International Journal of Enhanced Research in Science Technology & Engineering, ISSN: 2319-7463
Vol. 3 Issue 5, May-2014, pp: (27-30), Impact Factor: 1.252, Available online at: www.erpublications.com.

Quantum Cryptography: Pitfalls and Assets

Deepshikha Sharma
Research Scholar, The IIS University, Jaipur, India

Abstract: Secure transmission of messages has been a major goal since ages, for which cryptography is used. Cryptography is a mathematical techniques used for secure communication. Classical cryptography is traditional means that comprises mathematical functions to restrict eavesdropping problem in communication. Quantum cryptography is a new approach towards secure communication which uses phenomenon of quantum mechanics. It incorporates Heisenberg's uncertainty principle and principle of photon polarization concepts of quantum mechanics with cryptographic techniques This paper compares classical cryptography with quantum cryptography and outlines the advantages and major limitations or problems quantum cryptography is currently facing.

Keywords: Cryptographic system, key generation, quantum cryptography, quantum computers, BB84 protocol.

I. INTRODUCTION

Earlier or ancient civilizations used some form of cryptography to keep their messages secret. The ciphers used by these people were advanced at the time, but were undoubtedly not resilient [1]. A major breakthrough in cryptography is the introduction of Quantum Cryptography in 1970's by Stephen Wiesner. The development of quantum cryptography was motivated by the short-comings of classical cryptographic methods, which can be classified as either "public-key" or "secret-key" methods. This paper will first give a brief overview of classical cryptography and discuss the different kinds, then moves to quantum cryptography and finally go over the limitations of quantum cryptography [3]. Section II and section III describes the classical cryptography and quantum cryptography .Sections IV, V, talks about the advantages and limitations of quantum cryptography respectively. Section VI gives the conclusion of the paper which is followed by references in sections VII.

II. CLASSICAL CRYPTOGRAPHY

Cryptography, as derived from Greek kryptos, "secret" and graph, "writing", is the practice and study of hiding information .It means to keep the messages secret during transmission i.e., hiding of information from untrusted and unreliable elements. Cryptography is also defined as converting the original or plain text into encrypted or cipher text. The cipher text is produced with various cryptographic algorithms and keys. Keys used are secret and variable as without these the message could be decrypted by just knowing the algorithm used therefore useless. The cipher text is then sent across the transmission media and is deciphered or decrypted in its original form on the other side by the receiver. Mainly there are two main forms of cryptography: Symmetric and Public-key cryptography.

A. Symmetric-key cryptography

Symmetric key cryptography uses the same cryptographic algorithm and the same key to encipher and decipher messages. The key is chosen randomly from all possible keys. Examples of commonly used symmetric encryption algorithms are Data Encryption Standard (DES), 3 DES, Rivest Cipher (RC-4) and International Data Encryption Algorithm (IDEA).

B. Public-key (Asymmetric) cryptography

Asymmetric key cryptography uses two different but mathematically relayed keys for encryption and decryption process, one to encrypt and the other corresponding key for decryption. The key which is known publicly is called public key and the one which is kept private is called the private key. Examples of commonly used asymmetric encryption algorithms are RSA, Deffie-Hellman key exchange, ElGamal, Elliptic curve cryptography.

III. QUANTUM CRYPTOGRAPHY

Quantum cryptography is a new approach to cryptography where it uses quantum mechanics elements: Heisenberg's uncertainty principle and principle of photon polarization with cryptographic techniques for secure communication. It

enables two parties to produce shared random keys known only to them, which can then be used to encrypt and decrypt messages. It uses photons to transmit a key; once the key is transmitted the encryption and decryption can be done using the basic or classical cryptographic methods (algorithms).Heisenberg's uncertainty principle states that, it is impossible to measure the quantum state of any system without disturbing that system. In particular when measuring the polarization of a photon, the choice of what direction to measure affects all subsequent measurements. The principle of photon polarization states that an eavesdropper cannot copy unknown qubits i.e. unknown states due to no cloning property of photons [3].

Quantum cryptography can be used for the distribution of the secret key but for distribution of secret key we need to secure the key and for the different basis of photon polarization are used. A pair of polarization states used to describe photon polarization such as horizontal/vertical is referred to as basis.

