Nonequivalence of two flavors of oblivious transfer at the quantum level

Guang Ping He
Department of Physics and Advanced Research Center, Zhongshan University, Guangzhou 510275, China

Z. D. Wang
Department of Physics and Center of Theoretical and Computational Physics, The University of Hong Kong, Pokfulam Road, Hong Kong, China

(Received 12 January 2006; published 26 April 2006)

Though all-or-nothing oblivious transfer and one-out-of-two oblivious transfer are equivalent in classical cryptography, we here show that a protocol built upon secure quantum all-or-nothing oblivious transfer cannot satisfy the rigorous definition of quantum one-out-of-two oblivious transfer due to the nature of quantum cryptography. Thus the securities of the two oblivious transfer protocols are not equivalent at the quantum level.

DOI: 10.1103/PhysRevA.73.044304 PACS number(s): 03.67.Dd, 03.67.Hk, 03.67.Mn, 89.70.+c

I. INTRODUCTION

The mystery of quantum cryptography has long intrigued scientists. On one hand, several cryptographic tasks such as the quantum conjugate coding [1] and the well-known quantum key distribution [2–4] have had great success. They achieved theoretically unbreakable security which can never be reached by their classical counterparts. But, on the other hand, some no-go theorems were established, indicating that quantum cryptography is not always powerful for any task. In particular, the Meyers-Lo-Chau (MLC) no-go theorem [5,6] rules out the possibility of nonrelativistic unconditionally secure quantum bit commitment (QBC), and the Lo's insecurity proof of ideal one-sided two-party quantum secure computations [7] indicates that a one-out-of-two oblivious transfer is impossible either.

Oblivious transfer (OT) is an important concept found to be very useful in designing multiparty cryptography protocols [8]. There are two major flavors of OTs. The original one [1,9] is simply known as oblivious transfer, while sometimes it is also referred to as all-or-nothing OT. Another related notion was proposed later, which is called one-out-of-two OT [10]. In classical cryptography, it was shown that these two are computationally equivalent [11]. Essentially, a protocol was presented in Ref. [11] to illustrate that secure all-or-nothing OT can lead to secure one-out-of-two OT. Furthermore, it was believed that secure one-out-of-two OT can lead to secure bit commitment (BC) [7]. This standard classical reduction chain reveals the connection between the security of OT and BC protocols at the classical level.

Very recently, a quantum all-or-nothing OT protocol was developed [12]. This OT does not rigorously satisfy the requirement of ideal one-sided two-party quantum secure computation protocols, on which the Lo's insecurity proof was based. Thus it could remain unconditionally secure against the cheating strategy in the Lo's proof. Nevertheless, at first glance, this result would conflict with the Lo's conclusion and in turn with the MLC no-go theorem (i.e., secure quantum one-out-of-two OT and QBC would be possible) if the mentioned standard classical reduction were justified.

But intriguingly, it has also been realized that "reductions and relations between classical cryptographic tasks need not necessarily apply to their quantum equivalents" [13]. Indeed, it will be shown in this paper that once we intend to build an one-out-of-two OT protocol on a secure quantum all-or-nothing OT protocol with the method developed in Ref. [11], it is impossible that the resultant protocol can satisfy the rigorous definition of one-out-of-two OT on which the Lo's proof was based. In this sense, secure quantum all-or-nothing OT does not imply secure quantum one-out-of-two OT, i.e., the above classical reduction chain is broken in the present quantum cryptography case. As a result, there exists no logical conflict between the existence of secure quantum all-or-nothing OT protocol and the MLC no-go theorem of QBC, giving more room for quantum cryptography applications.

The paper is organized as follows. In Secs. II and III, the definitions of two flavors of OTs will be stated precisely and a brief review on their classical equivalence will be presented. The nonequivalence of these two OTs at the quantum level will be revealed in Sec. IV, along with its impact on the security of the protocols. In Sec. V, it will be indicated that the breaking of the reduction chain is not simply a matter of the definition, rather is originated from the nature of quantum cryptography itself. A detailed elaboration on one crucial conclusion in Sec. IV is presented in the Appendix.

II. DEFINITIONS

Let us first state precisely the definitions of different OTs on which the study in this paper is based. In Ref. [11], where the classical equivalence between these OTs was proven, the definitions of all-or-nothing OT and one-out-of-two OT were summarized as follows:

Definition A: all-or-nothing OT

(A-i) Alice knows one bit b.

