International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 2, Issue 2, February 2013 ISSN 2319 - 4847

An Invention of Quantum Cryptography over the Classical Cryptography for Enhancing Security

Miss. Payal P. Wasankar[1], Prof. P. D. Soni[2]

[1]M.E. First year CSE
P R Patil COET, Amravati, India.

[2]P R Patil COET, Amravati, India

ABSTRACT

Quantum Cryptography is based on the use of subatomic particles (photons) and their intrinsic quantum properties (photon polarization) to develop an unbreakable system. It is not possible to measure the quantum state of any system without affecting the system. This property provides secure transmission of key between sender and receiver. Quantum Cryptography is a way to combine the relative ease and convenience of key exchange in public key cryptography with the ultimate security of a one-time pad. Quantum techniques for key distribution, the classically impossible task of distributing secret information over an insecure channel whose transmissions are subject to inspection by an eavesdropper, between parties who share no secret key initially. Quantum Cryptography uses the principles of Quantum Mechanics to implement a cryptographic system. The key problem which is solved by using quantum techniques is that of eavesdropping detection. The bits are represented as qubits, physically modeled by photons, and communicated over a quantum channel. The polarization states of photons represent 0's and 1's.

Keyword: Asymmetric key, Cryptography, Protocols, Quantum, symmetric key

1. INTRODUCTION

Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called adversaries). More generally, it is about constructing and analysing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation. Modern cryptography intersects the disciplines of mathematics, computer science, and electrical engineering. Applications of cryptography include ATM cards, computer passwords, and electronic commerce.

There are two branches of modern cryptographic techniques: public key encryption [2] and secret key encryption [1, 2]. In Public Key Cryptography, messages are exchanged using an encryption method so convoluted that even full disclosure of the scrambling operation provides no useful information for how it can be undone Each participant has a "public key" and a "private key"; the former is used by others to encrypt messages, and the latter is used by the participant to decrypt them.

Modern cryptosystem uses Quantum Cryptography that makes the key unconditionally secure with quantum mechanics. Quantum Cryptography is composed of two words: Quantum and Cryptography. Quantum is the smallest discrete quantity of some physical property that a system can possess and Cryptography enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. So, Quantum Cryptography is using the quantum for doing cryptographic tasks. Quantum Cryptography is based upon conventional cryptographic methods and extends these through the use of quantum effects. [3] Quantum Key Distribution (QKD) is used in quantum cryptography for generating a secret key shared between two parties using a quantum channel and an authenticated classical channel. The private key obtained then used to encrypt messages that are sent over an insecure classical channel (such as a conventional internet connection).

2. CLASSICAL CRYPTOGRAPHY TECHNIQUES

Cryptography is the process of transforming plain text or original information into an unintelligible form (cipher text) so that it may be sent over unsafe channels or communications. The transformer process is controlled by a data string (key). Anyone getting hold of the cipher text while it is on the unsafe channel would need to have the appropriate key

to be able to get to the original information. The authorized receiver is assumed to have that key. [4] Cryptography is study of methods of sending message in disguised form so that only the intended recipients can remove the disguised message. It is the art of converting message into different form, such that no one can read them without having access to 'key'. The message may be converted Using 'code' or a 'cipher'.
Cryptosystems come in two main classes:

2.1 Asymmetric Cryptography

In asymmetric cryptography the problem of key distribution is solved. It uses a pair of keys for encryption as shown in figure no. 1: a public key, which encrypts data, and a corresponding private, or secret key for decryption. You publish your public key to the world while keeping your private key secret. Anyone with a copy of your public key can then encrypt information that only you can read. [9]

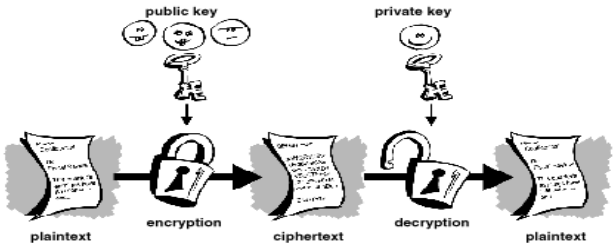

Figure1: Asymmetric Cryptography

2.2 Symmetric Cryptography

In symmetric cryptography, also called secret-key or symmetric-key encryption, [5] one key is used both for encryption and decryption. Figure 2 is an illustration of symmetric cryptography where plain text is encrypted and decrypted using same key (private key). This cryptography has disadvantage of private key distribution among sender and receiver.

