International Journal of Application or Innovation in Engineering & Management (IJAIEM)
Web Site: www.ijaiem.org Email: editor@ijaiem.org, editorijaiem@gmail.com
Volume 3, Issue 2, February 2014 ISSN 2319 - 4847

Quantum Cryptography: Realizing next generation information security

Miss. Payal P. Kilor[1], Mr.Pravin.D.Soni[2]

[1]M.E. Ist year (CSE), P.R.Patil COET, Amravati,India.
[2]P.R.Patil COET, Amravati, India.

Abstract

Quantum cryptography is a technology that ensures ultimate security. Compared to current cryptography that could be defeated by by the development of an ultra high-speed computer, quantum cryptography ensures secure communication because it is based on the fundamental physical laws. It is an emerging technology in which two parties may simultaneously generate shared, secret cryptographic key material using the transmission of quantum states of light. Quantum cryptography is a new method for secret communications offering the ultimate security assurance of the inviolability of a Law of Nature. The quantum cryptography relies relies on two important elements of quantum mechanics-the Heisenberg Uncertainty principle and the principle of photon polarization. This research paper concentrates on the principle of quantum cryptography, and how this technology contributes to the network security. This paper outlines the real world application implementation of this technology and the future direction in which quantum cryptography accelerates.

Keywords: Quantum cryptography, network security, Quantum key distribution(QKD)

1. Introduction

In our modern age of telecommunications and the Internet, information has become a precious commodity. Sometimes it must therefore be keep safe from stealing - in this case, loss of private information to an eavesdropper. There are many features to security and many applications, ranging from secure commerce and payments to private communications and protecting passwords. One essential feature for secure communications is that of cryptography [1], which not only protects data from stealing or modification, but can also be used for user authentication. The main aim of cryptography is to protect data transffered in the likely presence of an enemies. A cryptographic transformation of data is a procedure by which plaintext data is encrypted, resulting in an modified text, called cipher text, that does not expose the original input. The cipher text can be reverse-altered by a designated recipient so that the original plaintext can be recaptured.The techniques of cryptography are usually categorised as traditional or modern. Traditional techniques use operations of coding i.e. use of alternative words or phrases, transposition i.e. reordering of plaintext, and substitution i.e.alteration of plaintext characters). Whereas, modern techniques use computers, and depends upon extremely long keys, convoluted algorithms, and intractable problems to achieve assurances of security. There are two main fields of modern cryptographic techniques: Public key encryption [2] and Secret key encryption [1],[2]. A public-key encryption, in which a message is encrypted with a recipient's public key. The message cannot be decrypted by anyone who does not possess the matching private key, who is thus presumed to be the owner of that key and the person associated with the public key. A secret key is an encryption key known only to the party or parties that exchange secret messages. The risk in this system is that if either party loses the key or it is stolen, the system is broken. The development of quantum cryptography was encouraged by the short-comings of classical cryptographic methods, which can be devided as either “public-key” or “secret-key” methods. Quantum cryptography is an approach to a cryptography based on the laws of quantum physics.

2. Literature review

Quantum cryptography was first recommended by Stephen Weisner in the early 1970s. The plan was issued in 1983 in Sigact News, and at the same time two scientists Bennet and Brassard, familiar with the idea of Weisner, were ready to issue their own ideas. Then in 1984, they delivered the first quantum cryptography protocol called the "BB84." The protocol is provably secure, depending 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. The first experimental prototype based on this was made in 1991. It functioned over a distance of 32 centimeters. Over time, the technology has been improved and the distance extended to kilometers. Later on in June 2004, The first computer network in which communication is secured with quantum cryptography is up and running in Cambridge, Massachusetts. The leader of the quantum engineering team at BBN Technologies in Cambridge, Chip Elliott, transmitted the first packets of data across the Quantum Net. After that, a team at the University of Vienna transffered entangled photons across the river Danube, through free space in June 2003. In April 2004, the first money transfer encrypted by quantum keys occurred between two Austrian banks. The two buildings were 500 meters away from each other, yet fibre optics were fed through 1.5 kilometers of sewage system to link them together.

