© 2016 IJSRST | Volume 2 | Issue 3 | Print ISSN : 2395-6011 | Online ISSN : 2395-602X
Themed Section: Science and Technology

Quantum Key Distribution : A Comprehensive Study

Bhavesh Prajapati
Assistant Professor, IT Department, L.D.College of Engineering, Ahmedabad, Gujarat, India

ABSTRACT

Cryptography is age old technique used for secret communication of messages. Quantum cryptography is providing cryptographic solutions based on laws of quantum physics. Quantum public key distribution is prominent solution using which two parties can communicate securely using quantum physics. Heisenberg uncertainty principle, no cloning theorem and photon polarization are used as basic properties for quantum key distribution. Photons are basic quantum particles and they are quantized for encryption. They are also known as qubits. This paper discusses concepts behind quantum key distribution and how it is secure against eavesdropper and future advances in technology.

Keywords : Quantum Cryptography, Quantum Key Distribution, Entanglement, BB84 Protocol, No-Cloning Theorem

I. INTRODUCTION

Quantum key distribution is earliest discovery in the field of quantum cryptography which facilitates secret key distribution between Alice and Bob, two parties involved in communication. Quantum key distribution is often abbreviated as QKD. Quantum key distribution is based on principles of Quantum physics according to which presence of eavesdropper becomes visible as it generates disturbance in measurements. Based on the volume of disturbance measured Alice and Bob can decide that whether someone sniffing the information or not. If rate of disturbance is higher than predefined one then Alice and Bob discard the key and starts all over.

Stephen Wiesner first suggested quantum cryptography and idea then extended by Bennett and Brassard in 1984 in their proposed BB84 protocol. This protocol can be used for generation of secure cryptographic key which then can be used as one time pad in combination with classical cryptography.

II. CONCEPTS BEHIND QUANTUM CRYPTOGRAPHY

Quantum cryptography is applied branch of quantum information processing using laws of quantum physics and mathematical framework. The concepts behind quantum computing and cryptography are simple but counterintuitive to believe and understand.

Entanglement is the weirdest principle of quantum physics which plays important role in many quantum cryptographic applications. Entanglement is basic fundamental of Nature and its forms of energy and entropy. Einstein was very reluctant to believe the entanglement properties. He jointly published a paper with Podolsky and Rosen to demonstrate thought experiment which can prove quantum concepts wrong and infeasible.

Entanglement can be described as co relation between subatomic particles. In quantum computing we are using photons as micro particles and they are entangled with each other. More precise study of entanglement will give diverse research opportunities.

No-cloning theorem is published by Wootters, Dieks and Zurek which states that any arbitiary quantum state cannot be copied. This limitation is turned into biggest advantage by researchers to use in most of security protocols. If eavesdropper tries to intercept any information encoded using quantum techniques, it disturbs the quantum states and revels her existence.

Heisenberg's uncertainty principle is one of the fundamental concepts of quantum physics. As per the principle we cannot measure two properties of particle simultaneously like momentum and position. When we try to measure the property of photon, it will change it. Here photon particles are also remain in uncertainity and are in super position of two states. When we try to measure them they take any one position/state randomly. So when we actually try to measure the property of photon, we disturb its superposition state.

III. QUANTUM KEY DISTRIBUTION

Charles Bennett and Gilles Brassard have extended Wiesner's work and published quantum key distribution protocol in 1984. Quantum key distribution is becoming widely used tool by cryptographers. It provides secure key distribution over public non trusted channel.

Quantum key distribution also uses information reconciliation and privacy amplification to nullify the effects of noise and presence of eavesdropper. A flow chart describing the quantum key distribution procedure is given in Figure 1.

