Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

STUDY ON QUANTUM OBLIVIOUS TRANSFER AND QUANTUM BIT COMMITMENT

[1] XIAOQIANG GUO, [2] CUILING LUO [3] YAN YAN

[1]College of Science, Hebei United University, No.46 Xinhua West Street, Tangshan 063009, Hebei Province, China

E-mail: [1]guoxiaoqiang@heuu.edu.cn , [2]guoxq2004@163.com

ABSTRACT

Oblivious Transfer and Bit Commitment are typical foundation agreements to secure multi-party computations. Both of them are hotspots in the field of information security. Using of the quantum channel and the principles of the quantum mechanics, Quantum Oblivious Transfer can be achieved higher security and higher efficiency than the Classic Oblivious Transfer, while it also has a unique advantage in found eavesdropping. Quantum Bit Commitment scheme can be used to build up zero knowledge proof, verified secret sharing, throwing coins etc agreements. We had given out a very novel QOT scheme based on three-particle entangled states. And we had investigated unconditional secure Quantum Bit Commitment existence. At last, we constructed a new bit commitment model – double prover bit commitment. The Quantum Bit Commitment Protocol can be resistant to errors caused by noise.

Keywords: *Quantum Oblivious Transfer, Quantum Bit Commitment, Secure multi-party computations, Information Security*

1. INTRODUCTION

The Oblivious Transfer means the recipient can get their wanted messages from the sender's secret message set, but you cannot get the other messages, and the sender does not know which messages the recipient choose. The basic ideas of bits commitment are as follows: the sender called Alice promises a bit b to receiver Bob, in the commitment stage, Alice promises the bit b to Bob, but Bob cannot know the information of b; in the reveal stage, Alice confirms her commitment in the first stage indeed b, but she cannot cheat Bob in the second stage tampering with the value of b. The Oblivious Transfer and the Bit Commitment are important concepts in modem cryptography. Both of them constitute the basis of secure multi-party computations. Now they are widely used to build zero-knowledge proof, verified secret sharing protocol, throwing coins etc agreements to solve practical problems, such as electronic voting, elections, e-commerce[1].

The concept of Oblivious Transfer was first proposed by Rabin in [11]. Subsequently Even, Goldreich, Lempe1 developed the concept into alternative model $\binom{2}{1}$-OT in [12]. Crepeau proved Rabin's OT and $\binom{2}{1}$-OT are equivalence in [13]. The concept of Bit Commitment first was proposed by M.Blum in [3]. Yao gave Bit Commitment model in [2] called Yao Model. H.K. Lo and H.E. Chau constructed LC model in [4]. Later development many new OT model were constructed e.g. $\binom{2}{1}$-OT^k, ANDOS, GOT,UOT.

T. S. Zhao and J. H. Ge constructed GCOT model in [9]. C.M. Tang, Z.A. Yao and D.Q. Xie first proposed verifiable oblivious transfer protocol (VOT) in [10].

In section 2 we mainly study on quantum oblivious transfer. We construct a QOT scheme based on three-particle entangled state and give the validity analysis. In section 3 we will discuss unconditional security of quantum bit commitment existence. After we will use QOT to build QBC model and analysis its security.

Journal of Theoretical and Applied Information Technology
10th January 2013. Vol. 47 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

2. OBLIVIOUS TRANSFER BASED ON THREE-PARTICLE ENTANGLED STATES

2.1 Entanglement

Schrodinger first proposed the word "entanglement ", it is to show multi-particle system or multi-freedom system cannot be expressed as the direct product forms of superposition state. Composite system cannot be writen its subsystem state tensor product state called entanglement[3].

