Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 6.017

IJCSMC, Vol. 6, Issue. 7, July 2017, pg.208 – 213

CENTRALIZED KEY DISTRIBUTION USING QUANTUM CRYPTOGRAPHY

Aparna Singh
Department of Computer Science & Engg., SRGI, India
aparnasingh2211@gmail.com

Abstract— The current data protection mechanism that typically comprises of cryptographic systems relies on the computational hardness as a means to protect sensitive data. With the recent advancements in quantum computing, quantum computers pose a serious challenge to such cryptographic systems. Interest in quantum cryptography has been stimulated by the fact that quantum algorithms like Shor's algorithm for integer factorization and discreet logarithms threatens the security of classical cryptosystems. Quantum Cryptography or Quantum Key distribution provides ultimate security assurance over a optical fiber communication link by resisting interception and retransmission by an eavesdropper between two communicating parties. Based on the foundations of quantum mechanics, the goal of quantum cryptography is to thwart attempts by third party to gain knowledge of the key. The third party trying to eavesdrop on the keys must in some way measure it and thus introducing detectable anomalies.
This paper focuses on quantum cryptography and how this technology can be used for secure key distribution in both centralized and decentralized network, along with its limitations.
Keywords— Quantum key distribution, decentralized network, centralized network, cryptography, symmetric encryption

I. INTRODUCTION

Quantum cryptography is the only approach to privacy ever proposed that allows two parties (who do not share a long secret key ahead of time) to communicate with perfect secrecy even in the presence of an eavesdropper. The security of quantum cryptography relies on the foundation of quantum mechanics and can detect eavesdropping by comparing bit by bit of a subset of the data communicated by the two parties.

Quantum cryptography is based on the fundamental principles of quantum mechanics, Heisenberg's Uncertainty Principle and principle of photon polarization. According to the Heisenberg Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at the point when it is measured. This ensures that the eavesdropper's activities must produce an irreversible change in the quantum states before they are transmitted to the intended recipient. Quantum cryptography has a quantum no-cloning theory. This theory shows that it is not possible to receive a single photon and duplicate the photon without giving the notice to others. Secondly, the photon polarization principle describes how light photons can be oriented or polarized in specific directions. Moreover, a photon filter with the correct polarization can only detect a polarized photon or else the photon will be destroyed. It is this "one-way-ness" of photons along with the Heisenberg Uncertainty principle that make quantum cryptography an attractive option for ensuring the privacy of data and defeating eavesdroppers.

Quantum Cryptography was proposed first by Stephen Wiesner in the early 1970s when he introduced the concept of quantum conjugate coding. His paper "Conjugate Coding" was rejected by IEEE Information Theory but was eventually published in 1983 in SIGACT News. Building upon this work Charles H. Bennett, of the IBM Thomas J. Watson Research Center, and Gilles Brassard, of the University of Montreal, elaborated a method for secure communication based on Wiesner's "conjugate observables". Bennet and Brassad stated that an encryption key could be created depending on the amount of photons reaching a recipient and how they were received. According to the protocols developed, the photons are polarized with various orientations and these orientations are used to represent bits (composing of 0s and 1s). The representation of bits through polarized photons is the foundation of quantum cryptography that serves as the underlying principle of quantum key distribution.

The remainder of this paper is organized as follows. In section 2, I describe the basis of cryptography & it's limitations to describe the motivation behind the development of Quantum key distribution. Section 3 covers the BB84 protocol in detail which also covers the immunity of quantum key distribution to eavesdropping. In section 4 I shall describe how QKD can be used for session key distribution in both centralized and decentralized network followed by section 5 that describes the challenges faced by QKD. Section 6 covers the advancements made in this field and finally in section 7 I shall represent the conclusion and the future scope.

II. CRYPTOGRAPHY

Cryptography is the art and science of developing cryptographic systems that are used to convert a plaintext message into a cipher text. Although confidentiality is the traditional application of cryptography, it is used nowadays to achieve broader objectives, such as authentication, digital signatures.

