ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Communication through Photon Using Quantum Cryptography: A Survey

Leenata B. Isal[1], Prof. Chetan J. Shelke[2]

M.E Student, Dept of CSE, P. R. Patil college of Engineering and Technology, Amravati, Maharashtra, India

Professor, Dept of IT, P. R. Patil college of Engineering and Technology, Amravati, Maharashtra, India.

ABSTRACT: Quantum cryptography is an approach toward secure communication by applying the phenomena of quantum physics. As compared to the classical cryptography, quantum cryptography provides more secure communication whose security depends only on the validity of quantum theory. It is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic key material using the transmission of quantum states of light. Quantum cryptography is one of the few commercial applications of quantum physics at the quantum level. The quantum relies on two important elements of quantum mechanics- the Heisenberg uncertainty principle and principle of photon polarization. This paper focuses on the principle of quantum cryptography and how this technology contributes in security of network.

KEYWORDS: Quantum Cryptography, network security, Quantum Key Distribution (QKD), BB84 protocol.

I. INTRODUCTION

One of the important issues in the network (wired or wireless) is the security. When we talk about security, the important aspects of any system are confidentiality, integrity, availability, non-repudiation and authentication. Cryptography is the strongest tool for controlling against many kinds of security threats. The classical cryptography is based on symmetric key or asymmetric key technique.

Quantum cryptography is the technique of secret writing that uses the concept of quantum physics to develop a cryptosystem, which provide a secure communication between two parties by establishing the channel called quantum channel, so that eavesdropper cannot intercept the knowledge of key. The important feature of quantum cryptography is to detect the presence of third party (eavesdropper) trying to access the knowledge of key. Quantum cryptography provide high level of security and robust network for standard Internet traffic flows such as web-browsing, e-commerce, and streaming video; and 100% compatible with conventional Internet technology. It will be a beneficial for the military, research & development, academics and industries.

II. RELATED WORK

The first quantum cryptographic ideas were proposed by Stephen Wiesner wrote "Conjugate Coding" [1, 2] in 1983 was rejected by IEEE Information Theory but was eventually published in 1983 in SIGACT News (15:1 pp. 78-88, 1983). Stephen Wiesner showed in his paper how to store or transmit two messages by encoding them in two "conjugate observables", such as linear and circular polarization of light, so that either, but not both, of which may be received and decoded.

In the mean time, Charles H. Bennett (who knew of Wiesner's idea) and Gilles Brassard picked up the subject and brought it to fruition in a series of papers that culminated with the demonstration of an experimental prototype that established the technological feasibility of the concept. Most quantum cryptographic key distribution protocols developed during that time were based on Heisenberg's Uncertainty Principle and Bell's Inequality. The first quantum cryptographic communication protocol, called BB84, was invented in 1984 by Bennett and Brassard as part of research study between physics and information at IBM lab[3,4].

In [3], Wiesner used bright light to construct a quantum cryptosystem (S. Wiesner, 1993). Huttner and Peres employed noncoupled photons to exchange keys (B. Hutter and A. Peres, 1994), and Huttner et al. also applied a weak

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

correlation to reduce significantly the level of tapped information (B. Hutter, 1995). Phoenix et al.(S.J.D. Phoenix, 1995) introduced a method of developing a quantum cryptographic network. Biham et al. (E.Biham, 1996) was developed a quantum non-localization cryptosystem rather than quantum cryptographic network.

In [3], the first one who examined the security of quantum cryptosystems was Lutkenhaus (N. Lutkenhaus, 1996). In (E. Biham and T. Mor, 1997a, b) Biham and Mor presented a method of resolving collective attack. Mayers and Salvail (D. Mayers and L. Salvail, 1994), Yao (A.C.-C. Yao, 1995) and Mayers (D. Mayers, 1996) based their research on BB84 Protocol, believing that this method could provide unconditional security and resist various attacks.

III. FUNDAMENTALS OF QUANTUM CRYPTOGRAPHY

Quantum cryptography uses the concept of quantum physics. In classical physics, a thing is described by its state, where as in quantum physics, a thing is described by the probabilities that the thing is in a certain state. Quantum communication involves encoding information in quantum states, or qubits, in contrast to classical communication's use of bits. A quantum bit (qubit) can be 0 or 1 at the same time. It cannot be copied (no cloning theorem) and its state will collapse if it is observed or measured. For qubits, we need a two-state system. In principle, any property in the microscopical world that has two possible states may serve as a qubit.