Quantum entanglement is such a quantum mechanics phenomenon: entanglement state only of two or more particles combined with other particles, even though all particles described in the space between the quarantined (or even be separated any distance)[6]. This feature will cause physical system observable properties correlates. As for three-particle entangled state, through SLOCC (Stochastic Local Operations and Classical Communication) means, Dur demonstrated any non-trivial can be transformed into one of the following two standard forms: namely

GHZ state: $|GHZ\rangle = \frac{1}{2}(|000\rangle + |111\rangle)$

And W state:

$$|W\rangle = \frac{1}{\sqrt{3}}(|001\rangle + |010\rangle + |100\rangle)$$

2.2 Quantum Oblivious Transfer (Qot) Scheme Based On Three-Particle Entangled State

To simplify the analysis and proof, we also assume that the used quantum channel is error-free. That is to say, channel noise must be caused by the eavesdropper.

Let b_0 and b_1 are two bits of Alice owns, and Bob's choice b_c is Bob hope to get. Before the start of the agreement, Alice and Bob agreed a safety parameters n (specifically, n is 8 multiples).

Protocol 2.1 QOT-Using Tripartite Entangled States

(i) Alice uniform randomly selected a binary bit string $A = a_1 a_2 \cdots a_n$, Bob set an empty temary string $T = t_1 t_2 \cdots t_n$, where t_i will be determined in step 3.

(ii) For each a_i of A, according to the value of a_i, Alice prepared a three-particle entangled state: if $a_i = 0$, then she randomly prepared a GHZ state or quantum state $|\Omega\rangle = |100\rangle$ each with probability $1/2$; otherwise, she prepared a W state. Then she ordinal put these three-particles entangled state in accordance with the order sent to Bob.

(iii) After Bob received each state, in accordance with the following rules, quantum measurements:

He first uses the base $\{|0\rangle, |1\rangle\}$ for particle 1 to projection measurement. If the result is $|1\rangle_1$, and he continues to use the base $\{|0\rangle, |1\rangle\}$ for particle 2 to projection measurement. In this case, if the result of the measurement is $|1\rangle_2$, then he set $t_i = 0$; otherwise he set $t_i = \perp$.

On the other hand, if the result of the measurement for particle 1 is $|0\rangle_1$, then he unite particle 2 and 3 for Bell measurement. In this case, if the result of the measurement is $|\phi^+\rangle$ or $|\phi^-\rangle$, then he set $t_i = 0$; If the result is $|\psi^+\rangle$, then he set $t_i = 1$; If the result is $|\psi^-\rangle$, then Bob can be concluded that there exist eavesdropper on quantum channel, he informs Alice to terminate the agreement.

(iv) Bob divided the measurement results into two sets $M_0 = \{j_0, j_1, \cdots, j_\theta\}$ and $M_1 = \{j_\theta, j_{\theta+1}, \cdots, j_{2\theta}\}$, where $\theta = 3n/8$, and for every $j_i \in M_0 (i \in [0, \theta])$, Bob certainly knows the value of a_{j_i}. Then Bob will send tuple $(X, Y) = (M_C, M_{1-C})$ to Alice.

(v) Alice calculated $m_0 = \bigoplus_{x \in X} a_x$ and $m_1 = \bigoplus_{y \in Y} a_y$, then she sends Bob tuple $(d_0, d_1) = (b_0 \oplus m_0, b_1 \oplus m_1)$.

(vi) Bob calculated $d_c \oplus m_c$ to get his secret bit b_c.

2.3 Validity Analysis

Suppose Alice and Bob is honest (That is, they are honest implementation of the above agreement).

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

We will analyze and give the following conclusions: after the end of step 6 execution of Protocol 2.1, Alice successfully sent Bob her choice of bits. In step 3, if Bob gets the results $|1\rangle_1$ after orthogonal measurements to particle 1, then the remaining particles 2 and 3 may be in the following two states: $|11\rangle$ (corresponding to the initial state is $|GHZ\rangle$), or $|00\rangle$ (corresponding to the initial state is $|\Omega\rangle$ or $|W\rangle$). Therefore, then Bob gets the result $|1\rangle_2$. He can draw a firmer conclusion: Alice prepared in the initial state must be $|GHZ\rangle$. Similarly, if the particle 2 measurement result is $|0\rangle_2$, then Bob cannot determine what is Alice made the initial state, because the state $|\Omega\rangle$ and $|W\rangle$ can obtaine the same results.