1. "|" denotes a photon in vertically polarized state.
2. "." denotes a photon in horizontally polarized state.
3. "/" denotes a photon in a 45 degree polarized state.
4. "\" denotes a photon in a 135 degree polarized state.
5. "+" denotes the pair of states {|,.}, also called as the +- basis.
6. "X" denotes the pair of states {\,/}, also called as the x-basis.

In 1984, a protocol called BB84 was introduced by C.H. Bennett and G. Brassard, which was the first protocol for secret quantum key distribution. The steps of the protocol are as follows, let X be the sender, Y be the receiver and Z be the eavesdropper.

1. X creates a random bit (0 or 1) and then randomly selects one of her two basis to transmit.
2. X then prepares a photon polarization state depending both on the bit value and basis.
3. X then transmits a single photon in the state specified to Y, using the quantum channel.
4. This process is then repeated.
5. Y does not know the basis the photons were encoded in, so select a basis at random to measure.
6. After receiving all photons Y communicate X on public channel.
7. X broadcasts the basis each photon was sent in, and Y the basis each was measured in.
8. To check for the presence of eavesdropping X and Y now compare a certain subset of their remaining bit strings.
9. If a third party (Z) has gained any information about the photons' polarization, this will have introduced errors in Y's measurements.

X's random bit	0	1	1	0	1	0	0	1
X's random sending basis	+	+	x	+	x	x	x	+
Photon polarization X sends	↑	→	↘	↑	↘	↗	↗	→
Y's random measuring basis	+	x	x	x	+	x	+	+
Photon polarization Y measures	↑	↗	↘	↗	→	↗	→	→
Public Discussion Of Basis								
Shared secret key	0		1			0		1

Table1 : Sharing of secret key using BB84 protocol

Basis	0	1
+	↑	→
x	↗	↘

Table 2: Basis Format

IV. ADVANTAGES OF QUANTUM CRYPTOGRAPHY

The purpose of quantum cryptography is to propose a radically different foundation for cryptography, viz. the uncertainty principle of quantum physics. Quantum cryptography can achieve most of the benefits of public-key cryptography, with the additional advantage of being provably secure, even against an opponent with superior technology and unlimited computing power, barring fundamental violation of accepted physical laws [2].In conventional information theory and cryptography, digital communications can always be tracked and copied, even by someone who is unaware of their meaning. Such copies can be stored and can be used in future, such as decryption of the message encrypted with the same secret key. However, when elementary quantum systems, such as polarized photons, are used to transmit digital information, the uncertainty principle gives rise to novel cryptographic phenomenon, unachievable with traditional transmission media. This principle can be used to propose a communication channel whose transmissions cannot be read or copied an eavesdropper ignorant of certain key information used in forming the transmission. The eavesdropper cannot even gain partial information which is likely to be detected by the channel's legitimate users [2].

V. LIMITATIONS OF QUANTUM CRYPTOGRAPHY

There are some inherent problems with using quantum states to transmit information, some to do with quantum theory itself, and some practical ones regarding equipment efficiency which affects the security of protocols.

A. Point to Point links and Denial of Service

The quantum channel is a specialized piece of equipment, which by its very nature is a point-to-point connection: X and Y have to be at each end of it, with their photon sources and detectors. The point-to-point nature of QKD restricts potential growth, and gives rise to the possibility of a denial-of-service attack: if Z can't obtain key information, then cutting the physical link will mean X and Y can't either, which might serve Z's purposes just as well [6].

B. High Bit Errors Rate

The bit error rate of a quantum key distribution is several percentages higher than an optical communication system, which can be devastating in terms of practicality.There is an error control protocol called CASCADE that can correct the bit errors, but it also opens the system up to new attacks. The problem with CASCADE is there is a chance that a number of bits of the private key may be leaked to an attacker. One way to nullify these leaked bits is to use a process called privacy amplification. Privacy amplification takes the bit error corrected key and performs a compression function on it. This will guarantee that the bits leaked to an eavesdropper will become useless and that both parties will have the same key. This solves one problem but at the same time it weakens the security of the actual key because it is compressing the number of bits [1].