(A-ii) Bob gets bit b from Alice with the probability 1/2.

(A-iii) Bob knows whether he got b or not.

(A-iv) Alice does not know whether Bob got b or not.

Definition B: one-out-of-two OT

(B-i) Alice knows two bits b_0 and b_1.

(B-ii) Bob gets bit b_j and not $b_{\bar{j}}$ with $Pr(j=0)=Pr(j=1)=1/2$.

(B-iii) Bob knows which of b_0 or b_1 he got.

(B-iv) Alice does not know which b_j Bob got.

In the Lo's insecurity proof of ideal one-sided two-party quantum secure computations [7], a more rigorous definition of one-out-of-two OT was specifically introduced as follows:

Definition C: rigorous one-out-of-two OT

(C-i) Alice inputs i, which is a pair of messages (m_0, m_1).

(C-ii) Bob inputs $j=0$ or 1.

(C-iii) At the end of the protocol, Bob learns about the message m_j, but not the other message $m_{\bar{j}}$, i.e., the protocol is an ideal one-sided two-party secure computation $f(m_0, m_1, j=0)=m_0$ and $f(m_0, m_1, j=1)=m_1$.

(C-iv) Alice does not know which m_j Bob got.

Meanwhile, the definition of ideal one-sided two-party quantum secure computations used in the Lo's proof reads:

Definition D: ideal one-sided two-party secure computation

Suppose Alice has a private (i.e., secret) input $i \in \{1, 2, \ldots, n\}$ and Bob has a private input $j \in \{1, 2, \ldots, m\}$. Alice helps Bob to compute a prescribed function $f(i, j) \in \{1, 2, \ldots, p\}$ in such a way that, at the end of the protocol:

(a) Bob learns $f(i, j)$ unambiguously;

(b) Alice learns nothing [about j or $f(i, j)$];

(c) Bob knows nothing about i more than what logically follows from the values of j and $f(i, j)$.

Obviously, definition C is a special case of definition D. In Ref. [7] it is proven that any protocol satisfying definition D is insecure. Therefore as a corollary, there should not exist a secure quantum one-out-of-two OT protocol which satisfies definition C rigorously.

III. CLASSICAL EQUIVALENCE

The proof of the classical equivalence between the two flavors of OTs is provided in Ref. [11]. The major part of the proof is the following procedure, showing how secure one-out-of-two OT can be implemented upon secure all-or-nothing OT.

Protocol P:

(1) Alice and Bob agree on a security parameter s;

(2) Alice chooses at random Ks bits $r_1, r_2, \ldots, r_{Ks}$;

(3) For each of these Ks bits Alice uses the all-or-nothing OT protocol to disclose the bit r_k to Bob;

(4) Bob selects $U=\{i_1, i_2, \ldots, i_{\alpha_s}\}$ and $V=\{i_{\alpha_s+1}, i_{\alpha_s+2}, \ldots, i_{2\alpha_s}\}$ where $\alpha_s=Ks/3$ with $U \cap V=\varnothing$ and such that he knows r_{k_l} for each $k_l \in U$;

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

(6) Alice computes $c_0=\oplus_{x \in X} r_x$ and $c_1=\oplus_{y \in Y} r_y$;

(7) Alice returns to Bob $b_0 \oplus c_0$ and $b_1 \oplus c_1$;

(8) Bob computes $\oplus_{u \in U} r_u \in \{c_0, c_1\}$ and uses it to get his secret bit b_j.

IV. NONEQUIVALENCE AT THE QUANTUM LEVEL

The two definitions of one-out-of-two OT (definitions B and C) seem to be consistent with each other, however, here we show that, at the quantum level, if a secure quantum all-or-nothing OT protocol satisfies definition A and can be used as a "black box," a protocol P built upon it via the above procedure does not satisfy definition C rigorously, though it satisfies definition B.

