Secure Data Communication Using Quantum Cryptography

Yogendra Kumar[a] , Madan Pal[b]
[a]Deptt. of Physics, V.S.P. Govt. (P.G.) College, Kairana, Shamli (U.P.) India
[b]Deptt. of Mathematics, V.S.P. Govt. (P.G.) College, Kairana, Shamli (U.P.) India
Corresponding Author: Yogendra Kumar

Abstract

Quantum Cryptography is an emerging field to securing data communications by applying the phenomena of quantum physics. Unlike traditional classical cryptography, which uses mathematical techniques to restrict eavesdroppers, quantum cryptography is focused on the physics of information. Quantum cryptography provides secure data communication, whose security depends only on the validity of quantum theory, *i.e.*, it is guaranteed directly by the laws of physics. Most cryptographic mechanisms such as symmetric and asymmetric cryptography, often involve the use of cryptographic keys. However, all cryptographic techniques will be ineffective if the key distribution mechanism is weak. Quantum Key Distribution or Quantum Cryptography is attracting much attention as a solution of the problem of Key Distribution; QKD offers unconditionally secure communication based on quantum mechanics. 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, Quantum Key Distribution, QKD, BB84, Qubits.

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. While the modern cryptosystems are said to be very effective in other words they are said to be “INTRACTABLE” then why a lot of money is been spent to develop a new cryptosystem – quantum cryptography ? 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 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.

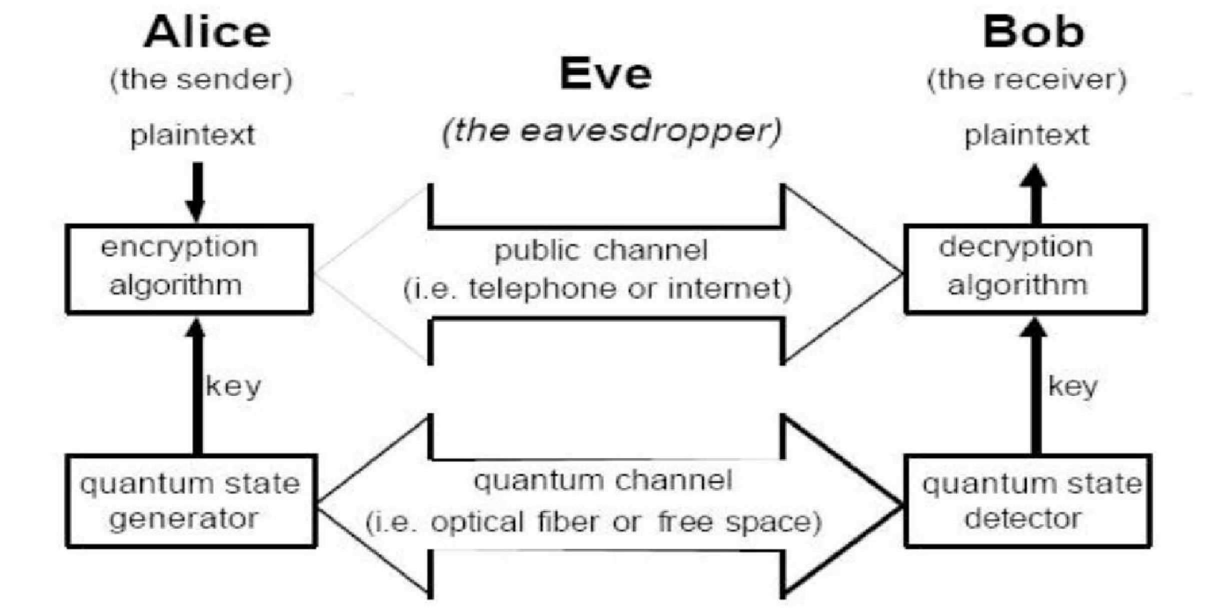

Figure . Quantum Key Distribution

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 . 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. Depending on the theory of physics , 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.