3. Mechanics of Quantum Cryptography

The quantum cryptography depends on two important components of quantum mechanics-the Heisenberg Uncertainty principle and the principle of photon polarization [3]. The Heisenberg Uncertainty principle states that, it is impossible to determine the quantum state of any system without distributing that system. The theory of photon polarization states that, an eavesdropper cannot copy unknown qubits i.e. unknown quantum states, due to no-cloning theorem which was first introduced by Wootters and Zurek in 1982.

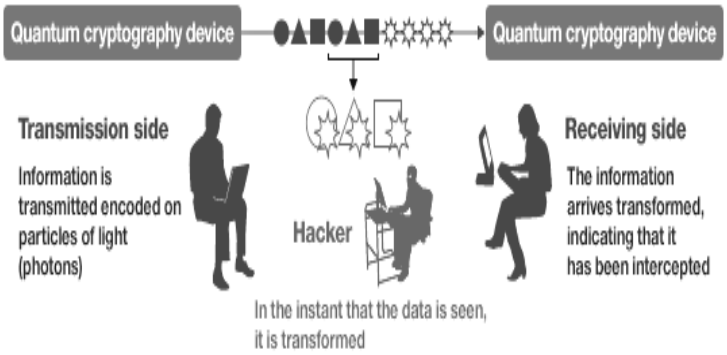

Figure 1: Mechanics of Quantum Cryptography

Depending on the theory of physics [4], quantum cryptography does not make it possible to eavesdrop on transmitted information. It is attracting considerable attention as a replacement for other contemporary cryptographic methods, which are based on computational security. Quantum cryptographic transmission encrypts the 0s and 1s of a digital signal on individual particles of light called photons. By contrast, modern optical transmission expresses the 0s and 1s of the digital signal as the strength and weakness of light respectively. Because the strong and weak light are made up of tens of thousands of photons which each convey the same information, if several photons are stolen (i.e., the signal is eavesdropped on) during transmission, it is not detected. On the other hand, in the case of quantum cryptography, if a third party detects (eavesdrops on) the signal, the information on the photons is suddenly transformed, meaning both that it is immediately noticable that eavesdropping has appeared and that the third party is not able to to decrypt the information.

4. Application of quantum cryptography

The most infamous and developed application of quantum cryptography is quantum key distribution (QKD). Quantum key distribution [6] is a method used in the framework of quantum cryptography in order to produce a perfectly random key which is shared by a sender and a receiver while making sure that nobody else has a chance to learn about the key, e.g. by capturing the communication channel used during the process. The best known and popular scheme of quantum key distribution is based on the Bennet–Brassard protocol(i.e. BB84), which was invented in 1984 [7]. It depends on the no-cloning theorem [7],[8] for non-orthogonal quantum states. Briefly, the Bennet–Brassard protocol works as follows:

- The sender (usually called Alice) sends out a series of single photons. For each photon, it arbitarily selects one of two possible base states, with one of them having the possible polarization directions up/down and left/right, and the other one polarization directions which are angled by 45°. In each case, the actual polarization direction is also arbitarly selects.
- The receiver (called Bob) detects the polarizations of the incoming photons, also randomly selecting the base states. This means that on average half of the photons will be determined with the “wrong” base states, i.e. with states not corresponding to those of the sender.
- Later, Alice and Bob use a public communication channel to talk about the states used for each photon (but not on the chosen polarization directions). In this way, they can find out which of the photons were by chance preserved with the same base states on both sides.
- Then they reject all photons with a “wrong” basis, and the others signify a sequence of bits which should be identical for Alice and Bob and should be known only to them, provided that the transmission has not been influenced by anybody. Whether or not this happened they can test by comparing some number of the obtained bits via the public information channel. If these bits agree, they know that the other ones are also correct and can finally be used for the actual data transmission.