To achieve this goal the original message (plain text) is encoded into a coded message known as cipher text. This process of converting from plain text to cipher text is known as enciphering or encryption; restoring the plain text from cipher text is called deciphering or decryption. The central problem in cryptography is the key distribution problem, for which there are essentially two solutions: one based on mathematic laws and one based on physics (Quantum Cryptography). While classical cryptography relies on the computational difficulty of factoring large integers, quantum cryptography relies on the universal laws of quantum mechanics.

Symmetric encryption, also referred as conventional encryption or single key encryption, was the only type of encryption is use prior to the development of public-key encryption in the 1970.

A.Symmetric Encryption

1. Requires the use of single key for both encryption and decryption
2. The sender and the receiver must share the algorithm and the key
3. Requires secure communication channel for key distribution
4. The key must be kept secret

B.Asymmetric Encryption

1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption
2. The sender and receiver must each have one of the matched pair of keys.
3. One of the two keys must be kept secret

The security of public key cryptosystem is based on the computational complexity. The existence of secure asymmetric cryptosystem depends on the one way function. So far, no one has proved the existence of any one-way function with a trapdoor which poses a serious threat to these cryptosystems

III. BB84 PROTOCOL

BB84 (Bennett and Brassard, 1984) protocol is the first quantum protocol which is proposed by Charles Bennett and Gilles Brassard in 1984. The single photon may be polarized with four states: horizontal |h>, vertical |v>, left circle polarized |lcp> and right circle polarized |rcp>. BB84 use two pairs of states, with each pair conjugate two the other pair. Pairs of orthogonal states are referred to as basis. The usual polarization state pairs are the rectilinear basis (of 0˚ and 90˚) and diagonal basis (of 45˚ and 135˚).

Basis	0	1
+	↕	↔
×	⤢	⤡

Fig.1. States for polarization of a photon

The first state in BB84 is quantum transmission. To exchange secret keys between sender and receiver (Alice and Bob) we need two channels, quantum channel (allows quantum states to be transmitted) and a public, authenticated channel. Neither of

these channels needs to be secure. The security of the protocol comes from encoding the information in non orthogonal states. Quantum indeterminacy means that these states cannot in general be measured without disturbing the original state.

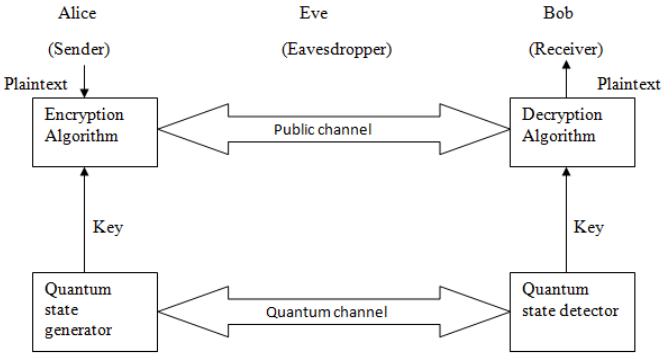

Fig. 2. Quantum Key Distribution using BB84 Protocol

Alice selects a random bit (0 or 1) and then selects one of her two basis (rectilinear or diagonal) to transmit it.

1. She then prepares a photon polarization state depending both on the bit value and the basis. For e.g. 0 in rectilinear basis is encoded as ↑. Alice sends the polarized photon to Bob via quantum channel. The process is repeated to form a random sequence of polarized photons all transmitted via quantum channel.
2. After transmission is completed Bob randomly chooses his detector, either rectilinear basis or diagonal basis. He does this for each photon he received, recording the result of each.
3. After measuring all the photons Bob communicates with Alice on the public channel, where they both share the correct basis of each photon (coming from Alice) and the basis each photon was measured in (coming from Bob)
4. They both discard photon measurement (bits) where Bob used different basis which is half on average, leaving half the bits as shared key.

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

Fig. 3. Transmission of quantum bits between Alice and Bob with the resultant key

QKD does not prevent us from eavesdropping but it enables users to discover it. To check the presence of an eavesdropper, Alice and Bob now compares a predetermined subset of their remaining bits. If a third party has gained any information about the photon's polarization, this introduces error in Bob's measurements. If more than p bits differ, they abort the key and try again.

