**From Traditional Cryptography to Quantum Cryptography**

Lu Lin

CPSC 6126

Columbus State University

Cryptography is one such method of protecting sensitive data from being stolen or intercepted by unwanted third parties [1]. Traditionally, cryptographic security relies on mathematics and computation powers that have developed. Quantum cryptography is different from traditional cryptographic systems in that it relies more on physics, rather than mathematics, as a key aspect of its security model.

The foundation of quantum cryptography lies in the Heisenberg uncertainty principle, and the origins of quantum cryptography can be traced to the work of Stephen Wiesner, who published his work “Conjugate Coding” in 1983. The first protocol for sending a private key using quantum techniques was published by Bennett and Brassard [2]. Over time, quantum cryptography protocol is proposed, and experimental prototype are made. More recently, the first computer network in which communication is secured with quantum cryptography is up and running in Cambridge, Massachusetts. In 2006, Zhou et al proposed a quantum block encryption algorithm [3], which can be used to encrypt classical messages as well as quantum messages.

Cryptography is one area that must be ahead of technology. The theoretical exponential increase in computing power of quantum computer has prompted cryptographers to begin devising improved cryptography methods. There are four major possible methods that may provide immunity from a quantum computer attack: error-correcting codes, hash-functions, lattice cryptography systems, and multivariate public-key cryptography systems [4].

Both traditional and quantum cryptography can be compared on following aspects:

1. Traditional cryptography is concerned there is frequent requirement of using longer keys as computational power doubles in every 18 months; whereas security in quantum cryptography is based on quantum mechanics, there may not be major changes requirements for future.
2. There are three essential algorithms: key generation, signatures, and key verification. These algorithms cannot be implemented in quantum cryptography easily, hence quantum cryptography lacks many critical features like digital signature [5].
3. For quantum cryptography, the existing infrastructure is sophisticated, and the cost is very high; whereas for traditional quantum cryptography the existing infrastructure is widely used, and the cost is very low.
4. The communication range of quantum cryptography now is about 10 miles, whereas for traditional cryptography is millions of miles. The reason why the length of quantum cryptography capability is so short is because of interference [6].
5. The private key the cryptosystem is an example of the traditional cryptosystem. There is a problem in the private key cryptography which is called the problem of key distribution. To establish the key, two users must use a very secure channel. An eavesdropper can monitor the channel without the users being aware that an eavesdropping has taken place. Quantum cryptography solve the problems of secret key by providing a way for two users who are in different locations to securely establish a secret key, and to detect if eavesdropping has occurred [7, 8].

At present, although traditional cryptography is still dominant over quantum cryptography, there are many interesting open problems require further investigations in quantum cryptography. In the near future one can expect most of the implementation problems in quantum cryptography to be overcome.

**References:**

[1] M. Bhatt, A. Aneja, and S. Tripathi, “Classical Cryptography v/s Quantum Cryptography A Comparative Study”, International Journal of Electronics and Computer Science Engineering, ISSN-2277-1956, pp.121-129.

[2] R. J. Hughes, D. M. Alde, P. Dyer, G. G. Luther, G. L. Morgan, and M. Schauer, “Quantum Cryptography”, LA-UR-95-806.

[3] Z. Cao, “Improvement of One Quantum Encryption Scheme”, International Journal of Quantum Information 2009(7): 335-339.

[4] T. L. Swaim, “Quantum Computing and Cryptography Today: Preparing for a Breakdown”, University of Maryland.

[5] A. Goyal, S. Aggarwal, and A. Jain, “Quantum Cryptography & its Comparison with Classical Cryptography: A Review Paper”, 5th IEEE International Conference on Advanced Computing & Communication Technologies, ISBN 81-87885-03-3, pp. 428-432.

[6] N. Mehta, “Traditional Cryptography versus Quantum Cryptography”, International Journal of Engineering Research and Application, ISSN: 2248-9622, Vol. 2, Issue 2, Mar-Apr 2012, pp.1411-1413.

[7] N. Chhabra, “Secret Key Generation and Eavesdropping detection using Quantum Cryptography”, International Journal of Computer Science and Information Technologies, Vol. 3(2), 2012, 3348-3354.

[8] I.V. Volovich, “On Classical and Quantum Cryptography”, Trento, Italy, July 25-31, 2001.