Quantum Cryptography: An Overview

A. G. Sharma
Department of Computer Science and Engineering
MGICOET, Shegaon
Maharashtra, India
ashwini.unnati@gmail.com

N. N. Kasliwal
Department of Computer Science and Engineering
MGICOET, Shegaon
Maharashtra, India
kasliwaln@gmail.com

***Abstract*—** in this generation of information technology, security plays the most vital role. Because most storage of confidential information, the need for a computer data security becomes increasingly important. Protect this Therefore, great care against both the two operating systems and user's information from unauthorized access. One such method of cryptography to protect sensitive data from being stolen or intercepted unwanted third parties. Traditional cryptology certainly clever, but like any encryption code-breaking story, and this is they abolished. Quantum mechanics is used in Quantum cryptography insures secure communications. This allows the two sides random bit sequence to produce a common, but they are known which can be used as a key to encrypt and decrypt messages. Utilizing the unpredictable nature of matter at the quantum physicists a way to exchange information secret keys. Putting information on the spin of photons in the core of Quantum Cryptology. Briefly, processes encoding (cryptography) and decoder (crypto analysis) of information or message (the so-called plain text) an otherwise unintelligible data (encrypted text) in combination with cryptology. And when the keys used for this process are photons, this is known as quantum cryptology.

Keywords- *cryptography, RSA, BB84, encryption, decryption.*

*****

I. INTRODUCTION

Classical cryptography is directly affected by these breakthroughs because it relies solely on the hardness of computing a mathematical problem that cannot be solved by current computers in polynomial time, but theoretically can be solved on a quantum computer. This realization is what spurred the research in quantum cryptography because quantum cryptography does not rely on computational security, but rather on the laws of quantum physics [4]. Cryptography means that we keep a message secret during transmission through untrusted and secure channel. Its simple means- encoding and decoding messages and has existed as long as people have distrusted each other and sought forms of secure communication. This encoding and decoding is perform by the some special key which is Secret key. The main concept of cryptography is to transmit information at the perfect node or actual receiving node. Originally the security of a cryptosystem or a cipher depended on the secrecy of the entire encrypting and decrypting procedures. In Cryptography cipher means that the encoded message or it is also called the encrypted message. In such ciphers a set of specific parameters, called a key, is supplied together with the plaintext or original text as and input to the encrypting algorithm, and together with the cryptogram as an input to the decrypting algorithm. This can be written as

Me (P) = C;

and conversely,

Mdk (C) = P;

Where P stands for plaintext, C for cryptotext or cryptogram, k for cryptographic key, and Me and Md denote an encrypted and decrypted messages respectively. It was shown, that as long as the key is truly random, has the same length as the message, and is never reused then the one-time pad is perfectly secure. So, if we have a truly unbreakable system.

What is wrong with classical cryptography?

In classical cryptography use the concept of key distribution. In this when the key is established, sub-sequent communication involves sending cryptograms over a channel. However in order to establish the key, two users, who share no secret information initially, must at a certain stage of communication use a reliable and very secure channel.[1]

In principle any classical key distribution can always be passively monitored, without the legitimate users being aware that any eavesdropping has taken place. In classical cryptography concept use the secret key encryption technique.

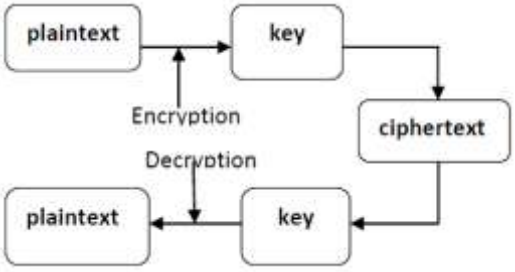

Fig: encryption concept [1]

The interesting solution for the concept of key distribution problem proposed by the Whitfield Diffie and Martin Hellman.

It involved two keys, one public key for encryption and one private key for decryption:

E (P) = C, and, D(C) = P

Key distribution problem method is that do not use the same key for encryption and decryption of the message. For encryption which is sender node side use the public key and receiver side use the private key for decrypt the message. Every user has his own two keys; the public key is publicly announced and the private key is kept secret. This concept is perform by using the RSA algorithm. Suppose that Alice wants to send an RSA encrypted message to Bob (Alice and Bob are two individuals who want to communicate secretly). This method is generally called the Public Key Cryptography. [1]

The RSA encryption scheme works as follows:

Encryption: Alice obtains Bob public key = (e; n) from some sort of yellow pages or an RSA public key directory. Alice then writes her message as a sequence of numbers.