Rather than depending on the complexity of factoring large numbers, quantum cryptography is based on the fundamental and unchanging principles of quantum mechanics. In fact, quantum cryptography rests on two pillars of 20th century quantum mechanics –the Heisenberg Uncertainty principle and the Uncertainty principle, it is not possible to measure the quantum state of any system without disturbing that system. Thus, the polarization of a photon or light particle can only be known at the
point when it is measured. This principle plays a critical role in thwarting the attempts of eavesdroppers in a cryptosystem based on quantum cryptography. Secondly, the photon polarization
principle describes how light photons can be oriented or polarized in specific directions. Moreover, a photon filter with the correct polarization can only detect a polarized photon or else the photon
will be destroyed. It is this "one-way-ness" of photons along with the Heisenberg Uncertainty principle that make quantum cryptography an attractive option for ensuring the privacy of data and defeating eavesdroppers. Charles H. Bennet and Gilles Brassard developed the concept of quantum cryptography in 1984 as part of a study between physics and information. Bennet and Brassad stated that an encryption key could be created depending on the amount of photons reaching a recipient and how they were received. Their belief corresponds to the fact that light can behave with the characteristics of particles in addition to light waves. These photons can be polarized at various orientations, and these orientations can be used to represent bits encompassing ones and zeros. These bits can be used as a reliable method of forming onetime pads and support systems like PKI by delivering keys in a secure fashion. The representation of bits through polarized photons is the foundation of quantum cryptography that serves as the underlying principle of quantum key distribution. Thus, while the strength of modern digital cryptography is dependent on the computational difficulty of factoring large numbers, quantum cryptography is completely dependent on the rules of physics and is also independent of the processing power of current computing systems. Since the principle of physics will always hold true, quantum cryptography provides an answer to the uncertainty problem that current cryptography suffers from; it is no longer necessary to make assumptions about the computing power of malicious attackers or the development of a theorem to quickly solve the large integer Factorization problem.

Discussion and 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.

Quantum cryptography is still in its infancy and so far looks very promising. This technology has the potential to make a valuable contribution to e-commerce and business security, personal security, and security among government organizations. If quantum cryptography turns out to eventually meet even some of its expectations, it will have a profound and revolutionary affect on all of our lives.

REFERENCES

[1] C. Bennett and G. Brassard, “Quantum Cryptography:Public Key Distribution and Coin Tossing,” International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 1984.

[2] A. Ekert, “Quantum Cryptography Based on Bell’s Theorem,” Phys. Rev. Lett. 67, 661 (5 August 1991).

[3] Ekert, Artur. "What is Quantum Cryptography?" Centre for Quantum Computation – Oxford University.Conger., S., and Loch, K.D. (eds.). Ethics and computer use. Commun. ACM 38, 12 (entire issue).

[4] Johnson, R. Colin. "MagiQ employs quantum technology for secure encryption." EE Times. 6 Nov. 2002..

[5] Mullins, Justin. "Quantum Cryptography's Reach Extended." IEEE Spectrum Online. 1 Aug. 2003.

[6] Petschinka, Julia. "European Scientists against Eavesdropping and Espionage." 1 April 2004. 7. Salkever, Alex. "A Quantum Leap in Cryptography." BusinessWeek Online. 15 July 2003.

[7] Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004..

[8] MagiQ Technologies Press Release. 23 November 2003.

[9] Schenker, Jennifer L. "A quantum leap in codes for secure transmissions." The IHT Online. 28 January 2004.

[10] C. Elliott, “Building the quantum network,” New J. Phys. 4 (July 2002) 46.

[11] Pearson, David. "High!speed QKD Reconciliation using Forward Error Correction." *Quantum Communication, Measurement and Computing*. Vol. 734. No. 1. AIP Publishing, 2004.

[12] Curcic, Tatjana, et al. "Quantum networks: from quantum cryptography to quantum architecture." *ACM SIGCOMM Computer Communication Review* 34.5 (2004): 3-8.

[13] Shor, Peter W., and John Preskill. "Simple proof of security of the BB84 quantum key distribution protocol." *Physical Review Letters* 85.2 (2000): 441.
[14] Bienfang, J., et al. "Quantum key distribution with 1.25 Gbps clock synchronization." *Optics Express* 12.9 (2004): 2011-2016.
[15] Inoue, Kyo, Edo Waks, and Yoshihisa Yamamoto. "Differential phase-shift quantum key distribution." *Photonics Asia 2002*. International Society for Optics and Photonics, 2002.
[16] Barnum, Howard, et al. "Authentication of quantum messages." *Foundations of Computer Science, 2002. Proceedings. The 43rd Annual IEEE Symposium on*. IEEE, 2002.
[17] Elliott, Chip, David Pearson, and Gregory Troxel. "Quantum cryptography in practice." *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*. ACM, 2003.
[18] Buttler, W. T., et al. "Fast, efficient error reconciliation for quantum cryptography." *Physical Review A* 67.5 (2003): 052303.
[19] Poppe, A., et al. "Practical quantum key distribution with polarization entangled photons." *Optics Express* 12.16 (2004): 3865-3871.
[20] Lütkenhaus, Norbert. "Estimates for practical quantum cryptography." *Physical Review A* 59.5 (1999): 3301.