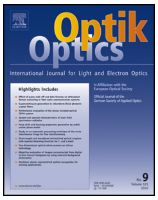
Optik 125 (2014) 5409–5413

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo



Quantum oblivious transfer with an untrusted third party

Yu-Guang Yang[a,b,*], Peng Xu[a], Ju Tian[a], Hua Zhang[c]

[a] *College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China*
[b] *State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China*
[c] *State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China*

ARTICLE INFO

Article history:
Received 4 October 2013
Accepted 27 May 2014

PACS:
03.67.Dd
03.67.Hk

Keywords:
Quantum oblivious transfer
Untrusted
Third party

ABSTRACT

Given the Mayers–Lo–Chau (MLC) no-go theorem, unconditionally secure quantum bit commitment (QBC) is impossible and hence quantum oblivious transfer (QOT) based on QBC is insecure. In this paper, we propose a secure all-or-nothing QOT protocol and a one-out-of-two QOT protocol respectively. The unique merit of the proposed protocols lies in that it is not based on QBC but based on an untrusted third party. Moreover, the proposed protocols do not violate Lo's no-go theorem so that their security can be achieved.

1. Introduction

As we know, the basic principles of quantum physics ensure classical unattainable security in a lot of cryptography applications, such as quantum key distribution, one of the most mature applications of quantum cryptography. However, some no-go theorems show that quantum cryptography cannot satisfy the security requirements for all tasks. For example, Mayers, Lo and Chau demonstrated the insecurity of QBC (against an Einstein–Podolsky–Rosen (EPR) type of attack with delayed measurements) [1–3], which is referred to as the MLC no-go theorem and is a serious drawback in quantum cryptography. According to the theorem, all QBC-based protocols are insecure and hence QOT based on QBC is insecure unless the participants are restricted to individual measurements [4]. And the Lo's no-go theorem shows that ideal one-sided two-party quantum secure computation [5] is insecure and hence a one-out-of-two QOT is impossible either.

These remarks apply particularly to oblivious transfer (OT), an important primitive extensively used in many cryptographic protocols [6–13]. There are two major types of OTs. The original one [6] is simply known as oblivious transfer, also referred to as all-or-nothing OT, in which a sender (say Alice) can send a one-bit message b to a receiver (say Bob) through communication channels. Bob learns the value of b with the probability 50%, Bob knows whether he got b or not. Alice does not know whether Bob got b or not. Another type of OT is called one-out-of-two oblivious transfer [7] and allows Alice to send two one-bit messages to Bob. Bob can choose to receive either one of these two messages but not both, while Alice does not know Bob's choice.

Given the MLC no-go theorem and Lo's no-go theorem, secure QOT seems impossible. Intriguingly, He et al. [14] proposed an all-or-nothing QOT protocol with stand-alone security. This QOT protocol does not rigorously satisfy the definition of ideal one-sided two-party quantum secure computation, on which the Lo's insecurity proof [5] was based. Thus it could evade the two no-go theorems and remain unconditionally secure against the cheating strategy in the Lo's proof.

In mutually untrusted two-party and multiparty computations, the party who takes charge of generating quantum signals has a bigger advantage of cheating than the other parties. Obviously, this strategy works for one-sided two-party quantum computation including QBC and QOT. In fact, not only the QBC and QOT protocols, but also the other quantum cryptographic protocols, such as controlled quantum secure direct communication (CQSDC) protocols [15], quantum secret sharing (QSS) [16,17], quantum direct communication with authentication [18] and quantum signature [19] and so on have similar hidden troubles.

As far as secure QOT is concerned, additional assumption is necessary. In this paper an untrusted third party is introduced, based on which we propose two protocols for all-or-nothing QOT and one-out-of-two QOT respectively. Moreover, these two QOT protocols do not belong to a class of protocols denied by the Lo's

[*] Corresponding author.
E-mail address: 17431644@qq.com (Y.-G. Yang).

http://dx.doi.org/10.1016/j.ijleo.2014.06.023
0030-4026/© 2014 Elsevier GmbH. All rights reserved.

no-go theorem of one-sided two-party secure computation [5], and so their security can be achieved.

2. The description of QOT

Our protocols are based on the two-qubit entangled state with the following form:

$$|\Psi\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|\varphi_0\rangle_B + |1\rangle_A|\varphi_1\rangle_B), \tag{1}$$

where

$$|\varphi_0\rangle = \cos\frac{\theta}{2}|0\rangle + \sin\frac{\theta}{2}|1\rangle, \quad |\varphi_1\rangle = \cos\frac{\theta}{2}|0\rangle - \sin\frac{\theta}{2}|1\rangle, \tag{2}$$

where $|\varphi_0\rangle$ and $|\varphi_1\rangle$ represent the bits 0 and 1, respectively. The parameter $\theta \in (0, \pi)/2$. Qubits A and B in each pair compose S_A sequence $\{A_1, A_2, \ldots, A_n\}$ and S_B sequence $\{B_1, B_2, \ldots, B_n\}$ respectively.

Eq. (1) can be rewritten as

$$|\Psi\rangle_{AB} = \cos\frac{\theta}{2}|+\rangle_A|0\rangle_B + \sin\frac{\theta}{2}|-\rangle_A|1\rangle_B, \tag{3}$$

where

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle).$$

2.1. All-or-nothing QOT

(1) The third party, Trent prepares n photon pairs in the same quantum state $|\Psi\rangle_{AB}$ and sends S_A sequence to Alice, S_B sequence to Bob respectively.

