International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 4 | ISSN : 2456-3307

Quantum Key Distribution Protocols : A Review

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

ABSTRACT

Quantum cryptography is constantly growing branch which is offering huge challenge to classical cryptography. Quantum key distribution often abbreviated as QKD is based on basic principles of quantum mechanics. Principles like Heisenberg's uncertainty principle, No-cloning theorem and Entanglement are underlying principles in key assumptions in quantum cryptography. Quantum key distribution is very popular application of quantum cryptography and many companies and government agencies are implementing it. Researchers across globe are suggesting more and more real life applications of quantum key distribution. Compare to classical key distribution, quantum key distribution is future proof and not constrained to advances in computing power. In this paper we are discussing different quantum key distribution protocols and work done by many research scholars.

Keywords : Quantum Key Distribution, BB84 Protocol, B92 Protocol, SARG04 Protocol

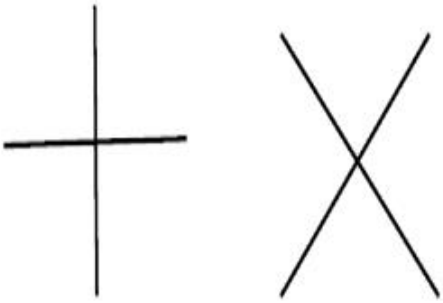
I. INTRODUCTION

Quantum cryptography is a prominent technology where two entities can communicate securely by implementing the sights of quantum physics. QPKD commences with the transmission of photons which are prepared in four quantum states randomly, relating to two mutually conjugate bases, rectilinear and diagonal. The rectilinear basis has two states i.e. polarizations namely 0° represented horizontally and 90°represented vertically. The diagonal basis 45° and 135° .The transmissions are secure as it is depended on the Inalienable quantum mechanics laws. The two predominant Constituents of quantum mechanics i.e. the principle of Heisenberg Uncertainty and the principle of photon polarization are the foundations of quantum cryptography. The **Heisenberg Uncertainty principle** defines that the observer simultaneously cannot measure two physical properties which are related with each other. In regard to this definition, the measurement of a photon cannot be done simultaneously in rectilinear basis and diagonal basis. If done, it randomizes the other. The principle of photon polarization defines that the replica of qubits cannot be made as per **Theorem of No-Cloning**. It was recognized that photons were used for transmitting the information instead of storing it which was the major revolution in the area of quantum cryptography.

A. Polarization of Photon

The photon is polarized in one of the bases to represent a bit known as a qubit. A 0° polarization of photon in the rectilinear basis or 45° in the diagonal basis is used to represent a binary 0.

A 90° polarization in the rectilinear basis or 135° in diagonal basis is used to represent a binary 1 as shown in figure:



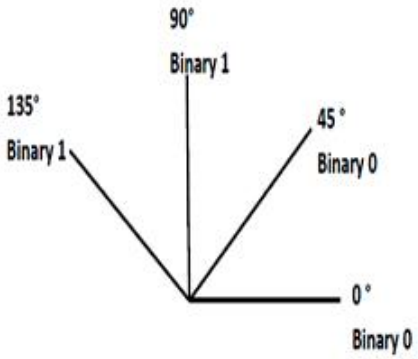


Figure 1. Rectilinear and Diagonal bases **Figure 2.** Polarization of photons to represent bits

B. Representing Information- Qubits and Quantum States

The underlying unit of quantum cryptography is qubit. It has two states, labeled as |0> and |1> (vertical bars | and angle brackets >) and referred as a state.

A bit can be in the state 0 or 1 whereas a qubit can occur in the state |0> and |1> .It can also occur in superposition state which is a linear combination of the states |0> and |1> .A state can be labeled as |ψ>. The state in superposition is noted as

$|\psi\rangle = \alpha\,|0\rangle + \beta\,|1\rangle$ where α, β are complex numbers.