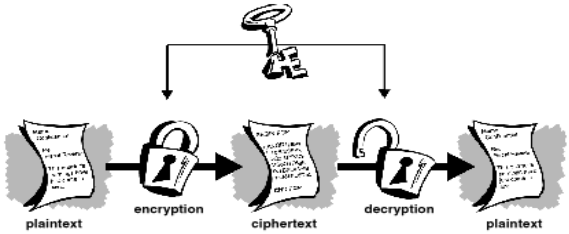

Figure 2: Symmetric Cryptography

Classical cryptographic systems are subject to a number of disadvantages and for that quantum cryptography is done:

3. QUANTUM CRYPTOGRAPHY

Quantum Cryptography is composed of two words: Quantum and Cryptography. Quantum is the smallest discrete quantity of some physical property that a system can possess and Cryptography enables to store sensitive information or transmit it across insecure networks so that it cannot be read by anyone except the intended recipient. So, Quantum Cryptography is using the quantum for doing cryptographic tasks. Quantum Cryptography is based upon conventional cryptographic methods and extends these through the use of quantum effects. [6] Quantum Key Distribution (QKD) is used in quantum cryptography for generating a secret key shared between two parties using a quantum channel and an authenticated classical channel as shown in Figure: 3 The private key obtained then used to encrypt messages that are sent over an insecure classical channel (such as a conventional internet connection). [10]
Modern cryptosystem uses Quantum Cryptography that makes the key unconditionally secure with quantum mechanics. For example: Heisenberg's Uncertainty Principle, Wave/Particle duality, Qubits and No cloning Theorem. Heisenberg's Uncertainty principle states that the more precisely one property is measured, the less precisely the other can be measured. [7] Using this principle Quantum Cryptography successfully provides unconditional security. [8] The concept of Wave/Particle Duality is being used in photon polarization. A qubit or quantum bit is a unit of quantum information. Like a bit a qubit can have values 0 or 1, a qubit can retain superposition state of these two bits. The no cloning theorem implies that a possible eavesdropper cannot intercept measure and reemit a photon without introducing a significant and detectable error in the reemitted signal. Thus, it is possible to build a system that allows two parties, the sender and the receiver, commonly called "Alice" and "Bob", to exchange information and detect where the communication channel has been tempered with.
The key obtained using quantum cryptography can then be used with any chosen encryption algorithm to encrypt (and decrypt) a message, which can be transmitted over a standard communication channel. Once the secret key using

Quantum Cryptography is established, it can be used together with classical cryptographic techniques such as the one-time-pad to allow the parties to communicate meaningful information in absolute secrecy.

In QKD, two parties, Alice and Bob, obtain some quantum states and measure them. A QKD system consists of a quantum channel and a classical channel. The quantum channel is only used to transmit Qubits (single photons) and must consist of a transparent optical path. The classical channel can be a conventional IP channel. The Key generation in QKD is done by communicating through quantum channels [3].They communicate through classical channel to determine which of their measurement results could lead to secret key bits. QKD [9] systems continually and randomly generate new private keys that both parties share automatically.

A compromised key in a QKD system can only decrypt a small amount of encoded information because the private key may be changed every second or even continuously. To build up a secret key from a stream of single photons, each photon is encoded with a bit value of 0 or 1, typically by a photon in some superposition state, such as polarization. These photons are emitted by a conventional laser as pulses of light so dim that most pulses do not emit a photon. This way of communication has the ability to create true random and secret key, which can then be used as seeds to conventional cryptographic methods for the generation of suitable keys.

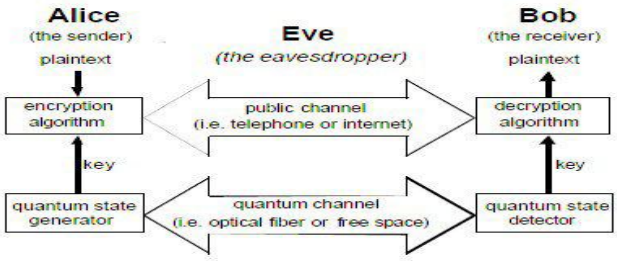

Figure 3: Quantum Cryptography

4. PROTOCOLS OF QUANTUM CRYPTOGRAPHY

A quantum (cryptographic) protocol is a data communications procedure which employ quantum phenomenon is designed to ensure secure communications. Quantum protocols such as BB84 were originally developed for the exchange of cryptographic keys only. If such a Cryptography that is perfect, such as one time pad, can be protocol is used to exchange cryptographic keys, the keys are guaranteed to be secure. A classical Cryptography that makes use of these keys can then be used to communicate data in secrecy. Indeed, a classical used once the keys have been exchanged. This means that probably unbreakable Cryptography is possible. The three main quantum cryptographic protocols proposed to date are as follows:

4.1 BB84 Protocol

BB84 is a quantum key distribution scheme developed by Charles Bennett and Gilles Brassard in 1984. It is the first quantum cryptography protocol. The protocol is provably secure, relying on the quantum property that information gain is only possible at the expense of disturbing the signal if the two states we are trying to distinguish are not orthogonal (see no cloning theorem). It is usually explained as a method of securely communicating a private key from one party to another for use in one-time pad encryption. [14]

4.2 E91 Protocol

The Ekert scheme uses entangled pairs of photons. These can be created by Alice, by Bob, or by some source separate from both of them, including eavesdropper Eve. The photons are distributed so that Alice and Bob each end up with one photon from each pair.

