Unconditionally secure cryptosystem based on quantum cryptography

Yu Fang Chung[1] Zhen Yu Wu[2] Feipei Lai[1&3] Tzer Shyong Chen[4]

[1] Electrical Engineering Department, National Taiwan University, Taipei, Taiwan

[2] Computer Science and Information Engineering Department, National Cheng-Kung University, Tainan, Taiwan

[3] Computer Science and Information Engineering Department, National Taiwan University, Taipei, Taiwan

[4] Information Management Department, Tunghai University, Taichung, Taiwan

E-Mail: d92921014@ntu.edu.tw

Abstract

Most cryptographic works these days have employed mathematical concepts to design cryptosystems and algorithms. Therefore, mathematical concepts have become critical in the designing of cryptosystems, and are generally used to analyze cryptosystems and protocols, supporting the allegation that the intended cryptosystem is secure. In earlier cryptosystems, most algorithms were based on either factorization or discrete logarithm problem. This system has an overtly simple mathematical background and so, requires extensive secondary index computation. Therefore, a securer method must be developed to protect system security and to optimize system efficiency. Quantum cryptography detects intrusion and wiretapping. In quantum mechanics, a wiretap is not external or passive, but the opposite—changing its entity according to the internal component of the system. The status of the system changes once a wiretap is detected. Therefore, only the designer of the system can determine the quantum status of the system; eavesdroppers can neither determine the quantum status nor duplicate the system. Since quantum cryptosystem can reach unconditional security, it actually guarantees secure communication. Accordingly, this study examines quantum cryptography and contributes to secure quantum cryptography.

Keywords: Cryptosystem, quantum cryptography, quantum mechanic, and unconditional security.

1. Introduction

Proposal for a quantum computer

Computer science has been frequently improved and new related technologies have emerged. Improvement has been rapid, from vacuum tube to transistor technology to super-sized integrated circuit. In recent years, the size of the transistor in the processors has been vastly reduced, which is the key to the improvement of functions of computers. However, this continuous size reduction cannot persist for very long. Transistors that are too small constrain the overall functionality of the computer. Hence, in 1982, Richard Feynman [2], Nobel Prize winning physicist, proposed the concept of quantum computer, which exploits the benefits of quantum machinery.

In traditional computers, the most basic structural element, the bit, can exist in one of only two mutually exclusive states, 0 or 1, but in the quantum computer proposed by Feynman, this rule does not apply. A quantum bit can exist not only in the traditional 0 or 1 state, but also in continuous or overlapping states. When a quantum bit is in one of these states, it can be recognized to be in two domains, 0 and 1. However, operations based on such a kind of quantum bit affect two values simultaneously, as shown in Fig. 1. Operating on a single quantum bit, is therefore, in reality, to work on two values. Similarly, a bi-quantum bit system can work on four values, and a tri-quantum bit can operate on eight values. Accordingly, as the number of quantum bits increases, the quantum collateral effect obtained from the system is increased by the index method.

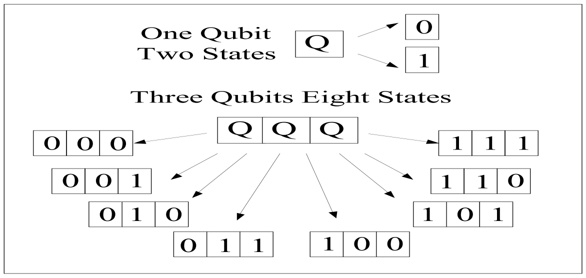


Fig. 1: State of quantum bit cache

For a long time, the concept of quantum computers remained purely theoretical. However, recent developments in quantum computers have attracted people's interest. Peter Shor's [3] research laboratory designed an algorithm that enables large amount of data to be calculated using quantum computers. A quantum computer can use this algorithm to solve simultaneously, problems like the *NP* problem or factorization, whose solutions depend on index operations. The temporal cost is a lot lower than that of any traditional computer, so research into quantum computers has become increasingly widespread. Numerous researchers are now vying to produce the first practical quantum computer.

Origin of quantum cryptographic system

Based on the above, a Shor's algorithm [3] quantum computer can solve the index equation problems in a few seconds, whereas most current cryptographic technologies, like RSA, DES, ECC, and others are based on factorization, discrete logarithms and other index operations. Restated, when quantum computers become practical, currently available cryptosystems will become useless and lack security. Furthermore, most public key cryptosystems have a simple mathematical background that can be hacked easily by scanning for loopholes and backdoors. This weakness is the shortcoming of modern cryptography. Accordingly, developing an entirely new cryptosystem has become the object of research in various fields. Such a system is the quantum cryptosystem.