Perhaps a qubit occurs in a superposition state |0> and |1>,but this state cannot be measured. Certainly, when a qubit is measured, it will occur in the state |0> or in the state |1>.The probability of obtaining the state |0>or |1> qubit is the modulus squared of α, β respectively according to quantum mechanics laws. That is to represent the probability of obtaining |ψ> in |0> state is $|\alpha|^2$ and the probability of obtaining |ψ> in |1>state is $|\beta|^2$. The probability of getting result of a measurement is obtained by squaring the coefficients. The condition is $|\alpha|^2 + |\beta|^2 = 1$.

II. QUANTUM KEY DISTRIBUTION PROTOCOLS

A. BB84 Protocol

Bennet and Brassard who had collaboration with Stephen Wiesner were proposed the first QPKD in 1984 and is familiarized as the BB84 protocol [12].

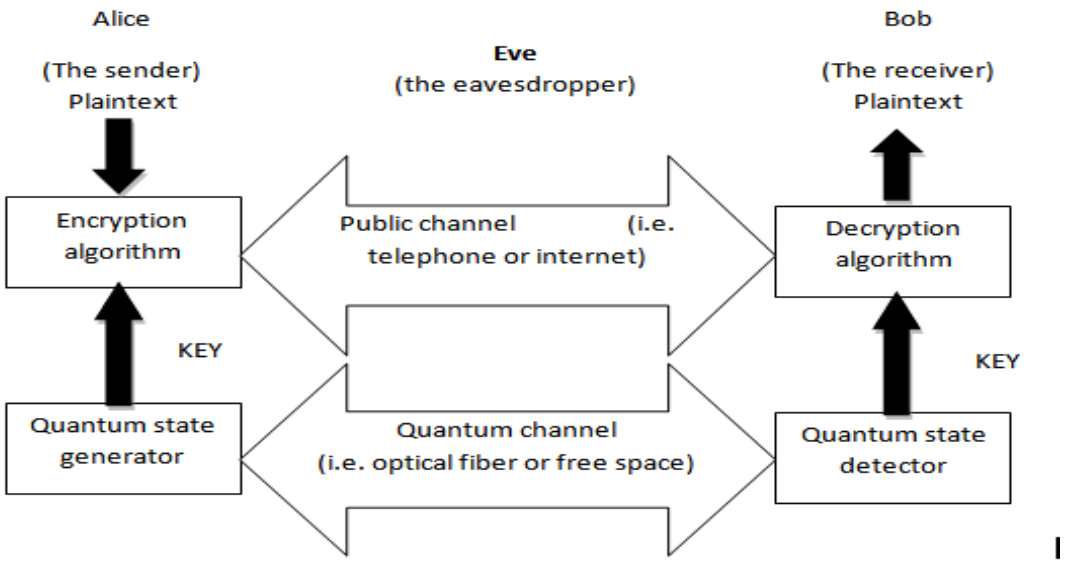


Figure 3. Quantum cryptographic communication System for securely transferring Random key

Bennet and Brassard proposed the quantum key distribution protocol for the first time in 1984 and familiarized as the BB84protocol depended on Heisenberg Uncertainty principle. The components of BB84 protocol are two bases that are to specify rectilinear (R) and diagonal (D) and four states of polarized photons. A 0° polarization of photon in the rectilinear basis or45° in the diagonal basis is used to represent a binary 0. A 90°polarization in the rectilinear basis or 135° in diagonal basis issued to represent a binary 1.

In QPKD, the communicating parties uses two communication channels namely a classical channel and a quantum channel. They transmit polarized single photons i.e. quits on the quantum channel and the conventional messages on classical channel. The following are the steps for secret key which is shared between two users.

a) The sender makes random bits in sequence manner and chooses random bases. He/she represents bits using polarized photons and sends the photons to receiver through the quantum channel.
b) The receiver measures each of them by choosing one of the two bases.
c) If the receiver selects the same basis as of sender's, then he/she will share the same binary information with sender, otherwise, with a different basis.
d) The receiver communicates this through the classical channel and sender tells receiver for which qubit he/she chose the same basis as he/she.
e) Both the parties will delete the bits which are of different bases and the other bits are the key known as sifted key.

