

"Modernization of Cryptography : A Quantum Approach"

Associate Prof. and Hod. Neeraj Prakash Shrivastava, Sahil Bafna, Tapan Vijayvergiya

Department of CSE, Anand ICE, Jaipur-302012, Rajasthan, India;
Neeraj.shrivastava@anandice.ac.in, sahilbafna9@gmail.com, tapanvijay@outlook.com

Abstract – Secure transmission of message between the sender and receiver is done via cryptography. Traditional cryptographical methods use either public or private key encryption schemes.

In either case the eavesdroppers/attacker can detect the key and hence find the sent message without the awareness of the sender and receiver. Quantum cryptography, also called quantum encryption, applies principles of quantum mechanics to encrypt messages in such a way that it is can't be read by anyone outside of the predetermined recipient. It takes advantage of quantum's multiple states, coupled with its "no change theory," which means it can't be interfered unintentionally.

It uses the distribution of random binary key known as the Quantum Key Distribution (QKD) and hence enables the communicating parties to detect the presence of potential eavesdropper/attacker.

Keywords– Classical cryptography, Photon polarization, Quantum Cryptography, Qubit, Quantum entanglement, Quantum Key Distribution, Sifting key.

I. INTRODUCTION

In this increasingly sophisticated era majority of the governments, industry, Large businesses to Small businesses do the work using computers. The capabilities possessed by computer devices is no doubt faster than humans, this is proved by the level of accuracy to a high speed in completing a job. Besides the advantage obtained from the use of computer, the most important thing to be considered is part of its security which if the information/data stored in the computer suffered damage or loss then it could lead to huge losses. The condition of a computer that is not secured properly, will be a great opportunity to the hackers to enter the computer, access and steal all the data he wants. Some examples of hacking cases in 2016, among others are "Ransomware" emerges as a top cyber threat to business, UK second only to US in DDoS attacks, 412 million user accounts exposed in Friend Finder Networks hack, Financial Conduct Authority concerned about cyber security of banks, and other cases caused by the weakness of the security system. For that we need a computer security system. Security of data in a computer is very important to protect the data from other parties that do not have the authority to modify or access the data. Security issues relate to risk areas such as being dependent on the public internet, unsecure external data storage, lack of control and integration with multiple security schemes.

II. LITERATURE REVIEW

The NIST Computer Security Handbook [NIST95] defines the term computer security as follows: The

protection afforded to an automated information system in order to attain the applicable objectives of preserving the integrity, availability, and confidentiality of information system resources (includes hardware, software, firmware, information/data, and telecommunications) .

Cryptography lies at the intersection of science, maths and engineering and that studies about information security / data to avoid adverse effects due to misuse of information by irresponsible and malicious parties. Cryptography is an important factor in maintaining the confidentiality/security of information both in the computer and at the time of information transaction.

So, a more hard-headed goal of cryptography is to make it too work intensive for attacker. The basic terms used in cryptography are as follows:

1. Plaintext

In cryptography, plaintext is a simple readable text before being encrypted into ciphertext. The data or information can be read and understood without any special measure is called plaintext.

2. Ciphertext

In Cryptography, the transformation of original message into non-readable message before the transmission is known as ciphertext. It is a message obtained by some kind of encryption scheme on plain text.

3. Encryption

Encryption is a process that encodes a message or file so that it can be only be read by particular individual.

It is a process of encoding plain text into cipher text. Encryption process requires encryption algorithm and key

of some size to convert the plain text into cipher or scrambled text. It is performed at sender's end.

4. Decryption

Decryption is the reverse process of encryption. It converts the cipher text into plain text. In cryptography decryption performed at receiver end.

5. Key

The Key is called symmetric key as it is used by both sender and receiver to encrypt and decrypt the information. The key is the numeric or alphanumeric value used for the encryption of plain text and decryption of cipher or scrambled text.

Currently the scientists in the field of cryptography has been a lot of research about the science of cryptography by creating a variety of new algorithms developed from previous algorithms.

III. CLASSICAL BITS AND QUBITS

1. Classical Bits

The classical information is represented using binary/classical bits i.e. 0 and 1. Classical cryptography works on classical bits. Quantum cryptography works on quantum bits also called as qubits. A qubit can be in a superposition between zero and one. Qubits are different from classical bits for e.g. they cannot be copied. The information represented in both classical and quantum cryptography is different and that's the reason that the quantum cryptography needs to be approached differently from classical cryptography. Referring to the various sources of quantum cryptography as listed in references below, the next section is an attempt to provide essential knowledge of qubit.

2. Qubits

A qubit (or quantum bit) is the quantum mechanical analogue of a bit or classical bit. In classical computing the information is encoded in bits as 0 and 1. In quantum computing the information is represented in qubits. A qubit is a two-level quantum representation where the two basic qubit states are usually written as $|0\rangle$ and $|1\rangle$. A qubit can be in state

$|0\rangle$, $|1\rangle$ or (unlike a classical bit) in a linear combination of both states at the same time due to a phenomenon called superposition. The states or bits are represented in a Dirac Notation.

Superposition is the ability of a system to be in multiple states at the same time until it is measured by an observer.