The meaningful deviation from definition C lies in (C-i) and (C-iii). Consider Alice's input i in protocol P. In step (7) of the protocol, we can see that i includes not only the secret bits b_0 and b_1, but also c_0 and c_1. The steps (5) and (6) show that c_0 and c_1 depend not only on Alice's input $r_1, r_2, \ldots, r_{Ks}$, but also on how Bob selects X, Y, U, and V, i.e., they depend on Bob's input j. Therefore, protocol P cannot be viewed as a black box function $f(i(m_0, m_1), j)$, where i and j are the private inputs of Alice and Bob, respectively. Instead, it has the form $f(i(m_0, m_1, j), j)$, where Alice's input i will be varied according to Bob's input j, and its value is not determined until Bob's input has been completed. That is, protocol P does not rigorously satisfy definition C, nor definition D, as the description of the function f is different.

Though the difference seems tiny at first glance, its impact on the security of protocol P at the quantum level is significant. This can be seen from two aspects.

On one hand, protocol P is not covered by the cheating strategy in the Lo's no-go proof of ideal one-sided two-party quantum secure computations [7], since it is not ideal. According to the strategy, Bob can change the value of j from j_1 to j_2 by applying a unitary transformation to his own quantum machine. Therefore he can learn $f(i(m_0, m_1), j_1)$ and $f(i(m_0, m_1), j_2)$ simultaneously without being found by Alice. However, for the function $f(i(m_0, m_1, j), j)$, the value $f(i(m_0, m_1, j_1), j_2)$ is meaningless. Without the help of Alice, Bob cannot change i from $i(m_0, m_1, j_1)$ to $i(m_0, m_1, j_2)$. Hence he cannot learn $f(i(m_0, m_1, j_1), j_1)$ and $f(i(m_0, m_1, j_2), j_2)$ simultaneously by himself. Namely, though the cheating strategy works for any protocol satisfying definition D, it does not work for protocol P. A rigorous elaboration is detailed in the Appendix.

On the other hand, though protocol P remains secure against Lo's cheating, new security problems arise when it is used to build other protocols. As argued in the Introduction of Ref. [7], to ensure that the standard classical reduction can apply to quantum cryptographic protocols, "one must be allowed to use a quantum cryptographic protocol as a 'black box' primitive in building up more sophisticated protocols and to analyze the security of those new protocols with classical probability theory." However, as mentioned above, protocol P cannot be used as such a black box since the sequence of the participants' inputs is important, i.e., we have to deal with the details of the protocol when it is used to build up sophisticated quantum protocols. Therefore its applications in quantum cryptography may not be as powerful as it was expected [8] from a rigorous quantum one-out-of-two OT.

A significant example is that the quantum all-or-nothing OT [12] cannot be used to implement secure QBC with the scenario described in Ref. [14]. The reason lies in that step (2) of the protocol COMMIT in Ref. [14] will become inexecutable, since Alice's input cannot be completed before Bob's input is entered in protocol P. Also, the protocol COMMIT is merely one block of the BC process [15]. It does not

satisfy the rigorous security requirement of BC even if it is made executable. It needs to be repeated many times in parallel to form a full BC protocol, as described in Ref. [15]. However, at the quantum level, this may leave room for the participant to perform quantum collective measurement on the inputs of all these one block BCs together. Then the security of the full protocol cannot be analyzed simply with classical probability theory, since protocol P is not an ideal black box. There may also exist other approaches to build QBC on protocol P. But due to the presence of the MLC no-go theorem, the resultant QBC protocol is inevitably either unbinding or unconcealed. That is, even the protocol COMMIT can be modified to be secure against Alice (e.g., by using protocol P reversely), it may not be secure against Bob since his input will depend on Alice's in this case. In this sense, the classical reduction chain from all-or-nothing OT to BC mentioned in the Introduction is broken in the present quantum case, since protocol P built upon quantum all-or-nothing OT is not a rigorous quantum one-out-of-two OT that can lead to a secure QBC protocol.

V. ORIGIN OF THE NONEQUIVALENCE

It is valuable to dig out the underlying reason why protocol P does not satisfy the rigorous definition C. An illusion is naively aroused that the reason is due to a relaxed definition A of all-or-nothing OT used in the present work. However, this is not really the case. In fact, we never need to deal with the details of the all-or-nothing OT in Sec. IV; we simply use it as a black box. Even when the most rigorous definition of all-or-nothing OT is used, the discussion in that the section is still valid. Thus it is not a matter of the definition that the classical equivalence between the two flavors of OTs cannot be applied to the present quantum case.