Encryption: Alice obtains Bob public key = (e; n) from some sort of yellow pages or an RSA public key directory. Alice then writes her message as a sequence of numbers.

Decryption: Receiving the cryptogram C; Bob decrypts it by calculating

D(C) = C^dmod =P

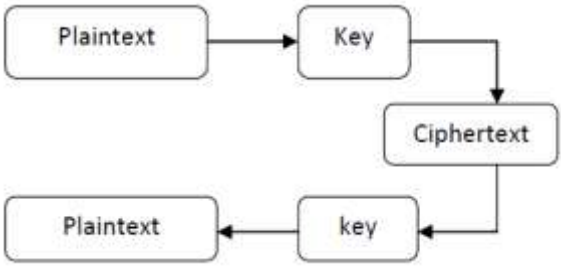

Fig: decryption concept [1]

II. EAVESDROPPING:

Eavesdropping is the act of an unintended receiver intercepting and reading a message between two communicating parties. Preventing eavesdropping is one of the main priorities of any key distribution system and quantum key distribution systems have an advantage [4]. Quantum theory has a principle called the Heisenberg uncertainty principle that guarantees any effort to monitor the communication will disturb it in some detectable way [4]. Although this does not prevent eavesdropping, it will allow the communicating parties to know if someone is eavesdropping. If someone is detected eavesdropping, the communicating parties can disregard the current key and not lose anything significant since it was a randomly generated key [5]

III. QUANTUM CRYPTOGRAPHY

It describes the use of quantum mechanical effects (in particular quantum communication and quantum computation) to perform cryptographic tasks or to break cryptographic systems [1].

The Well-known examples of quantum cryptography are the use of quantum communication to securely exchange a key (quantum key distribution) and the (hypothetical) use of quantum computers that would allow the breaking of various popular public-key encryption and signature schemes (e.g., RSA) [1].

The advantage of quantum cryptography lies in the fact that it allows the completion of various cryptographic tasks that are proven or conjectured to be impossible using only classical (i.e. non-quantum) communication.

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 [3]. 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 [3]. 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 [6].

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 [3]. Polarization such as horizontal/vertical is referred to as basis [3].

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. [3]

1. X creates a random bit (0 or 1) and then randomly selects one of her two basis to transmit.

 ISSN: 2321-8169
369 - 372

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. [3]

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 [3]

Basis	0	1
+	↑	→
x	↗	↘

Table 2: Basis Format [3]

Quantum cryptography can be used to distribute the secret digital keys important for protecting our personal data, such as bank statements, health records, and digital identity. Its security relies upon encoding each bit of the digital key upon a single photon (particle of light). If a hacker intercepts the single photons, they will unavoidably disturb their encoding in a way that can be detected. This allows eavesdropping on the network to be directly monitored. [2]

To perform quantum computations, one should have the following basic conditions:

(i) A two-level system (|0> and |1>) as a qubit
(ii) The ability to prepare the qubit in a given state, say |0>
(iii) The capability of measuring each qubit,
(iv) Construction of basic gate operations such as conditional logic gate (the control-not gate)
(v) Sufficient long DE coherence time. It is very important for a QC to be well isolated from any environmental interaction because they destroy the superposition of states. Furthermore, one has to use quantum error corrections, which have been invented in recent years [1].

IV. PROTOCOLS UTILIZING QUANTUM ENTANGLEMENT

Artur Eckert contributed a new approach to quantum key distribution where the key is distributed using quantum teleportation [Eckert91]. This section describes his protocol and its application to the protocols based on HUP described in the previous section.