The origin of the quantum cryptosystem is as follows. In the '70s, Stephen Wiesner [1] proposed the use of the one-time pad method for key distributions, exploiting the laws of physics to scan for system intrusion or wiretap. A wiretap is determined from whether the internal quantum state is changed. Quantum mechanics does not consider measurement to be an external and passive process, but changes the states of the system. Detection, wiretaps, and intrusion are types of measurement employed, where any wiretaps during key distribution can be detected. Therefore, a quantum cryptosystem achieves unconditional security.

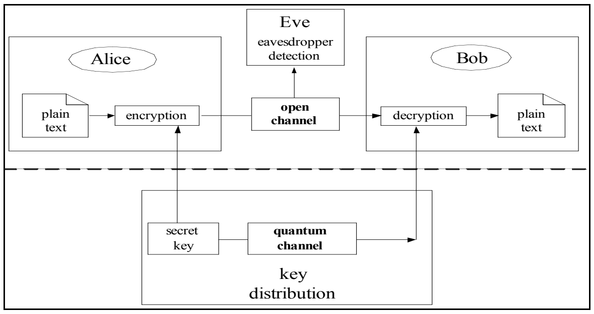


Fig. 2: Structure of quantum cryptosystem

Figure 2 shows an analysis of the system structure. Two main channels of communication are used. The first is the quantum channel, the purpose of which is to send and receive quantum bits, and to produce the secret (session) key. The second is the open channel, which is used by the sender and receiver to compare their quantum bits, and thus determine whether they are being tapped; they use their secret (session) key to encrypt plain text and decrypt cipher text, ensuring secure communication.

Once the workings of a quantum cryptosystem are understood, a quantum cryptographic protocol directed at key distribution can be designed, on the basis that a measurement can affect the quantum status of a system. The protocol is the mechanism for providing security by automatically detecting wiretaps. It is not merely the core of the entire system, but also the focus of development. The protocol is discussed in detail below.

2. Quantum cryptographic key distribution protocol

In the 1970s, Stephen Wiesner was the first to apply principles of quantum mechanics to the structure of cryptosystems. Reference [1] in the early '80s offered an entirely new vision of cryptography theory and technology. Thereafter, the unceasing efforts of Charles H. Bennett and Gilles Brassard were primarily responsible for the ongoing development of quantum cryptosystems. Most quantum cryptographic key distribution protocols developed during that time were based on Heisenberg's Uncertainty Principle, and Bell's Inequality (part of Bell's Theorem), both of which shall be explained in Section 3. Others, such as Eli Biham, BrunoHuttner and Tal Mor developed a cryptosystem that employed quantum non-localization. Users save a particle in the quantum memory of the sending center, such that users of the same center are guaranteed to be able to communicate securely. Simon J. D. Phoenix et al. introduced a method of developing a quantum cryptographic network that did not depend on quantum non-localization; Wiesner utilized bright light to construct a quantum cryptosystem; Bruno Huttner and Asher Peres employed non-coupled photons to exchange keys; Bruno Huttner et al. used a weak correlation to reduce substantially the amount of tapped information.

3. Quantum cryptosystems

Quantum cryptosystems based on Heisenberg's Uncertainty Principle

BB84 cryptosystem [4]

A polarized single photon is used to denote a 0 or 1 bit. Set *H* is a two-dimensional Hilbert Space whose element represents the polarization of the photon. Two different orthogonal bases, perpendicular polarization and polarization of 45 degrees, within *H* can be used.

Perpendicular polarization includes Ket, such as $|\uparrow\rangle$ and $|\rightarrow\rangle$; the former represents 1, and the latter 0. Also, 45 degrees polarization includes Ket, such as $|\nwarrow\rangle$ and $|\nearrow\rangle$; the former represents 1, and the latter 0.

Perpendicular polarization uses the instrument based on the measurement operation symbols, $|\uparrow\rangle\ \langle\downarrow|$ or $|\rightarrow\rangle\ \langle\leftarrow|$, to measure the polarization form. In addition, 45 degrees polarization uses the instrument based on measurement operation symbols, $|\nwarrow\rangle\ \langle\searrow|$ or $|\nearrow\rangle\ \langle\swarrow|$ as shown in Fig. 3, to measure the polarization form.

Instruments used to measure perpendicular polarization cannot be used to measure 45-degree polarization, just as instruments used to measure 45 degrees polarization cannot be used to measure perpendicular polarization. Figure 4 shows that if the polarization and instrument are similarly aligned, then the photon is accepted. Otherwise, the polarization of the accepted photon is uncertain.