(2) Alice and Bob select *checking mode* or *message mode* on their qubits respectively.

 (2.1) For each qubit A_i, Alice selects *checking mode* with a probability of c, and *message mode* with a probability 1-c. Here the selection of the value of c depends on whether Alice can verify the honesty of Trent successfully.

  i. ***Checking mode***: Alice performs measurement on the received qubit with $\{|+\rangle, |-\rangle\}$ basis.

  ii. ***Message mode***: Alice performs measurement on the received qubit with $\{|0\rangle, |1\rangle\}$ basis.

 (2.2) For each qubit B_i, Bob selects *checking mode* with a probability of d, and *message mode* with a probability 1-d. Here the selection of the value of d depends on whether Bob can verify the honesty of Trent successfully.

  i. ***Checking mode***: Bob performs measurement on the received qubit with $\{|0\rangle, |1\rangle\}$ basis.

  ii. ***Message mode***: Bob subjects qubit B_i to a measurement of P_0 or P_1. Here $P_0 = 1 - |\varphi_1\rangle\langle\varphi_1|$ and $P_1 = 1 - |\varphi_0\rangle\langle\varphi_0|$ be (non-commuting) projection operators onto subspaces orthogonal to $|\varphi_1\rangle$ and $|\varphi_0\rangle$, respectively.

(3) To verify the honesty of Trent, Alice and Bob select the measurement results in the positions which they both select for security check. For all checking qubits, Alice and Bob choose the announcement order randomly to announce their measurement results, i.e., Alice first, Bob second, or Bob first and Alice second in a random order. If Alice's and Bob's measurement results satisfy the correlations in Eq. (3), i.e., Alice's measurement result is $|+\rangle$ and Bob's measurement result is $|0\rangle$; or Alice's measurement result is $|-\rangle$ and Bob's measurement result is $|1\rangle$, they can judge that Trent is honest and he has sent the genuine quantum states $|\Psi\rangle_{AB}$. (As usual, we assume noiseless channels.) They discard the measurement results in those positions which not both of Alice and Bob select for security check and remain the remaining measurement results, say n' bits, which are all known to Alice and a fraction of $\sin^2\theta/2$ known to Bob.

(4) According to the conclusiveness of his measurement results, Bob can determine two sets $I_0 = \{i|\text{conclusiveness}\}$ and $I_1 = \{i|\text{inconclusiveness}\}$ from which some arbitrary elements can be added or removed in order to get $\#I_0 = \#I_1 = \lfloor (n'\sin^2\theta)/2 \rfloor = m$.

(5) Bob discloses to Alice the sets I_s and I_{1-s} for a random bit s that he keeps secret.

(6) Alice chooses $s' \in \{0, 1\}$ at random and computes $c_{s'} = \bigoplus_{i \in I_{s'}} r_i$, where r_i is Alice's von Neumann measurement result on qubit i. Then she publicly announces s' and returns to Bob $b \oplus c_{s'}$. If $s = s'$, then Bob can compute $\bigoplus_{i \in I_0} r_i$ and obtain the bit b; otherwise he fails to get it.

2.2. One-out-of-two QOT

In contrast to all-or-nothing QOT, the first four steps are same so that the description of the one-out-of-two QOT protocol starts from step (5′).

(5') Bob sends $(X,Y)=(U,V)$ or $(X,Y)=(V,U)$ to Alice according to a random bit j.

(6') Alice computes $c_0 = \bigoplus_{i \in X} r_i$ and $c_1 = \bigoplus_{i \in Y} r_i$, where r_i is Alice's von Neumann measurement result on qubit i. Then she returns to Bob $b_0 \oplus c_0$ and $b_1 \oplus c_1$.

(7') Bob computes $\bigoplus_{i \in U} r_i \in \{c_0, c_1\}$ and uses it to get the bit b_j.

3. Proof of security

Large gaps always exist between theory and practice, and the issue being discussed here is no exception. A problem that we face is that the real-life implementation of quantum cryptography protocols may differ from the ideal design. For example, the ideal single photon source required by the original BB84 protocol is unattainable in practice, and is thus often replaced by a laser source that generates a weak coherent state. The presence of multi-photons will cause the photon-number-splitting attack [20]. Practical device imperfections such as imperfect single photon detector, dark counts, the wave-length-dependent characteristic of a fiber beam splitter and so on can lead to various types of attacks [21–29].

Because it is impossible for us to consider all possible attacks on our protocols, we assume that the security of our protocols depends on six fundamental assumptions as follows:

Assumption 1. Trent, Alice and Bob's physical locations are secure and no unwanted information can be leaked to the outside.

Assumption 2. Alice and Bob have trusted random number generators.

Assumption 3. Alice and Bob have trusted classical devices to store and process the classical data.

Assumption 4. Alice and Bob share an open authenticated classical channel.

Assumption 5. Quantum physics is correct.

Assumption 6. The quantum channel is ideal, i.e., noise-free and no particle losses.

Next we prove generally that the protocols are secure against some possible cheating strategy from Trent, Alice or Bob.