In [5], Light waves are propagated as discrete quanta called photons. A photon is an elementary particle of light, carrying a fixed amount of energy. They are mass less and have momentum and angular momentum called spin. Spin carries the polarization. Based on physical law, light may be polarized; polarization is a physical property that emerges when light is regarded as an electromagnetic wave. The direction of a photon's polarization can be fixed to any desired angle (using a polarizing filter) and can be measured using a calcite crystal. If on its way we put a polarization filter a photon may pass through it or may not. An optical fiber is a thin, flexible medium that conducts pulses of light, with each pulse representing a bit.

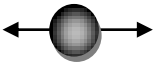
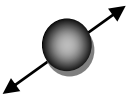
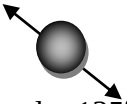
Rectilinear Polarization	 Angle=90°	 Angle=0°
Diagonal Polarization	 Angle=45°	 Angle=135°
Bit value	1	0

Fig.1. Photon polarization

Suppose sender uses 0-deg/90-deg polarizer sending photons to receiver. But he does not reveal which. Receiver can determine photons by using filter aligned to the same basis. But if he uses 45deg/135 deg polarizer to measure the photon he will not be able to determine any information about the initial polarization of the photon. The result of his measurement will be completely random. Each photon carries one qubit of information. A user can suggest a key by sending a stream of randomly polarized photons. This sequence can be converted to a binary key. If the key was intercepted it could be discarded and a new stream of randomly polarized photons sent.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

IV. QUANTUM KEY DISTRIBUTION(QKD)

In [6], Quantum key distribution as a cryptographic primitive offers security that is guaranteed by the laws of physics. Quantum Key Distribution as a method for secure key establishment is proven to be information theoretically secure against arbitrary attacks, including quantum attacks. Quantum key distribution uses the concept of public key cryptography but with quantum communication.

Conceptually, the security of QKD is achieved by encoding information in quantum states of light. Using quantum states allows security to be based on fundamental laws in quantum physics and quantum information theory. There are three deeply related notions from quantum physics that illustrate the source of the unique security properties of QKD:

1. The Heisenberg uncertainty principle [7] implies that by measuring an unknown quantum-mechanical state, it is physically changed. In the context of QKD, this means that an eavesdropper observing the data stream will physically change the values of some of the bits in a detectable way.
2. The no cloning theorem [8] states that it is physically impossible to make a perfect copy of an unknown quantum state. This means that it is impossible for an adversary to make a copy of a bit in the data stream to only measure one of the copies in hopes of hiding their eavesdropping.
3. There exist properties of quantum entanglement that set fundamental limits on the information leaked to unauthorized third parties.

Figure 2 shows quantum cryptographic communication system for securely transferring random key.

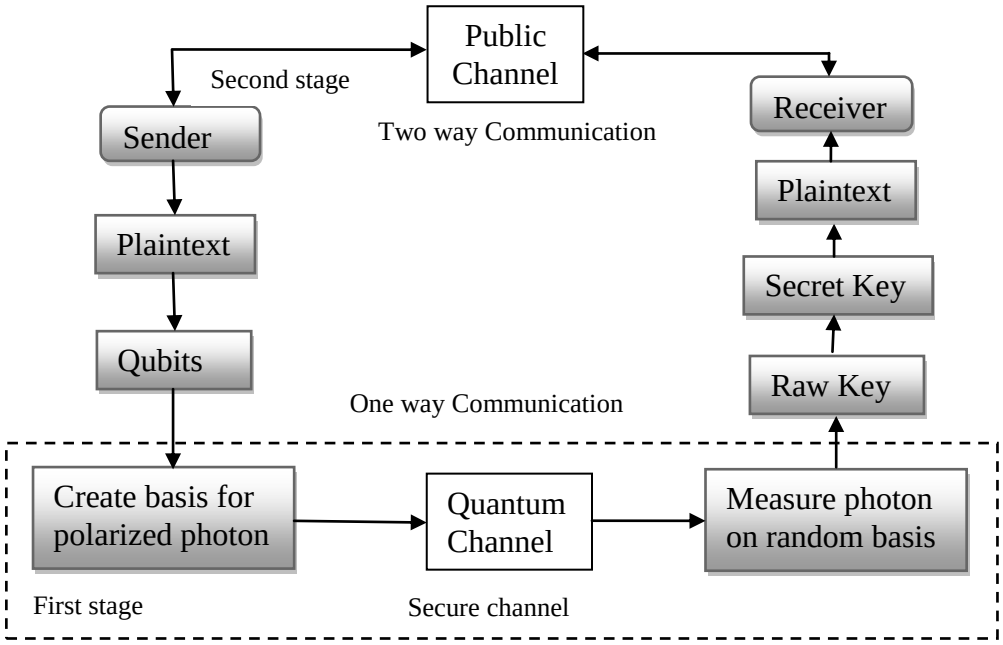


Fig.2. Quantum cryptographic communication system

Stage 1: Communication over a quantum channel:

In the first stage, Alice is required, each time she transmits a single bit, to use randomly with equal probability one of the two orthogonal basis + or x. Since no measurement operator of + is compatible with any measurement operator of x, it follows from the Heisenberg uncertainty principle that no one, not even Bob or Eve, can receive Alice's transmission with an accuracy greater than 75%.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Stage 2: Communication in two phases over a public channel:

In stage 2, Alice and Bob communicate in two phases over a public channel to check for Eve's presence by analyzing Bob's error rate.

Phase 1 of Stage 2: Extraction of raw key:

Phase 1 of stage 2 is dedicated to eliminating the bit locations at which error could have occurred without Eves eavesdropping. Bob begins by publicly communicating to Alice which measurement operators he used for each of the received bits. Alice then in turn publicly communicates to Bob which of his measurement operator choices were correct. After this two way communication, Alice and Bob delete the bits corresponding to the incompatible measurement choices to produce shorter sequences of bits which we call respectively Alice's raw key and Bob's raw key. If there is no intrusion, then Alice's and Bob's raw keys will be in total agreement.

Phase 2 of Stage 2: Detection of Eve's intrusion via error detection

Alice and Bob now initiate a two way conversation over the public channel to test for Eve's presence. In the absence of noise, any discrepancy between Alice's and Bob's raw keys is proof of Eve's intrusion. So to detect Eve, Alice and Bob select a publicly agreed upon random subset of m bit locations in the raw key, and publicly compare corresponding bits, making sure to discard from raw key each bit as it is revealed.

Should at least one comparison reveal an inconsistency, then Eve's eavesdropping has been detected, in which case Alice and Bob return to stage 1 and start over.

V. PRINCIPLE OF BB84 PROTOCOL

This BB84 protocol [9, 10] was invented by Charles Bennett and Gilles Brassard in 1984.The description of protocol is as follows:

1. A sender sends a stream of polarized photons to receiver. The photons can be polarized in rectilinear (0° or 90°) or diagonal direction (45° or 135°). A stream of photons is string of zeros and ones with direction specified for each bit.
2. Receiver measures this stream of photons with the help of randomly selected basis i.e. rectilinear or diagonal, and records the results. It is not necessary that sender and receiver will use same basis for measurement.
3. Receiver informs sender, his basis used for measurement of photons, through public channel.
4. Sender then compares the received basis with the actual basis and informs receiver over the public channel, the correct bits. The correct bits are those whose bases are same.
5. Then sender and receiver discard the incorrect bits and the correct ones are considered as a key.

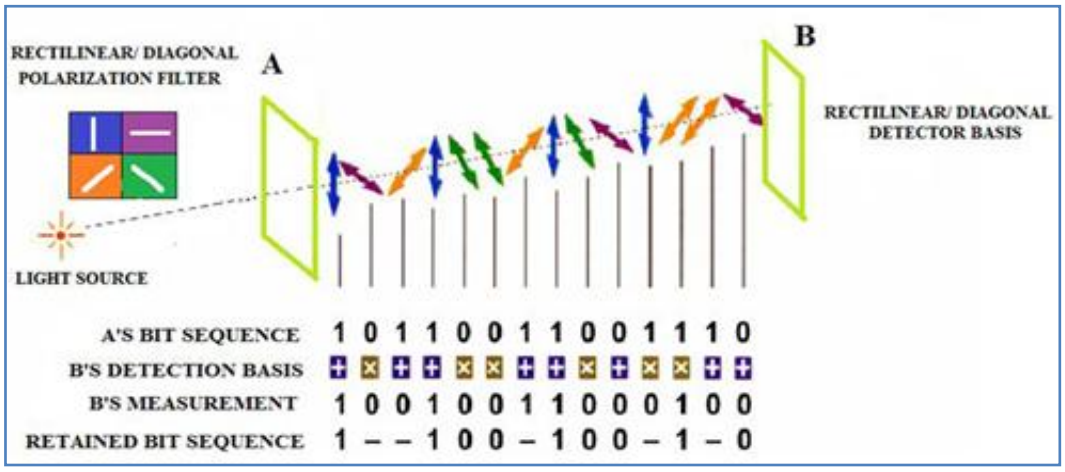


Fig.3. BB84 Protocol[10]