B. B92 protocol

Soon after BB84 protocol was published, Charles Bennett realized that it was not necessary to use two orthogonal basis for encoding and decoding. It turns out that a single non-orthogonal basis can be used instead, without affecting the security of the protocol against eavesdropping. This idea is used in the BB92 protocol, which is otherwise identical to BB84 protocol.

The key difference in BB92 is that only two states are necessary rather than the possible 4 polarization states in BB84 protocol.[2].

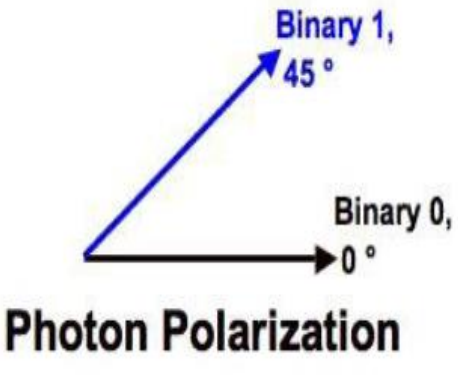


Figure 4. BB92 2-State Encoding

As shown in figure, can be encoded as 0 degrees in the rectilinear basis and 1 can be encoded by 45 degrees in the diagonal basis. Like the BB84 protocol, Client A transmit to Client B a string of photons encoded with randomly chosen bits but this time the bits Client A chooses dictates which bases Client B must use. Client B still randomly chooses a basis by which to measure but if he chooses the wrong basis, he will not measure anything; a condition in quantum mechanics which is known as an erasure. Client B can simply tell Client A after each bit Client B sends whether or not he measured it correctly.

C. SARG04 protocol

The SARG04 protocol is built when researcher noticed that by using the four states of BB84 with different information encoding they could develop a new protocol which would more robust when

attenuated laser pulses are used instead of single-photon sources. SARG04 protocol was proposed in 2004 by Scarani et.al [13].

The SARG04 protocol shares the exact same first phase as BB84. In the second Phase when Client A and Client B determine for which bits their bases matched, Client A does not directly announce her bases rather than Client A announces a pair of non-orthogonal states one of which she used to encode her bit. If Client B used the correct basis, he will measure the correct state. If he chose incorrectly he will not measure either Client A states and will not be able to determine the bit. If there are no errors, then the length of the key remaining after the sifting stage is ¼ of the raw key.

D. Steps of Quantum Key Distribution process

In order to generate final key that will be used in any encryption method, four steps are applied.
These steps are as follows :

Raw Key Extraction

This step deals with elimination of erroneous transmitted bits and it is carried over public channels like telephone, fax, e-mail etc. which are vulnerable to eavesdropping.

For BB84 protocol, at this step sending and receiving sides compare filter types which they used during sending/reading process for each photon. If they have used different types of filters for a photon's transmission then they eliminate the bit value corresponding to this photon. For BB84, sharing the type of filters used in reading/sending process over a public channel does not reveal any side's bit sequence. Because by using both filter types, polarized photons with any qubit value can be produced.

For B92 protocol, sending side does not reveal his/her used filter types because he/she can produce only two different types of polarized photon. Instead only receiving side announces indices of bits he/she read as "valid". Invalid bits are deleted from both side's bit sequences.

Error Estimation

If sides are using a QKD protocol over a noisy channel, this situation turns into an advantage for an eavesdropper. Because at any time slot, if both sides use same type of filter for sending/reading process and they do not have the same qubit value this can be due to not only existence of an eavesdropper but also physical noise of transmission medium. This situation prepares a suitable environment for attacks on QKD systems over physical channel's noise.