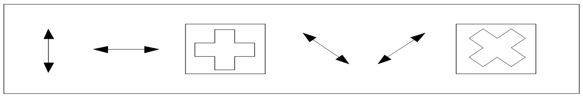


Fig. 3: Quantum polarization and measuring instrument

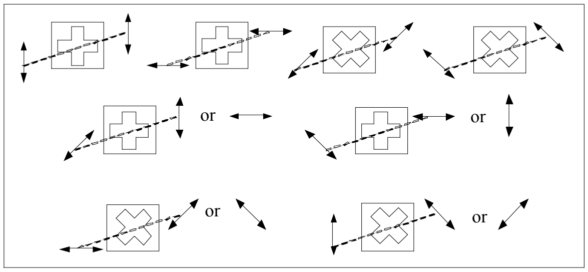


Fig. 4: Measurement of quantum polarization form

If two communicating parties use only one orthogonal base and measuring instrument, and if by coincidence the eavesdropper is using the same measuring instrument, then not only can the eavesdropper faultlessly obtain all bits transmitted by the sender, and remains undetected. Such a cryptosystem is thus easily hacked.

[Key distribution protocol]

Transmission via quantum channel

Sender Alice transmits to Bob, via a quantum channel, a bit string consisting of 0s and 1s. The 0s and 1s are denoted by the polarization of the photons. Only 1 bit is sent at a time. Furthermore, whether the transmitting bits are perpendicularly polarized or polarized at 45 degrees is randomly selected.

Transmission via open channel

First, Bob under open conditions, informs Alice of which polarization-measuring instrument is to be used and simultaneously measures every bit of data received. Next, Alice informs Bob of which bits were correct and which erroneous. Then, the erroneous bits are deleted, and the individual source keys are thus obtained.

Authentication on open channel

Alice and Bob are both in open transmission. Together, they select a part of the source key for comparison. A result of over 0.8% inconsistent bits indicates a presence of eavesdroppers, and requires Alice and Bob to return to the procedure in quantum channel. If the results show that under 0.8% are inconsistent bits, then the inconsistencies are assumed to be caused by noise, and that transmission segment is assumed to be secure. The exposed part of the source key is deleted, and a final secret (session) key is decided upon, which will be used for to and fro transmission.

Quantum cryptosystems based on Bell's Theorem

EPR cryptosystem [5]

First, isolated particles are formed into entangled photon pairs. A mutually connected perpendicularly polarized photon is constructed, and the form of its coupling is as follows.

$$|\Omega| = 1/\sqrt{2}(|\leftrightarrow\rangle_1 |\updownarrow\rangle_2 - |\updownarrow\rangle_1 |\leftrightarrow\rangle_2)$$

The symbol $|\theta\rangle$ denotes the photon's polarization form. In the formula, the suffixes 1 and 2 denote two different photons respectively; one has horizontal polarization form and the other vertical.

According to Bell's Inequality Theorem, suppose that photon entanglements at 0 degree, 22.5 degree and 45 degree violate the highest value of the inequality. Therefore, these three angles can be taken to be the measuring instruments for receiving photons, defined as M_0, M_1, M_2.

[Key distribution protocol]

Transmission via quantum channel

In each time slot, launch the entangled photon pair $|\Omega| = 1/\sqrt{2}(|\leftrightarrow\rangle_1 |\updownarrow\rangle_2 - |\updownarrow\rangle_1 |\leftrightarrow\rangle_2)$ described above; send one to Alice and the other to Bob, as shown in Fig. 5. Both Alice and Bob choose a measuring instrument from M_0, M_1, and M_2 to receive the photon, as shown in Fig. 6. Repeat several times the above process.

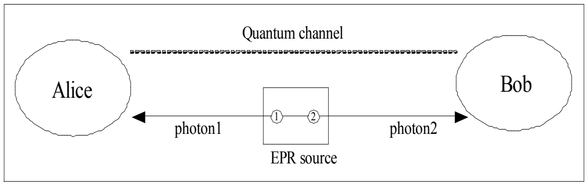


Fig. 5: Key distribution in EPR system

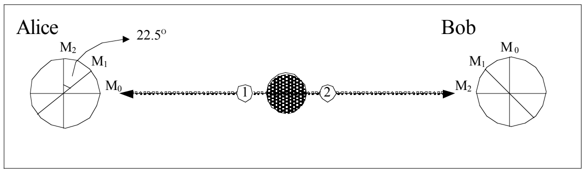


Fig. 6: Key distribution and receipt in EPR system

Transmission on open channel

Since entangled photons have correlations such that the photons sent to both parties employing the same measuring instrument have polarization forms of either $|\updownarrow\rangle$ or $|\leftrightarrow\rangle$. Consequently, we can say that if the received photon is $|\leftrightarrow\rangle$ then 0 has been received, and if the received photon is $|\updownarrow\rangle$ then 1 has been received. Hence, Alice and Bob can use the time slot where they employ a common measuring instrument to compose a 0-1 sequence source key, and use the rest of the photon bits for examination.