IV. QKD IN DECENTRALIZED NETWORK

The strength of any cryptographic system depends on the key distribution technique, which refers to the delivery of the key to the two communicating parties who wish to communicate with each other, in a secure manner without allowing the access of the key to any third party.

A. Proposed Algorithm

In cryptography, a key distribution centre (KDC) is a part of cryptosystem intended to reduce the risk involved in key exchange. This scenario assumes that each user shares a master key with the KDC for the purpose of secure key distribution. If there are N users then there will be N master key. This master key can be acquired initially in any secure manner without being

compromised or by physically delivering them. Master keys between KDC and each user can also be generated using the quantum channel thus making them even more secure.

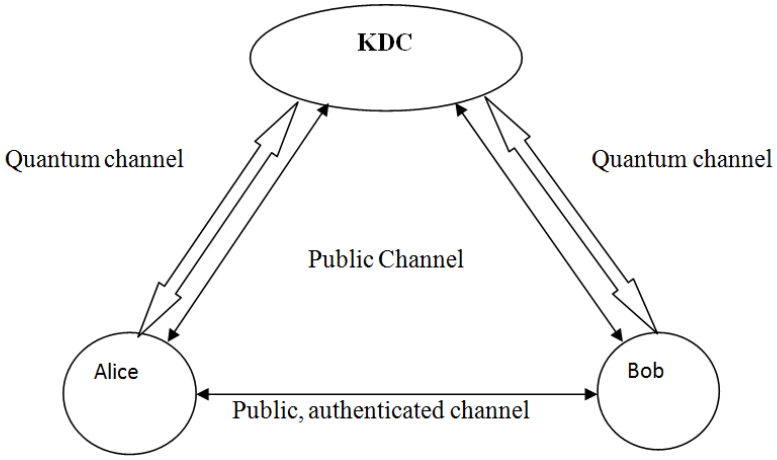

Fig. 4. Use of KDC to distribute session keys, in centralized network using quantum cryptosystem.

Keys can be distributed in the centralized network with the following sequence of steps:

1. Alice issues a request via the public, authenticated channel to the KDC for the session key to be able to communicate with Bob in a secure manner. The message includes the identity of Alice and Bob with a unique identifier N1 (nonce) for this transaction, which is encrypted by the master key shared between KDC and Alice, Ka. The nonce is used to identify each request uniquely.

   Alice→KDC
   E(Ka, (IDa ll IDb ll N1)) (via the public channel)
2. The KDC responds by initiating the process of key sharing between KDC and Alice via the quantum channel (same as BB84 protocol).

   KDC→Alice
   Ks (via the quantum channel)
3. Once the key is established between KDC and Alice, known as Ks, KDC sends a message to Alice via the public channel intended for Bob containing the session key Ks with the identity of A. These two items are encrypted with the master key shared between KDC and Bob, Kb.

   KDC→Alice
   E(Kb, (Ks ll IDa)) (via the public channel)
4. Alice stores Ks and forwards the message intended for B. Since the message is encrypted with Kb, only Bob will be able to decrypt the message and gain the key keeping it safe from any eavesdropper. Bob now knows the session key, knows that the other party is A because of the identifier and that the originator is KDC because of Kb.

   Alice→Bob
   E(Kb, (Ks ll IDa)) (via the public channel)

At this point both Alice and Bob have successfully shared a key that can be used for secure communication for an entire session. However, two more steps can be done that ensures the message received by Bob in step four was not a replay.

5. Using the newly formed session key, Bob sends a message to Alice containing a new nonce N2

   Bob→Alice
   E(Ks, N2) (via the public channel)

6. Also using Ks, Alice responds with f(N2) where f is a function that performs some transformation on N_2 .

   Alice→Bob
   E(Ks, f(N2)) (via the public channel)

B. Comparison with Decentralized Approach

A decentralized approach requires that the end systems be able to communicate with each other in a secure manner without the presence of any other authority or key distribution centre. For quantum key distribution decentralized approach is identical

to the working of BB84 protocol where two communicating parties (say, Alice and Bob) should share a quantum channel along with a public, authenticated channel to transfer quantum bits and the basis respectively.