C. Losses in the Quantum Channel

Free space quantum channels also have atmospheric and equipment dependent geometric losses. Since quantum signals cannot be amplified, eventually the losses on the channel will be so high that readings obtained at detectors will be indistinguishable from dark count rates. Unfortunately, it is impossible to avoid lossy channels: they introduce security weaknesses [6].

D. Key Distribution Rate

The length of the quantum channel also has an effect on the achievable rate of key distribution. The rate at which key material can be sent decreases exponentially with respect to distance, and is regarded as another limiting factor in the usability of QKD systems [6].

E. Photon Sources and Detectors

The quality of photon sources and detectors can have a significant impact on the security of a protocol. An ideal photon detector should have the following properties,

- High efficiency over a large spectral range
- Low probability of generating noise (i.e. low dark count)
- The time between the detection of a photon and the corresponding electrical signal should be as constant as possible.
- The dead time after a detection event should be as small as possible to allow for higher data transfer rates.

The detection process isn't 100% accurate, due to imperfections in the detection material and this is always different in different detectors, so there will be a mismatch in the dead times of the rectilinear and diagonal basis measurements. Z can observe this, and can then work out the exact mismatch between the bases [6].

F. Sending one photon of light at a time

The only way the Heisenberg's uncertainty principle will combat eavesdropping is if only one copy of the photon is sent. In practice this is one challenge that has faced researchers [1].

G. Classical Authentication

Quantum cryptography does not provide digital signature and related features, such as certified mail or the ability to settle a dispute before the judge [1].

H. Distance Limitation

One of the challenges for the researchers is distance limitation. Currently, quantum key distribution distances are limited to tens of kilometers because of optical amplification destroys the qubit state [3].

VI. CONCLUSION

Quantum Cryptography provides a secure communication technique which relies on the quantum physics laws in contrast to the mathematically compute classical cryptography, but there are some limitations to it such as: point to point link & denial of service, losses in quantum channel, high bit error rate, low key distribution rate, photon detectors inaccuracy, sending of one single photon of light at a time, classical authentication and distance limitation which are described above are to be first removed or corrected for better network security. From this paper we come to know about the rough image of quantum cryptography, its applications and hindrances in implementing it in the present scenario. So, until and unless inherent limitations are overcome quantum cryptography cannot promise to revolutionize secure communication. In future we would like to develop a tool or simulator which could overcome the above limitations of quantum cryptography.

REFERENCES

[1]. A.Mahdy, D. Chait, "A Survey on Quantum and Classical Cryptography ", Available:http://www.csc.org/southcentral/E-Journal/2008/papers/p-0006.final.pdf[Accessed: September 2013]

[2]. C.H. Bennett, G. Brassard, "An Update on Quantum Cryptography", G.R.Balkely and D.Chaum (Eds):Advances in Cryptology- CRYPTO'84, LNCS 196,©Springer- Verlag Berlin Heidelberg , pp. 475-480,1985

[3]. R.K.Jain, K.Hiran,G.Paliwal, "Quantum Cryptography:A New Generation Of Information Security System", Proceedings of International Journal of Computers and Distributed Systems, ISSN:2278-5183, Vol.No. 2,Issue 1, pp. 42-45, December 2012.

[4]. C.H.Bennett, G.Brassard , "Quantum Cryptography: Public key distribution and Coin tossing", Proceedings of International Conference on Computer System & Signal Processing, Bangalore, India, pp.175-179, December 1984.

[5]. A.K.Lal, Dr.S.Sharma, "The New Approach of Quantum Cryptography in Network Security", International Journal Of Emerging Technology and Advance Engineering, ISSN: 2250-2459 (online), Vol.No.3, Special Issue 2, pp. 122-126, January 2013.

[6]. S. Cobourne, "Quantum Key Distribution Protocols and Applications", Technical Report RHUL-MA-2011-05 , Department of Mathematics, Royal Holloway, University of London Egham, Surrey TW20 0EX, England, Available: http://www.rhul.ac.uk/mathematics/techreports, 8 March 2011.