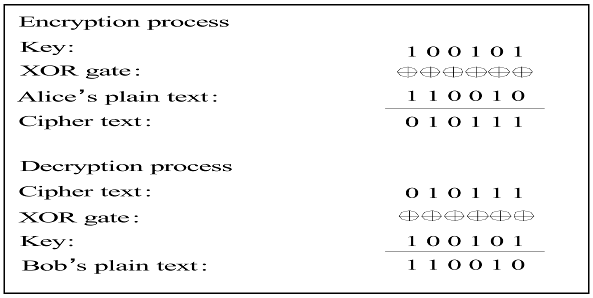
Authentication on open channel

The process of detecting wiretaps using Bell's Inequality is as follows. First, both parties use photons received by differing measuring instruments to perform examination. Since, the measuring instruments are different, the received photons, unlike received photons of common measuring instrument, do not have a regular pattern correlation. Nevertheless, because of the characteristic of entangled photons, in addition to the receiving instrument being the particular angle of $|\Omega|=1/\sqrt{2}(|\leftrightarrow\rangle_1|\updownarrow\rangle_2-|\updownarrow\rangle_1|\leftrightarrow\rangle_2)$ polarization form, therefore the result of the examination shall violate Bell's Equality and holds the highest value.

Apply this theorem and calculate each photon's degree of violation of Bell's Inequality. If the degree of violation is as expected, then there has been no eavesdropping. For if there were eavesdroppers during the process, then the status of the photons is bound to be altered, and the degree of violation will be lowered. Hence, eavesdropping and distortions during a process can be determined.

In a noise-congested environment, a key may include erroneous codes caused by instruments and other factors. This erroneous part of the code must be deleted. Hence, the source key is divided into a number of data blocks of length *l*, which are chosen such that no piece comprises more than one error code bit. Then, Alice and Bob both perform even-odd checks to determine the error on each segment of the source key. A binary search for finding the erroneous bit is conducted when dissimilarities are detected. The above action is repeated on every segment until all erroneous bits are eliminated. Thus, the final secret (session) key, which will be used for to and fro transmission, is obtained.

Finally, which protocol is used to generate the secret (session) key is unimportant. Both parties perform an XOR operation on the key, the plaintext and the ciphertext. The plaintext is encrypted and sent, whereas the received ciphertext is decrypted to obtain the plaintext. Thus, unconditional secure transmission is easily achieved, as shown in Fig. 7.



Encryption process	
Key:	1 0 0 1 0 1
XOR gate:	⊕⊕⊕⊕⊕⊕
Alice's plain text:	1 1 0 0 1 0
Cipher text:	0 1 0 1 1 1
Decryption process	
Cipher text:	0 1 0 1 1 1
XOR gate:	⊕⊕⊕⊕⊕⊕
Key:	1 0 0 1 0 1
Bob's plain text:	1 1 0 0 1 0

Fig. 7: The encryption-decryption process

4. Conclusions

Although quantum cryptosystems are still at the experimental stage and are unregulated, its development prospects well worth expecting. Paul D. Townsend of British Telecom Laboratories, John Rarity of Christophe Marand and other researchers have constructed an optical fiber that was about 30Km long. A key exchange process was designed on this optical fiber. Later, Richard and his colleagues at Los Alamos National Laboratory developed a 14 Km long underground optical fiber. Signals transmitted via this channel remained stable even after lengthy transmission. Japan's NEC used flat Planar Lightwave Circuit technology and a low-noise photon receiver to stretch the key transmission length to over 100 Km. In 2004, a transmission length of 150 km was reached [6], revealing that quantum cryptosystem, both in theory and in practice, has considerable potential.

Acknowledgement: This work was supported by the National Science Council, Taiwan, under contract No. NSC 95-2221-E-029-024.

References

[1] S. Wiesner, "Conjugate coding," *SIGACT News*, 15(1), pp. 78-88, 1983.

[2] R. Feynman, "Simulating physics with computers," *International Journal of Theoretical Physics*, 21(6&7), pp. 467-488, 1982.

[3] P. W. Shor, "Algorithms for quantum computation: discrete logarithm and factoring," *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science*, pp.124-134, 1994.

[4] C. H. Bennett and G. Brassard, "Quantum cryptography: Public key distribution and coin tossing," *International Conference on Computers, Systems & Signal Processing*, pp. 175-179, 1984.

[5] A. K. Ekert, "Quantum cryptography based on Bell's Theorem," *Physical Review Letters*, 67(6), pp. 661-663, 1991.

[6] http://www.optics.org/articles/news/10/3/11/1