsend, P., 1997, Simultaneous quantum cryptographic key distribution and conventional data transmission over installed fibre using WDM, Electron. Lett., 33, 188.

Toyran, M., 2003, Kuantum kriptografi, Yüksek lisans tezi, İstanbul Teknik Üniversitesi Fen Bilimleri Enstitüsü, 176 s.

KAYNAKLAR DİZİNİ (devam)

Toyran, M. "Kuantum kriptografi, benzetimi ve analizi". 15. İstatistik Araştırma Sempozyumu, 11-12 Mayıs 2006, Ankara.

Toyran, M., 2007, Kuantum kriptografi. Tübitak Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi. erişim. http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=4298797&userType=inst

Tübitak, 2009, RFID Mahremiyet protokolleri, Integration of CryptoD to Era FP7 Project ICE, 37 s.

Turgut, S., 2003a, Kuantum bilgisayar. Bilim ve Teknik Dergisi, 426, 50-52.

Turgut, S., 2003b, Karanlıkta kuantum görme. Bilim ve Teknik Dergisi, 428, 38-41.

Turgut, S., 2010, EPR düşünce deneyi. Bilim Felsefe ve Sanat Dergisi, 1, 20-27.

Türkpençe, D., 2006, Kuantum mekaniğine felsefi bakış. Yüksek lisans semineri, Ondokuz Mayıs Üniversitesi Fizik Anabilim dalı, 38 s.

Türkpençe, D., 2007, NMR Kuantum bilgisayarlarında iki kutriklik bazı mantık kapılarının oluşturulması ve uygulamaları, Ondokuz Mayıs Üniversitesi Fen Bilimleri Enstitüsü, 112 s.

Vandersypen, L. M. K., Steffen, M., Breyta, G., Yannoni, C. S., Sherwood, M. H., and Chuang, I. L., 2001, Experimental Realization of Shor's Quantum Factoring Algorithm Using Nuclear Magnetic Resonance, Nature, 414, 883.

Verevkin, A., Zhang, J., Sobolewski, R., Lipatov, A., Okunev, O., Chulkova, G., Korneev, A., Smirnov, K., Goltsman, G.N., and Semenov, A., 2002, Detection efficiency of large-active-area NbN single-photon superconducting detectors in the ultraviolet to near-infrared range, Appl. Phys. Lett., 80, 4687.

KAYNAKLAR DİZİNİ (devam)

Verevkin, A., Pearlmany, A., Slyszyz, W., Zhangy, J., Currie, M., Korneev, A., Chulkova, G., Okunev, O., Kouminov, P., Smirnov, K., Voronov, B., Goltsman, G. N. and Sobolewskiy, R., 2004, Ultrafast superconducting single-photon detectors for near-infrared-wavelength quantum communications, J. Mod. Opt., 51, 1447.

Volz, J., Kurtsiefer, and Weinfurter, H., 2001, Compact all-solid-state source of polarization-entangled photon pairs, Appl. Phys. Lett., 79, 869.

Waks, E., Inoue, K., Santori, C., Fattal, D., Vuckovic, J., Solomon, G. S. and Yamamoto, Y., 2002, Secure communication: Quantum cryptography with a photon turnstile, Nature, 420, 762.

Waks, E., Inoue, K., Oliver, W. D., Diamanti, E. and Yamamoto, Y., 2003, High Effciency Photon Number Detection for Quantum Information Processing, Los Alamos e-print archive: quant-ph/0308054.

Wang, X.-B., 2004a, Beating the pns attack in practical quantum cryptography, Los Alamos e-print archive: quant-ph/0410075.

Wang, X.-B., 2004b, A decoy-state protocol for quantum cryptography with 4 intensities of coherent light, Los Alamos e-print archive: quant-ph/0411047.

Wegman, M. N. and Carter, J. L., 1981, New hash functions and their use in authentication and set equality, Journal of Computer and System Sciences, 22, 265.

Wiener, M., 1997, Efficient DES Key Search – An Update, RSA Laboratories' Cryptobytes, 3 (2), 6.

Wooters, W. K. and Zurek,W. H., 1982, A single quantum cannot be cloned, Nature, 299, 802.

Yerlikaya, T., Buluş, E. ve Buluş, N. "Kripto algoritmalarının gelişimi ve önemi". Akademik Bilişim Konferansı, 9-11 Şubat 2006, Pamukkale Üniversitesi, Denizli.

KAYNAKLAR DİZİNİ (devam)

Yıldırım, K., 2006, Veri şifrelemesinde simetrik ve asimetrik anahtarlama algoritmalarının uygulanması (Hybrid şifreleme), Kocaeli Üniversitesi Fen Bilimleri Enstitüsü, 101 s.

Yıldırım, K. ve Demiray, H. E., 2008, Simetrik ve asimetrik şifreleme yöntemlerine metodlar: çırpılmış ve birleşmiş AKM ve VKM, Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 23,3, 539-548.

Yuan, Z. L., B. E. Kardynal, R. M Stevenson, A. J. Shields, C. J. Lobo, K. Cooper, N. S. Beattie, D. A. Ritchie, and M. Pepper, 2002, Electrically Driven Single-Photon Source, Science, 295, 102.

Yuan, Z. L. and A. J. Shields, 2005, Continuous operation of a one-way quantum key distribution system over installed telecom fibre, Opt. Exp., 13, 660.

Zhao, Y., Qi, B., Ma, X., Lo, H.-K. and Qian, L., 2005, Experimental Decoy State Quantum Key Distribution Over 15 km Los Alamos e-print archive: quant-ph/0503192.

Zukowski, M., A. Zeilinger, M. A. Horne, and A. Ekert, 1993, “Event-ready-detectors” Bell experiment via entanglement swapping, Phys. Rev. Lett., 71, 4287.

Zwiller, V., H. Blom, P. Jonsson, N. Panev, S. Jeppesen, T. Tsegaye, E. Goobar, M.-E. Pistol, L. Samuelson, and G. Björk, 2001, Single quantum dots emit single photons at a time: Antibunching experiments, Appl. Phys. Lett., 78, 2476.