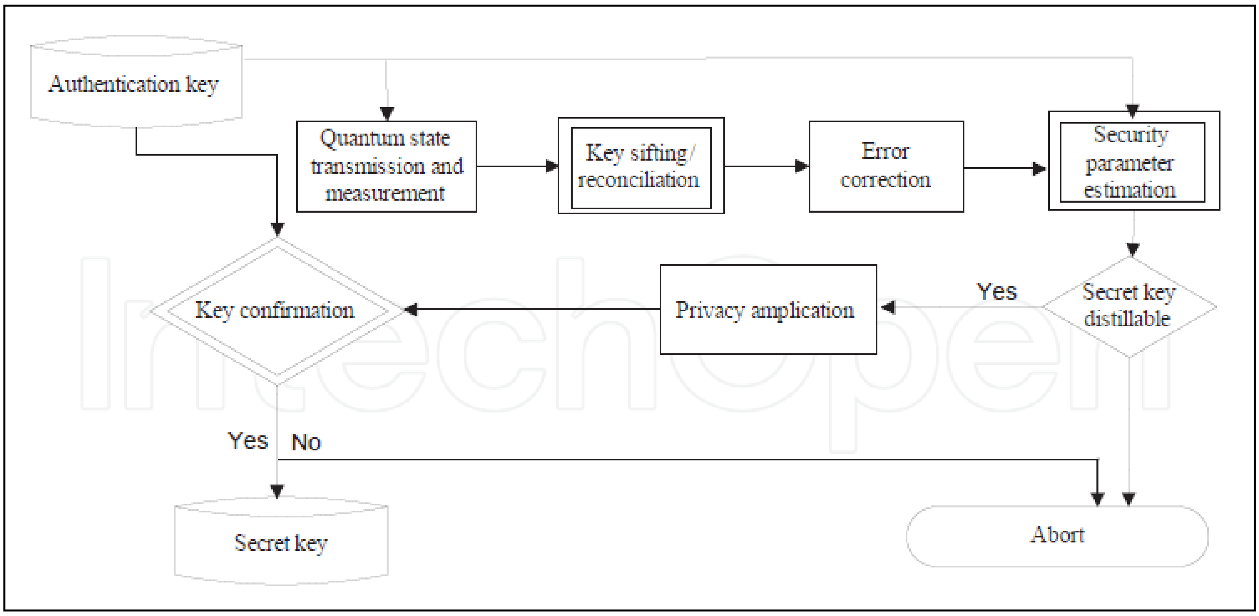


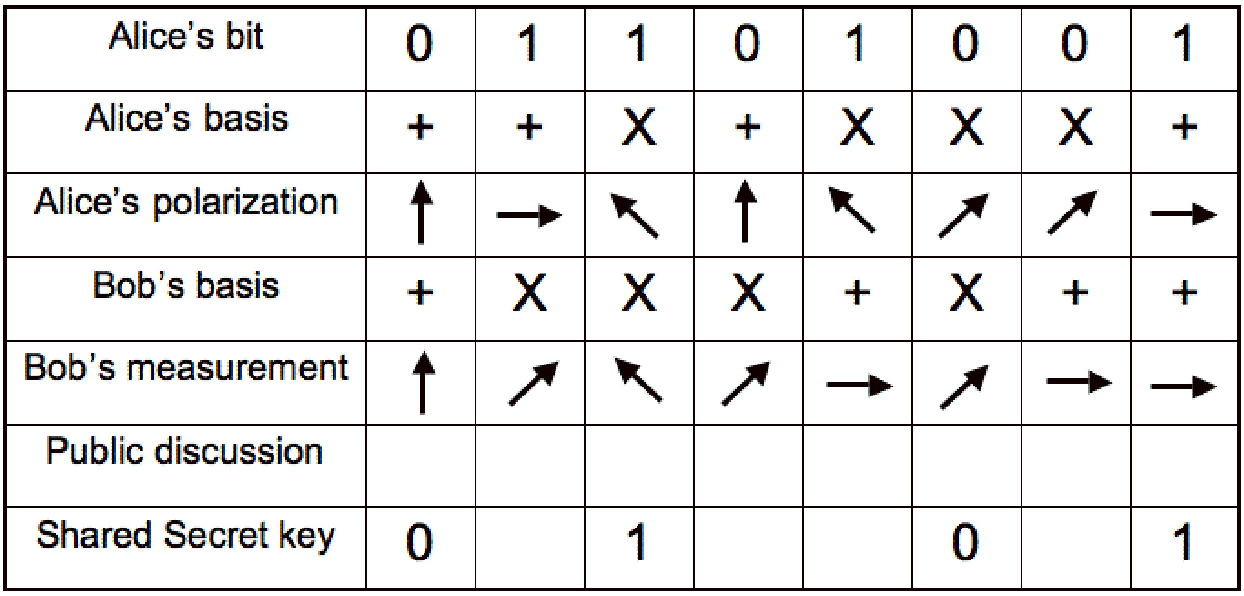
Figure 1. Flow chart of the stages of a quantum key distribution protocol. Stages with double lines require classical authentication.

Image Source: Xiaoqing Tan, Introduction to Quantum Cryptography, IntechOpen

In quantum key distribution procedure, two communicating parties Alice and Bob use quantum states also known as qubits. They both measure their qubits on different bases and decide how many of them can lead to establishment of secret key. Some of their measured bits may need to be discarded due to non matching of polarization angles. This process is called sifting. Later they perform error correction to find the presence of eavesdropper. If error is larger than predefined threshold then they discard the generated key and abort the procedure. If error rate is below the threshold then privacy amplification is performed to arrive at shared secret key.

