International Journal of Soft Computing 10 (3): 239-241, 2015
ISSN: 1816-9503

Applying Quantum Computing in Cryptosystem

Le Nhat Duy
Industrial University of HoChiMinh City, 12 Nguyen Van Bao Street,
Ward 4, GoVap District, HoChiMinh, Vietnam

Abstract: The study briefly introduces the historical development along with some raising concerns of quantum computing and proposes some quantum applications in solving cryptography problems. Quantum cryptography is the study of information security based on the laws of quantum physics. Unlike classical cryptography focusing on mathematical complexity of algorithm in protecting information from attacks, quantum cryptography concentrates on the fundamental physical properties of the objects carrying information. These objects are identified by their quantum states which are unattackable by the computational power and will be widely applied in the future. This research paper also presents some main research areas of quantum cryptography and the study of BB84 protocol. In this protocol, a series of polarized photons is used to transmit information on the quantum channel and their states are exchanged via public communication channel.

Key words: Quantum cryptography, entangled states, no cloning theorem, key distribution system, protocol

INTRODUCTION

Quantum computing was firstly introduced in 1982 by Feynman (1982) whose studies are related to computing models based on quantum computer. He found that computations require an exponentially explosive growth in space-time volumn of the physical system. Consequently, it is impossible to represent the quantum mechanical effects with a classical computer. From that point of view, Feynman (1982) suggests "A new kind of computer-a quantum computer" operating on the basis of quantum effects principle including superposition and entangled. Given his research works, he focuses on studying applications of quantum mechanics in solving problems that require enormous and complex resource.

Quantum computer models are firstly introduced by Binioff (Quantum Turing Machine). Then Deutsch (1985) developed and proposed a physically quantum schema for the quantum computer.

In principle, the quantum computation model obeys the Church-Turing principle that every physical system can be perfectly simulated by a quantum computer.

The differences between classical probability and quantum model are the effectiveness and the power of quantum computation.

Some advantages and disadvantages of quantum computation: The prominent advantage of quantum computation is its superposition property that a quantum register is capable of receive many states simultaneously. For instance, a n bit quantum register can receive 2^n distinct states while a classical one only accepts 1 state of all bits at certain time. However, recent quantum computing results are not sufficient because it requires large changes in amplitude and high-probability calculations. To solve these problems, another quantum computing devices should be used as interface among states and its new amplitude will be a linear permutation of old amplitudes.

Another important property is the ability to conduct an entangled state of set of qubits that is impossible to identify certain state of a particle (Poppe *et al*., 2004). Unentangled states require exponentially computations with complex amplitudes while entangled states offer linear computations. Therefore, entanged quantum becomes necessary condition to offer an exponential speed up quantum computations over classical one.

Subsequent researches by Jozsa and Linden (2003) and Vidal (2003) showed that maximum range in quantum computing is a constant independent from the number of qubits and the time needed to solve a problem with quantum computer can be represented as a polynomial time. In contrast, the efficiency of classical computing models depends on the number of qubits.

One of drawbacks of quantum computing is the inability to ultimately exploit its calculation power and development. Indeed, quantum computing checks all possible solutions at random and if a wrong answer will be found, the amplitudes will be canceled out which leads to the loss of amplitude of the basis states. Classical algorithms will stop processing if one possible solution is reached. Conversely, quantum algorithms measure all possible solutions at the end and if we would like to have quantum algorithms behave as classical one, there should be special structure.

Another feature of quantum computing is the ability to perform inverse transformations on quantum registers. However if the number of qubits is limited (approximately to ~0 (log n) qubit where n is the input size), the computational ability becomes more complex and leads to exponential complexity accordingly.

THE MAIN DEVELOPMENTS OF QUANTUM CRYPTOGRAPHY

In quantum cryptography, there are 2 fundamental research directions related to key distribution system. The first research direction would be the study of quantum states of a particle. According to the laws of quantum mechanics, it is impossible to distinguish reliably between two non-orthogonal quantum states.

In two-level quantum mechanical system, every quantum state defined as linear superposition:

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$$

where, $|0\rangle$ vα $|1\rangle$ are special states with complex coefficients satisfying the condition:

$$|\alpha|^2 + |\beta|^2 = 1$$

Yet quantum mechanics theory ensures that 2 different quantum states cannot be distinguished perfectly unless they are orthogonal.

The first study is developed based on no-cloning theorem. It is impossible to create perfect copies of an unknown quantum state because of linearity and unitarity of quantum mechanics. For instance to transmit a secret message, a sender and a receiver use two-level quantum system for encoding and decoding process. The text is decoded into quantum states and sent to the receiver. If an attacker interferes into the transmission channel sent by the sender, measures it and sends it to the receiver, the quantum states of the signal will be affected and different from its original states. So, eavesdropping attacks on quantum channel causes errors in the transmissions that can be noticed by the authorized users.