To avoid such attacks, both sides determine an error threshold value "Rmax" when they are sure that there is no eavesdropping on transmission medium. Then after each QKD session, they compare (sacrifice) some bits of their raw keys in order to calculate a transmission error percentage "R". By that way, for R >Rmax case they can be sure about existence of an eavesdropper.

III. RELATED WORK

Many researchers have contributed towards theatrical understanding of quantum key distribution protocols. Here Table 1 summarizes contribution of different researchers over the past years.

Table 1. Related work on QKD protocol

No	Paper Title	Summary
1.	Practical Challenges in quantum key distribution" by EleniDiamanti, Hoi-Kwong Lo, Nature Publications,2016	It Focuses on challenges on implementation of QKD protocols and its practical security. Also discusses major challenges in performance and cost.
2	Quantum cryptography and quantum key distribution Protocol: A Survey by V. Padmavati, B. Visnuvardan, A.V.N. Krishna, IEEE 6th International Conference, 2016	It explains basics of quantum cryptography, photon polarization, qubits and quantum states. Also discussed BB84, B92, Six state and SARG04 protocol. Real life examples of QKD networks are discussed.
3	Post quantum cryptography what advancements in quantum computing mean for IT professionalsby Logan O. Mailoux, IEEE 2016	Author has presented a readily understandable introduction and discussion of post-quantum cryptography, including quantum resistant algorithms and quantum key distribution.
4	QKDP's Comparison Based upon Quantum Cryptography Rulesby AbdulbastAbushgra, KhaledElleithy, IEEE, 2015	Detailed comparison of different QKD protocols are carried out on relevant parameters.
5	Quantum cryptography and its applications over the internet by Chi-Yuan Chen, Guo-jyunZeng, IEEE 2015	Author has introduced existing solutions and possible quantum cryptography applications which can be used in secret sharing, secure communication, cloud computing and e-commerce.
6	A Tutorial on Quantum Key Distributionby Baokang Zhao, Bo Liu, Ilsun You, IEEE 10th International Conference, 2015	This paper discusses BB84 protocol , the architecture of TOKYO QKD network and real life applications.
7	Quantum Cryptography: Pitfalls and Assets by Deepshikha Sharma, IJERSTE, 2014	Explained classical and quantum cryptography. BB84 protocol is discussed in details. Advantages and limitations of quantum cryptography is identified.
8	How secure is quantum cryptography by Renato Renner, Optical Society of America, 2013	Author demonstrated that practical quantum cryptographic schemes are vulnerable to hacking attacks. Discussed the source of this problem.
9	Key Distribution Protocol on Quantum Cryptography by Kondwani Makanda, Jun-cheolJeon, IEEE, 2013	BB84 protocol is explained in detail and compared with DH protocol.
10	Quantum cryptography and comparision of quantum key distribution protocols by Ergum Gumus, G.Zeynep, Journal of Electrical and Electronics engineering,2008.	This paper discusses basic terms of Quantum Cryptography. Also explains physics related to it. It discusses BB84 and B92 protocol in detail with simulation example.
11	The formal study of quantum cryptography protocols by Fan Yang, Yu-Jie, IEEE 2013	BB84 and B92 protocols are discussed. Both are analyzed using PRISM (Probabilistic symbolic model checker.)

IV. CONCLUSION

Today's classical world of cryptography and key distribution can be easily broken by Quantum computers. Quantum cryptography provides unconditional security and future proof also. Practical implementations of quantum key distribution have started overcoming the short falls. Many government agencies are keeping track of advances in quantum cryptography and decided to implement only those cryptographic applications which are future quantum safe. Quantum key distribution provides unconditionally secure authentication and secure cryptosystem.