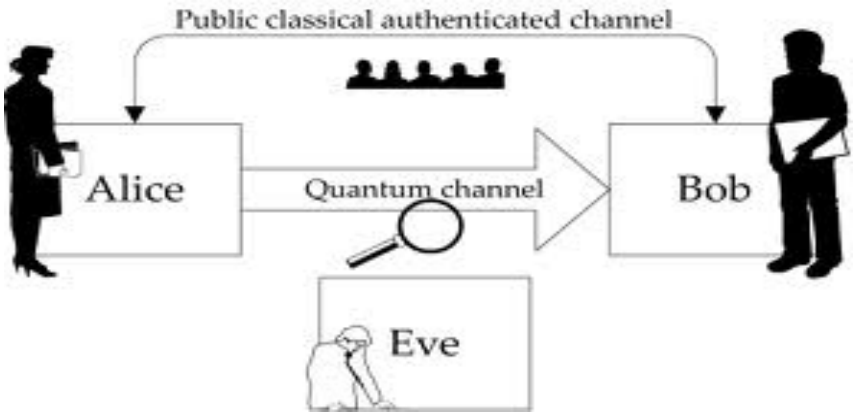

Figure 2: Quantum key distribution comprises a quantum channel and a public classical authenticated channel.

5. Future Direction

For now, non-quantum cryptography is very secure [10], because it depends on algorithms that can't be broken in less than the lifetime of the universe by all the currently existing computers. So in theory, there is not much demand for quantum cryptography yet; thus, we dont know when this technology will take a step forward and quantum cryptography techniques will become essential to protect our information. When quantum computers will come into play, the computational speeds will increase considerably, so the mathematical complexity of algorithms will become less of a challenge. It is still arguable [11] whether or not it will be possible to simply increase the numbers use in the algorithms and thus increase the complexity enough to outrun even quantum computer. Yet there is no question about the fact that quantum cryptography is a true invention in the field. It is still being refined and developed further. However, already it has been clear that even with its current defectiveness, it is many steps above everything that was settled before it. All we need is some years, or maybe decades or even centuries, to renew this method and make it feasible in the real world.

6. Conclusion

We presented an aspect of the workings of quantum cryptography and quantum key distribution technology. This technology is basically depends upon the polarization of photons, which is not a well regulated quantity over long distances and in multi-channel networks. Quantum cryptography could be the first attention of quantum mechanics at the single quanta level. Quantum cryptography promises to reform secure communication by providing security based on the elementary 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, such systems could start encrypting some of the most valuable and important secrets of government and industry.

References

[1] C.-H. F. Fung, K. Tamaki, and H.-K. Lo, "Performance of two quantum key- distribution Protocols," Phys. Rev. Avol. 73, 2006.
[2] Simmon, G. J. ,“Symmetric and asymmetric encryption”, ACM Computing Surveys, 11(4), 1979, pp. 305-330.
[3] Bennett, C. H., Brassard, G., and Ekert, A. K.Quantum cryptography. Sci. Am. 267, 4 (Oct.1992), pp. 50.
[4] C. Elliott, D. Pearson and G. Troxel, “Quantum Cryptography in Practice”, Preprint of SIGCOMM 2003 paper
[5] D.R. Stinson, Cryptography, Theory and Practice, CRC Press, Inc., Boca Raton, p. 4(1995).
[6] Mehrdad S. Sharbaf, “Quantum Cryptography: A New Generation of Information Technology Security System”. 2009, pp. 1644-1648..
[7] C. H. Bennett and G. Brassard, “QuantumCryptography: Public Key Distribution and Coin Tossing”,In Proceedings of IEEE International Conference onComputers Systems and Signal Processing, Bangalore,India, pp. 175-179, December 1984. (Bennet–Brassard protocol)
[8] W. K. Wooters and W. H. Zurek, “A single quantum cannot be cloned”, Nature 299, 802 (1982) (no-cloning theorem)
[9] N. J. Cerf and J. Fiurasek, “Optical quantum cloning – a review”, Prog. Opt. 49, 455 (2006).
[10] Young, A., “The future of cryptography: Practice and theory”, IEEE IT Professional Journal, 2003, pp. 62-64.
[11] Vishnu Teja, Payel Banerjee, N. N. Sharma and R. K. Mittal, “Quantum Cryptography: State-of-Art,Challenges and Future Perspectives”. 7th IEEE International Conference on Nanotechnology, 2007, pp. 1296-1301.

Author

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

Prof.Pravin D.Soni is Asst Professor in P.R.Patil College of Engg. He did his M.Tech at VJTI,Mumbai.