IV. THE BB84 QUANTUM KEY DISTRIBUTION PROTOCOL

The foremost and most popular quantum key distribution protocol is BB84 (Bennett and Brassard, published in 1984) protocol. The procedure of the protocol is as follows and also given in Figure 2.



Alice's bit	0	1	1	0	1	0	0	1
Alice's basis	+	+	X	+	X	X	X	+
Alice's polarization	↑	→	↖	↑	↖	↗	↗	→
Bob's basis	+	X	X	X	+	X	+	+
Bob's measurement	↑	↗	↖	↗	→	↗	→	→
Public discussion								
Shared Secret key	0		1			0		1

Figure 2. Procedure of BB84 protocol
Image source: https://www.cse.wustl.edu/~jain/cse571-07/ftp/quantum/

- Alice sends stream of photon to Bob through insecure quantum channel. Both Alice and Bob chooses their polarization angles randomly from four polarization angles (Vertical, Horizontal, 45 degrees and 135 degrees).
- For each received photon, Bob chooses any one of two measurement bases, either diagonal or rectilinear to perform measurement.
- Bob keeps memory of his used bases and measurements. Bob publically acknowledges receipt of received signals.
- Alice and Bob both announce their bases used for measurement.
- Alice and Bob both discard all measurements where they have chosen different bases for measurements.
- To check for sniffing or tampering, Alice randomly chooses small fraction of remaining events known as test events. For these test events, Alice publically announces their position and polarization angles.
- Bob also announces polarization angles for test events.
- Alice and Bob compute the error rate. If error rate is higher than pre defined threshold value then they discard the key and abort the procedure. If error rate is less than threshold value then they proceed with next step.
- Alice and Bob convert the polarization data into binary data called a raw key. Once having raw key in binary format, than classical procedures

as error correction and privacy amplification are performed to generate a final key.

V. CONCLUSION

Quantum key distribution is a most popular tool among quantum cryptographers. Theory of Quantum key distribution is very mature but practical implementations of QKD still need to be fine tuned for cost effectiveness and efficiency. Real systems are full of noise and efficiency is always tested in actual environment. Many researchers are proposing many real life applications of quantum key distribution like quantum internet, quantum banking and finance, open space communication and many more. Quantum key distribution gives us a glimpse of secured future with help off quantum physics law and drastic changes in classical cryptographic structures.

VI. REFERENCES

[1]. Vittorio, S., 2002, "Quantum Cryptography: Privacy Through Uncertainty" http://www.csa.com/discoveryguides/crypt/overview.php

[2]. Id Quantique White Paper, 2005, "Understanding Quantum Cryptography" http://www.idquantique.com/products/files/vectis-understanding.pdf

[3]. Ford, J., 1996, "Quantum Cryptography Tutorial" http://www.cs.dartmouth.edu/~jford/crypto.html#1

[4]. Bennett, C.H., Brassard, G., 1984, "Quantum Cryptography: Public Key Distribution and Coin Tossing"

[5]. Bennett, C.H., 1992,"Quantum Cryptography: Uncertainty in the Service of Privacy"

[6]. Papanikolaou, N., 2004, "Techniques For Design And Validation Of Quantum Protocols"

[7]. Goldwater, S., 1996, "Quantum Cryptography and Privacy Amplification" http://www.ai.sri.com/~goldwate/quantum.html

[8]. Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., 2004 , "Quantum cryptography"

[9]. Fuchs, C. A., Gisin, N., Grıffiths, R. B., Niu, C. S., Peres, A. , 1997, "Optimal Eavesdropping In Quantum Cryptography. I. Information bound and optimal strategy"

[10]. Petra Pajic, 2013, "Quantum Cryptography"

[11]. D.J. Bernstein, 2009 Post-Quantum Cryptography, Springer

[12]. Bhavesh Prajapati, 2014, Quantum Cryptography: A comprehensive study, IJSRSET

[13]. Anand Sharma, S.K.Lenka, 2014, Authentication in Online Banking Systems: Quantum Cryptography Perspective, International Journal of Scientific & Engineering Research

[14]. Bhavesh Prajapati, 2015, 'A Brief Study of Quantum Cryptography Applications', International journal of scientific research in science and technology.

[15]. Xiaoqing Tan, Introduction to Quantum Cryptography, IntechOpen