Bob gets the result $|0\rangle_1$ of the case is relatively simple, we omit concrete analysis for brevity.

Now we consider the probability that honest Bob reliably gets information a_i. By Protocol 2.1, we can know that if he got a record $t_i \neq \perp$, then he certainly won the value of a_i, this time $a_i = t_i$. Therefore the probability is:

$$\Pr: \frac{1}{4}*0+\frac{1}{4}*1+\frac{1}{2}*\frac{2}{3}=\frac{7}{12}.$$

So far Alice knew her preparation about $1-7/12=5/12$ of the quantum state no leaks useful information about a_i to Bob (in contrast is the case when Bob set $t_i = \perp$).

In step 3, if Bob dose not detect the eavesdropper, then from step 4 to step 6, he can get what he wanted from Alice and know nothing about Alice's another bit. Because according to the above probability analysis, Bob cannot get the information of a_i in collection M_1.

3. UNCONDITIONAL SECURITY OF QUANTUM BIT COMMITMENT EXISTENCE DISCUSSION

3.1 Standard Bit Commitment Model

Bit commitment as an important basis of secure computation, which is based on measurement and unitary transformation quantum agreement, generally follows a fixed model. The model is first proposed by A. C. Yao, even though Yao has not emphasized the generality of the model, but the model was evaluated as " really applies to any actual and secure computation "[2].

Model Yao: A both quantum protocol is a quantum machine through a certain quantum channel to interact in specific ways. Each machine is of a mixed quantum state in the initial stages. In form, consider the direct product H of three Hilbert space H_A, H_B and H_C, where H_A is Alice' machine, H_B is Bob' machine, H_C is a Hilbert space of quantum channel. For any one $D \in$ (Alice, Bob), he(she) controls their own part space $H_D \otimes H_C$ and measures the current status so that the state collapse on the results of measurement. Then, D carried on a unitary transformation in the space $H_D \otimes H_C$, and it accordingly caused a unitary transformation in the space H. The design principles of measurement and transformation is that Alice and Bob finally get some useful information about their joint initial state[2].

3.2 Unconditional Secure Multi-Party Quantum Oblivious Transfer Realize The Standard Model Bit Commitment

C.Crepeau thinks even though unconditional security of oblivious transfer existence cannot be reducted into unconditional security of bit commitment[4]. But he only considers a specific reduction, and therefore has not a representative. The reduction that will be given is a new, concise and elegant, whether quantum measurement or a classic way of communication, as long as there exists an unconditional security of oblivious transfer protocol. It is possible to construct unconditional security of bit commitment.

Below we combined with unconditional secure multi-party quantum oblivious transfer QOT( ), and establish safety parameters for N, described the specific agreement as following:

I. Commitment stage

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Protocol 3.1 commit QBC( )

For $X = 100$ to N

{ Set Bob to oblivious transfer two random bits b_{x_0} and b_{x_1}, he oblivious transfers to Alice the two bits with QOT( ). If Alice needs to commit the bit 0, then she secretly obtained information of b_{x_0}; otherwise she secretly got the information of b_{x_1}. Let Alice secret bit is b_{x_c} }

II. Reveal stage

Protocol 3.2 reveal QBC ( )

(i) Alice send her commitment bit to Bob.

(ii) For $X = 0$ to N

{ Alice send the bit x_c from Bob to Bob.

Bob tnen verify, for each x_c, has $x_c = b_{x_c}$ }

(iii) In setp 2, if every step of the validation is through, then Bob outputs "accept"; otherwise output "reject".