7. A key can be established with the following sequence of steps:
8. Alice chooses a random series of bits and transmits each bit with a random base choice.
9. Bob detects each bit using another random choice of basis (rectilinear or diagonal).
10. Bob publically announces his detector basis, using the authenticated channel
11. Alice publically announces her choice of correct basis
12. They discard the bits received from different choices and use the remaining bits as key.

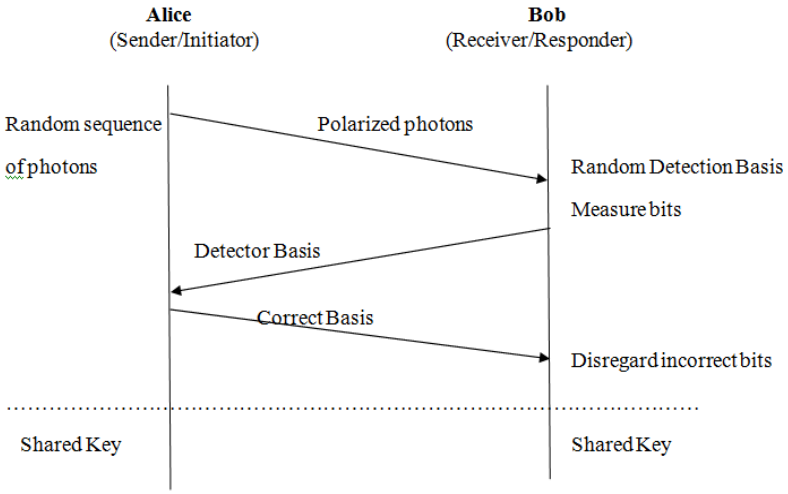

Fig.5. An example of decentralized key exchange between Alice and Bob by BB84 protocol

V. CHALLENGES FOR QUANTUM KEY DISTRIBUTION

1. The source should produce only one photon in response to a trigger pulse.
2. QKD is intrinsically point to point in nature, but has been demonstrated in a routed network topology over multi user optical fiber networks. These networks are currently being explored through research in optical fiber network.
3. The maximum distance over which quantum photon can travel is limited because of the absorption of the signal that occurs over long distance transmission in optical fiber. Due to the no cloning property of quantum information, repeaters cannot be used to transmit the quantum bits over the long distance. However intermediate nodes (quantum systems) can be incorporated to propagate the polarized sequence of photons over a longer distance.
4. QKD requires more cost for dedicated hardware. First generation QKD hardware is still being investigated for the security of their implementations. Attacks on QKD system rely on exploiting imperfections in the hardware to weaken the security.

VI. ADVACEMENTS MADE IN THE FIELD

Several QKD protocols have been successfully implemented in academic and commercial research labs, transmitting keys over long distances through either optical fibers or free space. QKD based on BB84 protocol has been demonstrated over distances over 100 km in length, reaching transmission speed on the order of one megabit per second over shorter distances. Researchers have developed a new method to overcome one of the main issues in implementing a QC system. By "seeding" one laser beam inside another, the researchers, from the University of Cambridge & Toshiba Research Europe, have demonstrated that it is possible to distribute encryption keys at rates between two and six order of magnitude higher than earlier attempts at a real world QC system.

The SARG protocol is similar to BB84 and has been used over a period of 21 months on the International Swiss Quantum network. Protocol that aim to enable long distance and high transmission rate QKD are the Differential- Phase Shift Protocol and the Coherent One-Way Protocol, which have exceeded 250 km transmission distance in optical fiber.

Most recently, votes casts in the Swiss canton of Geneva were protected for the first time by quantum cryptography.

VII.CONCLUSION

With rapid growth in the field of quantum computing and in the presence of quantum algorithms like Shor's algorithm or Grover's algorithm that can efficiently factor numbers and perform quick searches, there comes a threat to the existing cryptographic systems that base their security on the premises that certain computational problems are too difficult to solve. Without quantum safe encryption, everything that is being transmitted over a network is vulnerable to eavesdropping and public disclosure. Highly secure communication can be provided by using Quantum Channel to transmit symmetric keys. There are

number of commercial QKD systems available at present. These systems allow the distribution of symmetric keys to protect the sensitive information. Continued research will extend the range of these systems and will allow secure communication around the globe.