A. **Eckert's Protocol** Eckert describes a channel where there is a single source that emits pairs of entangled particles, which could be polarized photons [Eckert91]. The particles are separated and Alice and Bob each receive one particle from each pair. Alice and Bob would each choose random bases on which to measure their received particles. As in BB84, they would discuss in the clear which bases they used for their measurements. For each measurement where Alice and Bob used the same bases, they should expect opposite results due to the principle of quantum entanglement as described earlier. This means that if Alice and Bob both interpret their measurements as bits as before, they each have a bit string which is the binary complement of the other. Either party could invert their key or they would thus share a secret key [2]. The presence of an eavesdropper can be detected by examining the photons for which Alice and Bob chose different bases for measurement. Alice and Bob can measure these photons in a third basis and discuss their results. [2]

With this information they can test Bell's Inequality which should not hold for entangled particles [7]. If the inequality does hold, it would indicate that the photons were not truly entangled and thus there may be an eavesdropper present [2].

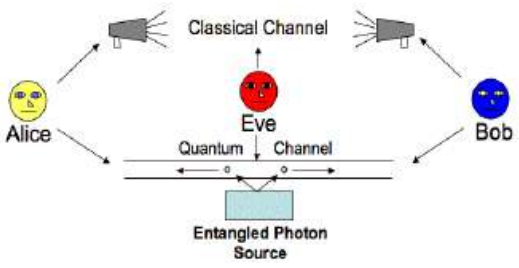

Figure: Entangled QKD Model [2]

Entangled BB84 Variants It is important to note the similarity between Eckert's protocol and BB84. If Alice was the source and Alice and Bob did not perform Eckert's entanglement check, we are essentially left with BB84. Bennet and Brassard [8] noted that any variant of BB84 could be adapted to use an entangled photon source instead of Alice being the source. In particular, Enzeretal 2002 [Enzer02] described an entangled version

of the SSP protocol with added security. Work has also been done that shows that the SARG04 protocol can tolerate fewer errors with a two-photon source (entangled) than a single-photon source (Alice) [9]. This section described the approach to QKD that utilized the principle of quantum entanglement

V. 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 [3]. 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 [10].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[3]. 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 [3]. 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 [10].

VI. Conclusion

From the survey we have studied that cryptographic no longer is dependent on the opponent computing resources, nor does it depend on mathematical advances. Quantum cryptography allows the exchange of encryption keys, the secret of which is future-proof and assured by the laws of quantum physics. Its combination with a conventional secret key encryption algorithms can increase the privacy of data transmissions to an unprecedented level. Quantum cryptography makes it possible to reach unprecedented levels of security provided by quantum physics for data transmission over optical networks.

REFERENCES

[1] International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459), An ISO 9001:2008 Certified Journal, Volume 3, Special Issue 2, January 2013) National conference on Machine Intelligence Research and Advancement (NCMIRA, 12), INDIA. Shri Mata Vaishno Devi University (SMVDU), Kakryal, Katra, INDIA. "The New Approach of Quantum Cryptography in Network Security."

[2] International Journal of Electronics and Computer Science engineering www.ijecse.org ISSN- 2277-1956 ISSN-2277-1956/V1N1-121-129 "Classical Cryptography v/s Quantum Cryptography A Comparative Study."

[3] 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, www.erpublications.com Quantum Cryptography: Pitfalls and Assets

[4] A SURVEY OF QUANTUM AND CLASSICAL CRYPTOGRAPHY Derrick Chait, Texas A&M University-Corpus Christi Faculty Advisor: Ahmed Mahdy, Texas A&M University-Corpus Christi

[5] Bennett, C. H., Quantum cryptography using any two non orthogonal states, Physical Review Letters, 68, (21), 3121–3124, 1992.

[6] [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.

[7] [Gisin02] Gisin, N., Ribordy, G., Tittel, W., Zbinden, H., "Quantum Cryptography", Reviews of Modern Physics, vol. 74, January 2002, pp. 146 - 195.http://www.gap-optique.unige.ch/Publications/Pdf/QC.pdf

[8] [BBM92] Bennet, C. H., Brassard, G., and Mermin, N., D., "Quantum cryptography without Bell's theorem.",

[9] Phys.Rev.Lett.68,1992,pp.557-559.http://prola.aps.org/pdf/PRL/v68/i5/p557_1

[10] [Fung06] Fung, C., Tamaki, K., Lo, H., "On the performance of two protocols: 10 SARG04 and BB84.", Phys.Rev.,A73,012337,2006.http://arxiv.org/pdf/quant-ph/0510025

[11] 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