3.3 Analysis

Commitment stage: because the premise is that the oblivious transfer is unconditional security. In each step of the commitment stage, Alice can only obtain Bob randomly selected one of the two bits, and Bob is impossible to know the choice of Alice before reveal stage. So it is impossible to get the information of Alice commitment bit a advanced before reveal stage. This is independent form Bob's computing capacity. Thus the above reduction program has been unconditionally hidden.

Reveal stage: if Alice wanted to cheat, namely she hoped to show any bit $(1, a)$ in reveal stage, she was only "correct answers" all bits of N to make Bob output "accept". In fact, taking into account the randomness of Bob each selection b_{x_0} and b_{x_1}, the probability of successful Alice cheat tends to infinitesimal as N increasing. Thus the above reduction program has unconditionally tied qualitative.

Based on the comprehensive of Protocol 3.1 and Protocol 3.2, we construct a new commitment model – double prover bit commitment. In this model, the commitment becomes by one person into two, they commit a bit or bit strings to third parties. We give classical bit commitment and quantum bit commitment agreement. And they are unconditional security, quantum bit commitment protocol can also be resistant to errors caused by noise in actual.

4. CONCLUSIONS

In this paper, we constructe a truly safe and efficient quantum oblivious transfer protocol which is based on three-particle entangled state, and carry out the validity analysis. Now there are mature preparation methods and the use of program for three-particle entangled form and GHZ state[5]. So we give out the protocol that is simple, safe and easy to implement. Also we constructe a new double prover bit commitment model. In this model, before commitment stage, two promissories can communicate freely to agree communication content. However, after the start of the agreement, require them no longer communicate. The most important characteristics of the model is one promissory responsible for showing information to third parties in reveal stage, then the another promissory has no possibility of cheating.

ACKNOWLEDGEMENTS

This work was supported by the Scientific Technology Research and Development Plan Project of Tangshan (No. 121302001a).

REFRENCES:

[1] S. S. Luo, "Cryptography and Information Security Technology", *Beijing University of Post and Telecommunications Press*, 2009.

[2] A. Yao, "Protocols for Secure Computation", *Proc of the 23rd IEEE Symposium on Foundations of Computer Science*, 1982, pp. 160-164.

[3] G. H. Zeng, "Quantum Cryptography", *China Science and Technology Press*, 2006.

[4] H.K. Lo and H.E. Chau, "Why Quantum Bit Commitment and Ideal Quantum Cointossing are Impossible", *Physica D.*,Vol. 120, 1998, pp. 177-187.

[5] R. Ursin, F . Tiefenbacher, M. T. Schmitt , et al, "Entanglement-based Quantum Communication over 144 kms", *Nature Physics*, 2007, pp.481-486.

[6] L. M. Duan and G. C. Guo, "Probabilistic Cloning and Identification of Linearly Independent Quantum States", *Physics Review letters*, 1998, pp. 4999-5002.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[7] China Science and Technology Association, "Cryptography Subject Development Report", *China Science and Technology Press*, 2007-2010.

[8] H. Chen, "Introduction of Quantum Confidential Communication", *Beijing Institute of Technology Press*, 2010.

[9] T. S. Zhao and J. H. Ge, "An Efficient PMPC Protocol", *Journal of Circuits and Systems*,Vol. 13, No. 2, 2008, pp. 26-30.

[10] C.M. Tang, Z.A. Yao and D.Q. Xie, "Verifiable Oblivious Transfer Protocol", *Journal of Guangzhou University(Natural Science Edition)*, Vol. 9, No. 2, 2010, pp. 20-24.

[11] M. O. Rabin, "How to Exchange Secrets with Oblivious Transfer", http: //eprint.iacr.org，Harvard University Technical Report, 1981.

[12] S. Even，O. Goldreich，A. Lempe1．"A Randomized Protocol for Signing Contracts", Proc．CRYPTO'82, New York：Plenum Press, 1983, pp. 205-210．

[13] C.Crepeau. "Equivalence between Two Flavours of Oblivious Transfers", CRYPTO'87, Berlin Heidelberg：Springer，1987.