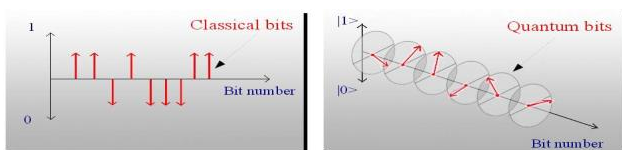


Fig.1. Information representation in Bits and QuBits.

IV. QUANTUM CRYPTOGRAPHY

Quantum cryptography solves the problems of private-key cryptography by providing the method for multiple users who may be in different regions to securely establish a secret or private key for communication and detect if eavesdropping has occurred. Quantum cryptography doesn't use hard mathematical problems for its security rather it accomplishes these remarkable results by exploiting the quantum properties of microscopic objects such as photons/neutrons/electrons. The photons have three chosen bases of polarization and the probable results of a analysis according to the bases are:

- Rectilinear (horizontal or vertical)
- Circular (left-circular or right-circular)
- Diagonal (45° or 135°).

1. Process of Quantum Coding

Many algorithms of encoding and decoding information using a given key have been created already, many years before practical quantum cryptography came into existence. Quantum cryptography isn't replacing existing cryptographic methods rather it is used for a more secure transfer of the secret-keys used in encryption and decryption. The maximum efficiency, speed, scalability and security of the transfer is achieved by transferring the secret key using quantum communication but encryption and transferring the data itself it done using traditional methods and algorithms of existing cryptographic methods.

2. Quantum Cryptography Model

In Quantum Key Distribution model, Alice is used to refer to as the sender, Bob as the receiver, and Eve as the eavesdropper. As Heisenberg Uncertainty Principle states that who was initially referring to the position and momentum of a particle, described how any conceivable measurement of a particle's position would disturb its conjugate property. Therefore, it is impossible to simultaneously know both the properties with certainty. Quantum cryptography can influence this principle but generally uses the polarization principal of photons on different bases as the conjugate property. The reason is that the photons can be exchanged over fibre optic links and it is the most practical quantum systems for communication between sender and receiver.

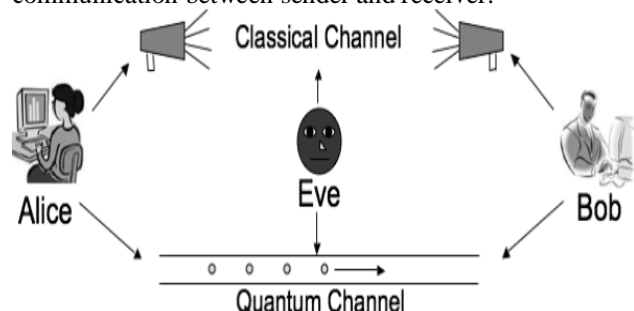


Fig.2. Cryptography communication model name.

3. Quantum key distribution-Key exchange methods

Consider a scenario in which the Alice and Bob communicates to agree on a key called a sifting key. This process is explained in two phases: -

Phase I: Sending

Alice determines the polarization (horizontal, vertical, left-circular or right-circular) of each burst of photons which she's going to send to Bob. A common key is agreed between the sender and the receiver and the aim is not to transfer a specific key.

Polarized photons are produced using a light source from a light-emitting diode (LED) or from a laser.

Phase II: Receiving and converting

Bob randomly generates a sequence of bases (rectilinear or circular) and measures the polarization of each photon.

Bob tells Alice which sequence of bases he used without worrying about other people hearing this information in the classical channel.

Alice publicly responds in the classical channel which bases were chosen correctly.

Alice and Bob discard all observations except the correctly chosen bases.

The remaining observations are converted on to binary code (left-circular or horizontal is 0, and right-circular or vertical is 1).

4. Alternative methods for Key Exchange

The information can be exchanged in several ways. The one-time pad method used is described as follows.

One-time pad method: -

The One Time Pad encryption method is a binary additive stream cipher, where a stream of truly random keys is generated and then combined with the plain text for encryption or with the ciphertext for decryption by an 'exclusive OR' (XOR) addition.

It is possible to prove that a stream cipher encryption scheme is unbreakable if the following preconditions are met: -

- The key must be in same a length as the plain text.
- The key must be non-deterministic and truly random.
- The key is one time use only.

5. Quantum entanglement

This process can be initiated by firing a laser through a crystal and splitting a single photon into two. If we modify the state of one photon's state, the other's state will change by itself no matter how far apart they are. This

was also termed as "Spooky action at a distance" by Albert Einsteinian. If one of the particles is measured according to the rectilinear basis and is in vertical polarization, then the other particle will be also in a vertical polarization if it is measured according to the rectilinear basis. If, the second particle is measured using circular basis, it may be found to have either left or right-circular polarization. This is extremely useful in detecting eavesdroppers.