The following example data was generated assuming that Alice sends 12 photons and the detector never fails.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

Table1. Procedure of BB84 Protocol[11]

Step	Description	1	2	3	4	5	6	7	8	9	10	11	12
1	Filters used by Alice to prepare photons	+	+	x	+	x	x	x	+	+	+	x	x
2	Polarizations of photons sent by Alice	↕	↔	⤡	↔	⤢	⤡	⤢	↕	↔	↔	⤢	⤡
3a	Measurement types made by Bob	+	+	+	+	x	x	x	X	+	x	x	+
3b	Results of Bob's measurements	↕	↔	↔	↔	⤢	⤡	⤢	⤡	↔	⤡	⤢	↔
4	Bob publicly tells Alice which type of measurement he made on each photon	+	+	+	+	x	x	x	X	+	x	x	+
5	Alice publicly tells Bob which measurements were the correct type	yes	yes	no	yes	yes	Yes	yes	no	yes	no	yes	no
6	Alice and Bob each keep the data from correct measurements and convert to binary	1	0		0	1	0	1		0		1	
7	Security test		0			1				0		1	
8	Secret key	1			0		0	1					

The string of bits now owned by Alice and Bob is: 1 0 0 1 0 1 0 1. This string of bits forms the secret key. In practice, the number of photons sent and the resulting length of the string of bits would be much greater.

VI. CONCLUSION

The quantum cryptography is a new approach for security in communication. This technology is basically depends upon the polarization of photons, no cloning theorem and Heisenberg uncertainty principle. Quantum cryptography is an application of quantum physics. Other applications to cryptography are, it can be used to break the classical cryptographic protocol and cryptographic method can be applied to protect quantum information instead of classical information. This technology can detect the presence of eavesdropper in communication. There is no doubt that the technology can be mastered and will find commercial application in next few years.

REFERENCES

1. Xiaoqing Tan," Theory and Practice of Cryptography and Network Security Protocols and Technologies" in INTECH pp 111-146, 2013.
2. Wiesner, S. Conjugate coding, Sigact News, 15(1), pp. 78-88, 1983.
3. Mohamed Elboukhari, Mostafa Azizi and Abdelmalek Azizi," Quantum Key Distribution Protocols: A Survey", International Journal of Universal Computer Sciences, Vol.1, Iss.2, pp. 59-67,2010.
4. Charles H. Bennett and Gilles Brassard, "quantum cryptography: public key distribution and coin tossing" International Conference on Computer Systems and Signal Processing, Bangalore India, December 10-12 1984.
5. Dr. Janusz Kowalik, "Introduction to Quantum Cryptography", IEEE talk Seattle, February 9,2005.
6. White paper for "Quantum Safe Cryptography" ETSI V1.0.0 (2014-10)
7. Goronwy Tudor Jones," The uncertainty principle,virtual particles and real forces" Physics Education,IOP Publishing Ltd, May 2002, pp. 223-233.
8. Nicolas Gisin, Gre´ goire Ribordy, Wolfgang Tittel, and Hugo Zbinden, "Quantum Cryptography", REVIEWS OF MODERN PHYSICS, VOLUME 74, pp. 145-190, JANUARY 2002.
9. Samuel J. Lomonaco, Jr. "A Quick Glance at Quantum Cryptography" University of Maryland Baltimore County, pp.3-44 November 8, 1998.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2015

10. Sharvari Gogte, Trupti Nemade, Shweta Pawar, Prajakta Nalawade, "Simulation of Quantum Cryptography and use of DNA based algorithm for Secure Communication" IOSR Journal of Computer Engineering, Volume 11, Issue 2 (May. - Jun. 2013), PP 64-71.
11. Karen Hunter, "Quantum cryptography" SCI 510: Quantum Todd Duncan, 12 November,2002.

BIOGRAPHY

Miss. Leenata B. Isal is a scholar of M.E.(Computer Science and Engineering),at P.R. Patil College of Engg. and Technology, Amravati, SGBAU,India.

Prof. Chetan J. Shelke is Asst. Professor in P.R. Patil College of Engg. and Technology, Amravati, SGBAU,India.He received Master of Engineering (M.E.) degree in 2011 from Amravati University, MS, India. His research interest is networking.