A quantum cryptography protocol based on orthogonal states is BB84. The second study should be developed relying on the effect of quantum entanglement. Since two quantum mechanics systems can be correlated if a measurement is carried out on one of these two quantum systems, the result of the other would be probabilistic inference. None of these systems is not entangled in a particular state. Therefore, an entangled state can not be written as a direct product of the subsystems. Two spin ½ particles is an example of an entangled state:

$$|\psi\rangle = \frac{|01\rangle - |10\rangle}{\sqrt{2}}$$

A measurement is carried out on one of these two quantum systems with the probabilistic result of its staes is $|0\rangle$ or $|1\rangle$. So, the result of the second system will be opposite of the first one. i.e. if the quantum state of the first system is $|1\rangle$, the second system's state will be $|0\rangle$ and vice versa.

Basic quantum key distribution protocol based on the effect quantum entanglement is EPR protocol (Einstein-Podolsky-Rosen).

The basic principles of these two research directions were the basis for the development of all quantum key distribution protocols.

QUANTUM CRYPTOGRAPHY QUANTUM KEY DISTRIBUTION

Quantum cryptography offers solution for absolute security. This can help to solve remaining problems of classical cryptography by using one-time pad key distribution. Hence, it allows absolute security information transmission among authorized users. However to ensure the key distribution in safe way to the receiver, all of three following conditions must be satisfied (Gisin *et al*., 2002; Grzywak and Pilch-Kowalczyk, 2009):

- Message encoded with random key is a sequence of 0 and 1's bits: it is a complex process
- Key length is equal or greater than message length
- Secret key is used only once

BB84 PROTOCOL

BB84 was introduced in 1984 by Bennett and Brassard (1984). The fundamental of quantum cryptography is photon states. A sender sends state and a receiver stores and decodes those states. According to the no cloning theorem, 2 quantum states are not measured precisely at the same time. Polarization of photons can be orthogonal, diagonal or circular. Measurement of polarized photons can lead to different results. So if the both sender and receiver do not agree beforehand on a correct polarization bases, the receiver will decode data wrongly and therefore, can not receive meaningful information.

The sender encodes information into a sequence of polarization bases. Then both parties confirm on the final result. This will ensure the sending and receiving transmitted codes coincide perfectly. Though, errors may

exist in transit due to "noise" or eavesdropping attacks, the information is unrevealed. During transmission, the polarization of photons is well-controlled. Hence, polarization may be orthogonal (horizontal or vertical), circular (left or right) and diagonal (45° or 135°).

Polarized light source is used in transit can be diodes or laser emitting. Light passing through a polarizing filter turns into short pulses with low intensity. The polarization of each pulse is controlled by the sender and in following states: horizontal, vertical, left or right circular.

The receiver measures the polarization of photons by using a random sequence of polarized bases (orthogonal or circular). Then he publicly reports to the sender the bases that he used. The sender confirms to the receiver which bases are corrects. All measurement and calculation are performed under the laws that information will be canceled out if the receiver uses bases different from the sender's. The result is represented in a binary bit: 0 standing for a horizontal or left-circular photon; 1 standing form a vertical or right-circular photon. The protocol may induce errors if noises exist in transmission. These errors can be detected and corrected by parity algorithm in which one bit of each transmitting block will be removed.

CONCLUSION

In the rapid development of computer technologies, information and data security is considered as a most concerning issue for enterprises and organizations. Applying quantum cryptography in information security ensures ultimate security, data authentication and secure communication (Kilor and Soni, 2014). It also provides new methods of protecting the most valuable and secret information for financial institutions, banks, airlines and multimedia.

REFERENCES

Bennett, C.H. and G. Brassard, 1984. Quantum cryptography: Public key distribution and coin tossing. Proceedings of the IEEE International Conference on Computers System and Signal Processing, December 10-12, 1984, Bangalore, India, pp: 175-179.

Deutsch, D., 1985. Quantum theory, the church-turing principle and the universal quantum computer. Proc. R. Soc. London, 400: 97-117.

Feyman, R.P., 1982. Simulating physics with computers. Int. J. Theor. Phys., 21: 467-488.

Gisin, N., G. Ribordy, W. Tittel and H. Zbinden, 2002. Quantum cryptography. Rev. Mod. Phys., 74: 145-195.

Grzywak, A. and G. Pilch-Kowalczyk, 2009. Quantum cryptography. Theor. Applied Info., 21: 149-166.

Jozsa, R. and N. Linden, 2003. On the role of entanglement in quantum computational speed-up. Proc. Math. Phys. Eng. Sci., 454: 2011-2032.

Kilor, P.P. and P.D. Soni, 2014. Quantum cryptography: Realizing next generation information security. Int. J. Applic. Innov. Eng. Manage., 3: 286-289.

Poppe, A., A. Fedrizzi, T. Loruenser, O. Maurhardt and R. Ursin *et al*., 2004. Practical quantum key distribution with Polarization-entangled photons. Optics Exp., 12: 3865-3871.

Vidal, G., 2003. Efficient classical simulation of slightly entangled quantum computations. Phys. Rev. Lett., Vol. 91.