ACKNOWLEDGEMENT

Thanks to my guide Assistant Professor C.P.Singh and other faculty members of SRGI, Jhansi for providing resources and helping in the development of this project in all possible ways. I also thank readers of this journal for showing interest in this topic and contributing towards enhancement of this topic as well.

REFERENCES

[1] C. Bennett and G. Brassard, "*Quantum Cryptography: Public Key Distribution and Coin Tossing*," International Conference on Computers, Systems, and Signal Processing, Bangalore, India.1984.
[2] HASEGAWA Toshio, NISHIOKA Tsuyoshi, ISHIZUKA Hirokazu, NAMBU Yoshihiro, TOMITA Akihisa, and TAJIMA Akio, "*Secure Communication with Quantum Cryptography*", Journal of the National Institute of Information and Communications Technology Vol.53 No.3 2006.
[3] Elboukhari, Mostafa Azizi and Abdelmalek Azizi. "*Verification of Quantum Cryptography Protocols by model checking*," International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4.2010
[4] Wang Xiangbin, "*A fully efficient secure quantum cryptography protocol*", Imai Quantum Computation and Information project, ERATO, Japan Sci. and Tech. Corp. Daini Hongo White Bldg. 201, 5-28-3, Hongo, Bunkyo, Tokyo 113-0033, Japan
[5] Simon Gr¨oblacher, Thomas Jennewein, Alipasha Vaziri,3 Gregor Weihs, and Anton Zeilinger,2006. "*Experimental Quantum Cryptography with Qutrits*" arXiv:quant-ph/0511163v2
[6] Kenneth G. Paterson, Fred Piper and RÄudiger Schack, "*Quantum cryptography: a practical information security perspective*" Quantum Communication and Security, Proceedings, NATO Advanced Research Workshop, edited by M. Z_ ukowski, S. Kilin and J. Kowalik, p. 175{180 (IOS Press, Amsterdam, 2007)
[7] Ajit Singh and Nidhi Sharma, "*Quantum Key Distribution: A Secure Key Exchange Method in Quantum Cryptography*". Copy Right © INDIACom-2011 ISSN 0973-7529 ISBN 978-93-80544-00-7,2007.
[8] Valerio Scarani, Christian Kurtsiefer, 2012."The black paper of quantum cryptography: real implementation problems". arXiv:0906.4547v2 [quant-ph]
[9] Charles H. Bennett, "*Quantum Cryptography: Uncertainty in the service of privacy*"1992
[10] Gilles Brassard, "*Brief History of Quantum Cryptography: A personal perspective"*2005
[11] A. K. Ekert, "Quantum cryptography based on Bell's Theorem", Phys. Rev. Lett. 67, 661
[12] Richard J.Hughes, D.M. Alde, P.Dyer, G.G.Luther, G.L.Morgan and M. Schauer "*Quantum Cryptpgraphy*"1991
[13] Carl A.Miller and Yaoyum Shi,."*Robust Protocols for securely expanding randomness and distributing keys using untrusted quantum devices*"2016
[14] E. Messmer. "*Quantum Cryptography to secure ballots in Swiss election, Network world*" ,available online at http://www.networkworld.com/news/2007/101007-quantum-cryptographysecure- ballots.html
[15] "*Quantum Safe Cryptography and Security*". ISBN No. 979-10-92620-03-0, 2007, June 2015
[16] Nitin Jain,Elena Anisimova,Imran Khan,Vadim Makarov,Christoph Marquardt and Gerd Leuchs,."*Trojan-horse attacks threaten the security of practical quantum cryptography*" arXiv:1406.5813v1 [quant-ph], 2014
[17] Hartwig Mayer, "*Quantum Resistant Public Key Exchange – The Supersingular Isogenous Diffie-Hellman Protocol*" 2016
[18] S. Vittorio,. "*Quantum Cryptography: Privacy though Uncertainty*", CSA Discovery Guides, http://www.csa.com/discoveryguides/crypt/overview.php.2002