6. Detecting eavesdropping

For eavesdrop detection; The photon polarization is measured. The concept behind detection is that the photon polarization can't be measured without destroying the polarization. So, if Eve eavesdrops and intercepts the signal then eve will have to send a new signal to the receiver so she may escape detection. However, eve will inevitably introduce errors in the signal, since eve doesn't know the state and polarization of the photon. Alice and Bob can publicly compare a randomly generated subset of the generate sequence to check for errors in the signal. If they get a higher error rate then feasible for communication then they can use a different channel for transmission as they can't stop from eve from listening in, they will know of here presence and then take proactive measures to safeguard the transmission.

V. LIMITATION

In case of entangled photons, which seems to be secure, there is also a practical problem not only with the cost, but also with keeping them entangled long enough to meet the needs of the real world, this issue is called decoherence. Another issue with the entangled photons is that for 50 kilometres or more distance, the noise or corruption of information becomes so great that error rates also increases drastically that the data is of no use for its applications. This makes the channel more unsecured for transmission and leaves it for no use as the channel is vulnerable to attacks and eavesdropping. However, in future, it might be possible for quantum keys to be exchanged wirelessly. Small telescopes may be set-up for signal detection. Some calculations suggest that photons could be detected by a satellite, which allows communication between any part of the

world. In fact, a wireless communication experiment via satellite was done by Chinese scientists in 2019 using QKD to transmit secure keys over communication mode.

VI. CONCLUSION

It is concluded that to transmit sensitive information between two or more points, some stronger technique is needed. It's evident that Quantum key distribution and other quantum encryption methods will allow us to secure sensitive information more effectively in the future. Quantum encryption methods are a powerful and right

step toward a future in which we won't be alarmed on what and how we share our information. We can also expect a sizable input from QKD into basic physics, which will give us a new perspective on the foundations of quantum mechanics that can be more "practical" than "philosophical. The paper briefs the reader on journey of cryptography from classical cryptography primitives to quantum cryptography. Then the difference between classical bits and qubits along with the representation is presented referring to the various sources in the references. Finally, Quantum Key Distribution methods are discussed.

REFERENCES

- [1]. Hiskett P, Hughes R, Lita E, Miller A, Nam S, Miller A, Nordholt J, Rosenberg D. Long-Distance Quantum Key Distribution in Optical Fibre., *New Journal of Physics*.2006.
- [2]. Wiesner S. Conjugate Coding, Written Circa 1970 and Belatedly Published in *Sigact News*. 1983; 15(1).
- [3]. Fernando GSL. Brandão and Jonathan Oppenheim, Quantum One-Time Pad in the Presence of an Eavesdropper, *Phys. Rev. Lett*. Jan 2012.
- [4]. Rishi Dutt Sharma. Quantum Cryptography: A New Approach to Information Security, *International Journal of Power System Operation and Energy Management (IJPSOEM)*. 2011; 1(1).
- [5]. Gottesman D. Chuang IL. Quantum Digital Signatures, *quant-ph/0105032*.
- [6]. Diffie Hellman. *New Directions in Cryptography*. IEEE Transactions on Information Theory. 1976; 22:644–54.
- [7]. Bennett CH, Brassard G, Crepeau C, Maurer UM. Generalized Privacy Amplification, *IEEE Transactions on Information Theory*. 1995; 41(6):1915–23.
- [8]. Sasirekha, N., And M. Hemalatha. "A Hybrid Indexed Table And Quasigroup Encryption Approach For Code Security Against Various Software Threats." *Journal of Theoretical & Applied Information Technology* 60.2 (2014).
- [9]. K. Ekert. Quantum Cryptography Based on Bell's Theorem. *Phys. Rev. Lett*. 67(6):661–663, 1991.
- [10]. Hughes, D. (2007, May). *Cyberspace Security via Quantum Encryption*. *Military Technology*,31(5), 84-87.
- [11]. Webb, W. (2006, July 20). Hack-proof design. (Cover story). *EDN*, 51(15), 4654.
- [12]. Anuja Priyam, "Extended Vigenère using double Transposition Cipher with One Time Pad Cipher", *Intl J Engg Sci Adv Research*; 1(2):62-65, ISSN No: 2395-0730, 2015.
- [13]. Borowski, M., Lesniewicz, M., "Modern usage of old one-time pad", *IEEE Conference :Communications and Information Systems*: 1-5, ISBN:978-1- 4673-1422-0, 2012.
- [14]. T. Gunasundari and K. Elangovan, "A Comparative Survey on Symmetric Key Encryption Algorithms," *International Journal of Computer Science and Mobile Applications*, ISSN no.2321-8363, 2014.
- [15]. William Stallings, "Cryptography and Network Security: Principles & Practices", Fifth edition, Prentice Hall, ISBN-13: 978-0136097044, 2010.
- [16]. M. Agrawal and P. Mishra, "A comparative survey on symmetric key encryption techniques," *International Journal on Computer Science and Engineering (IJCSE)*, vol. 4, pp. 877-882, 2012.
- [17]. "The-BB84-Quantum-Coding-Scheme", June2001. <http://www.cki.au.dk/experiment/qcrypto/doc/QuCrypt/bb84coding.html>
- [18]. "Quantum cryptography." Wikipedia, the free encyclopedia. http://en.wikipedia.org/wiki/Quantum_cryptography. Modified-17/September/ 2004.