V. REFERENCES

[1]. "Practical Challenges in quantum key distribution" by EleniDiamanti, Hoi-Kwong Lo, Nature Publications,2016

[2]. "Quantum cryptography and quantum key distribution Protocol: A Survey" by V. Padmavati, B. Visnuvardan, A.V.N. Krishna, IEEE 6th International Conference, 2016

[3]. "Post quantum cryptography what advancements in quantum computing mean for IT professionals" by Logan O. Mailoux, IEEE 2016

[4]. "QKDP's Comparison Based upon Quantum Cryptography Rules" by AbdulbastAbushgra, KhaledElleithy, IEEE, 2015

[5]. "Quantum cryptography and its applications over the internet" by Chi-Yuan Chen, Guo-jyunZeng, IEEE 2015

[6]. "A Tutorial on Quantum Key Distribution" by Baokang Zhao, Bo Liu, Ilsun You, IEEE 10th International Conference, 2015

[7]. "Quantum Cryptography: Pitfalls and Assets" by Deepshikha Sharma, IJERSTE, 2014

[8]. "How secure is quantum cryptography" by Renato Renner, Optical Society of America, 2013

[9]. "Key Distribution Protocol on Quantum Cryptography" by KondwaniMakanda, Jun-cheolJeon, IEEE, 2013

[10]. "Quantum cryptography and comparision of quantum key distribution protocols" by ErgumGumus, G.Zeynep, Journal of Electrical and Electronics engineering,2008.

[11]. "The formal study of quantum cryptography protocols" by Fan Yang, Yu-Jie, IEEE 2013

[12]. Bennett, C. H. & Brassard, G. Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing (ed. Goldwasser, S.) 175–179 (IEEE Press, 1984).

[13]. Scarani, A.Acin, Ribordy, G.Gisin.N."Quantum Cryptography protocols robust against Photon number Splitting attack." Physical Review Letters, vol.92.2004 http://www.qci.jst.go.jp/eqsi03/program/papers/O26-Scarani.pdf

[14]. Secure communication with a publicly known key.C. K. A. Beige, B.-G. Englert and H. Weinfurter. ActaPhysicaPolonica A, 101(3):357–368,2002.

[15]. Quantum cryptography: Public key distribution and coin tossing. C. H. Bennett and G. Brassard. Theoretical Computer Science, 560, Part1(0):7 – 11, 2014. Theoretical Aspects of Quantum Cryptography,celebrating 30 years of fBB84g.

[16]. Quantum digital signatures without quantum memory. V. Dunjko, P. Wallden, and E. Andersson. Phys. Rev. Lett., 112:040502, Jan 2014.

[17]. Quantum cryptography based on bell's theorem.A. Ekert. Phys. Rev.Lett., 67:661–663, Aug 1991.

[18]. Differential phase-shift quantum key distribution systems. K. Inoue. Selected Topics

in Quantum Electronics, IEEE Journal of, 21(3):1–7,May 2015.

[19]. Efficient quantum key distribution scheme and a proof of its unconditional security.H.-K. Lo, H. F. Chau, and M. Ardehali. J. Cryptol.,18(2):133–165, Apr. 2005.

[20]. Quantum cryptography protocols robust against photon number splitting attacks for weak laser pulse implementations V. Scarani, A. Acin, G. Ribordy, and N. Gisin..Phys. Rev. Lett., 92:057901, Feb 2004.

[21]. "Quantum Key Distribution Protocols: A Review," S. Reddy, Journal of Computational Information Systems, vol. 8, pp. 2839-2849, 2012.

[22]. M. M. Khan, M. Murphy, and A. Beige, New Journal of Physics,vol. 11, p. 063043, 2009.

[23]. "High error-rate quantum key distribution for long-distance communication," M. Elboukhari, M. Azizi, and A. Azizi, "Quantum key distribution protocols: A survey," International Journal of Universal ComputerSciences, vol. 1, pp. 59-67, 2010.

[24]. "Towards practical and fast quantum cryptography," N. Gisin, G. Ribordy, H. Zbinden, D. Stucki, N. Brunner, and V. Scarani, arXiv preprint quant-ph/0411022, 2004.

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

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

[27]. "Quantum Key Distribution : A Comprehensive Study", Bhavesh Prajapati, 2016, International Journal of Scientific Research in Science and Technology (IJSRST)