The scheme relies on two properties of entanglement. First, the entangled states are perfectly correlated in the sense that if Alice and Bob both measure whether their particles have vertical or horizontal polarizations, they will always get the same answer with 100% probability. The same is true if they both measure any other pair of complementary (orthogonal) polarizations. However, the particular results are completely random; it is impossible for Alice to predict if she (and thus Bob) will get vertical polarization or horizontal polarization.

Second, any attempt at eavesdropping by Eve will destroy these correlations in a way that Alice and Bob can detect.

4.3 BB92 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. The key difference in B92 is that only two states are necessary rather than the possible 4 polarization states in BB84. As shown in figure 3, 0 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, Alice transmits to Bob a string of photons encoded with randomly chosen bits but this time the bits Alice chooses dictates which bases she must use. Bob 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. Bob can simply tell Alice after each bit she sends whether or not he measured it correctly. [15]

5. CONCLUSION

Quantum cryptography promises to revolutionize secure communication by providing security based on the fundamental laws of physics, instead of the current state of mathematical algorithms or computing technology. The devices for implementing such methods exist and the performance of demonstration systems is being continuously improved. Within the next few years, if not months, such systems could start encrypting some of the most valuable secrets of government and industry.

REFERENCES

[1]Sheila Frankel and Ray Perlner "Quantum Key Distribution (QKD) and Commodity Security Protocols: Introduction and Integration" International Journal Network Security & Its Applications (IJNSA), Vol 1, No 2, July 2009.
[2] C. Elliott, D. Pearson, and G. Troxel, "Quantum cryptography in practice," Karlsruhe, Germany: Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications 2003.
[3] Alan Mink, dbart and S Wiesner, "Quantum cryptography or unforgeable subway tokens Advances in Cryptology" Proceedings of Crypto.August 1982
[4] Nelson, B., Phillips, A., Enfinger, F., and Steuart, C. Guide to Computer Forensics and Investigations.Boston:Thomson Course Technology, 2004.articles/cryptography/introduction-to-modern.
[5] Charles H. Bennett, "Quantum Cryptography Using Any Two Nonorthogonal States",IBM Rearch Division,T.J. Watson Research Center, Yorktown Heights,New York 10598
[6] Gerald Scharitzer, "Basic Quantum Cryptography" Vienna University of technology, Institute of Automation.
[7] Bennett C H G Brassard S Brei[1] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum key-distribution Protocols," Phys. Rev.vol. 73, 2006.
[8] Paul Busch, Teiko Heinonen, And Pekka Lahti, "Heisenberg's Uncertainty Principle", Physics Reports 452 (2007) 155-176.
[9] C. H. Bennett, F. Bessette, G. Brassard, L. Savail, and J. Smolin, "Experimental quantum cryptography" J. Cryptology 5, 1992
[10] Ajit Singh,Nidhi Sharma "Development of mechanism for enhancing data security in Quantum cryptography" Advanced Computing: An International Journal (ACIJ), Vol.2,No.3, May 2011.
[11] P. Shor, J. Priskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol", Physical Review Letters, Vol. 85, pp. 441 - 444, 2000.
[12]T.M.T. Nguyen, M. A. Sfaxi, and S. Ghernaouti-Hélie, "Integration of Quantum Cryptography in 802.11 Networks‖, Proceedings of the First Intenational Conference on Availability, Reliability and Security (ARES), pp. 116-123, Vienna, April 2006.
[13] Sheila Kinsella, Online Measurement of Entanglement of a Quantum State, National University of Ireland, Galway, Ireland, March 24th, 2006.
[14]Wikipedia,BB84, http://en.wikipedia.org/wiki/BB84
[15]Mart Haitjema, A Survey of the Prominent Quantum Key Distribution Protocols, http://www.cs.wustl.edu/~jain/cse571-07/ftp/quantum/index.html#b92

AUTHORS

Miss. Payal P. Wasankar is a scholar of ME, (Computer Science Engineering), at P R Patil COET, Amravati, under SGBAU, India.

Prof. P D Soni, Assistant Professor in Computer science department of P R Patil COET, Amravati, India. He has done his M.Tech. from Nagpur university, Nagpur, India.