The real origin of the nonequivalence may be dug out from a careful comparison between Eqs. (A13) and (A15) in the Appendix. One can see clearly that protocol P will become insecure if there does not exist a system D. That is, if Alice does not introduce the quantum system D in Eq. (A5), protocol P will show no difference from the protocols satisfying definition D. In classical cryptography, Alice surely does not have such a system, and thus the two flavors of OTs are equivalent. While in quantum cryptography, if Alice does not make full use of the computational power but simply executes the protocol with the quantum system A alone, she cannot defeat Bob's cheating. The difference between protocol P and a rigorous one-out-of-two OT can only be manifested when the protocol is indeed executed at the quantum level. In this sense, the underlying origin is the nature of quantum cryptography itself.

VI. SUMMARY

We have shown that though one-out-of-two OT can be built upon all-or-nothing OT in classical cryptography, a protocol P built upon a secure quantum all-or-nothing OT protocol via the same method cannot satisfy the rigorous definition C of quantum one-out-of-two OT. That is, this classical equivalence between these OTs cannot be rigorously applied to quantum cryptography. Therefore there is not any logical conflict between the existence of secure quantum all-or-nothing OT [12] and the MLC no-go theorem of QBC [5,6]. This finding demonstrates intriguingly that reductions and relations between classical cryptographic tasks need careful reexamination in quantum cases.

We thank Hoi-Kwong Lo for valuable discussions. The work was supported by an RGC grant of Hong Kong (Grant No. HKU7045/05P), the URC fund of HKU, the NSFC (Grant No. 10429401), and the Foundation of Zhongshan University Advanced Research Center.

APPENDIX A: DEFEATING THE LO'S CHEATING STRATEGY

Here we elaborate in more detail that protocol P is secure against the cheating strategy in the Lo's no-go proof of ideal one-sided two-party quantum secure computations [7]. For convenience, let us first recall the Lo's cheating strategy in more detail. According to Sec. III of Ref. [7], in any protocol satisfying definition D, Alice and Bob's actions on their quantum machines can be summarized as an overall unitary transformation U applied to the initial state $|u\rangle_{in} \in H_A \otimes H_B$, i.e.,

$$|u\rangle_{fin} = U|u\rangle_{in}. \tag{A1}$$

When both parties are honest, $|u^h\rangle_{in} = |i\rangle_A \otimes |j\rangle_B$ and

$$|u^h\rangle_{fin} = |v_{ij}\rangle \equiv U(|i\rangle_A \otimes |j\rangle_B). \tag{A2}$$

Therefore the density matrix that Bob has at the end of protocol is

$$\rho^{i,j} = \mathrm{Tr}_A |v_{ij}\rangle\langle v_{ij}|. \tag{A3}$$

Bob can cheat in this protocol, because given $j_1, j_2 \in \{1,2,\ldots,m\}$, there exists a unitary transformation U^{j_1,j_2} such that

$$U^{j_1,j_2}\rho^{i,j_1}(U^{j_1,j_2})^{-1} = \rho^{i,j_2} \tag{A4}$$

for all i. It means that Bob can change the value of j from j_1 to j_2 by applying a unitary transformation independent of i to the state of his quantum machine. This Eq. (A4) may be derived as follows [7].

Alice may entangle the state of her quantum machine A with her quantum dice D and prepares the initial state

$$\frac{1}{\sqrt{n}}\sum_i |i\rangle_D \otimes |i\rangle_A. \tag{A5}$$

She keeps D for herself and uses the second register A to execute the protocol. Supposing that Bob's input is j_1, the initial state is

$$|u'\rangle_{in} = \frac{1}{\sqrt{n}}\sum_i |i\rangle_D \otimes |i\rangle_A \otimes |j_1\rangle_B. \tag{A6}$$

At the end of the protocol, it follows from Eqs. (A1) and (A6) that the total wave function of the combined system D, A, and B is

$$|v_{j_1}\rangle_{in} = \frac{1}{\sqrt{n}}\sum_i |i\rangle_D \otimes U(|i\rangle_A \otimes |j_1\rangle_B). \quad \text{(A7)}$$

Similarly, if Bob's input is j_2, the total wave function at the end will be

$$|v_{j_2}\rangle_{in} = \frac{1}{\sqrt{n}}\sum_i |i\rangle_D \otimes U(|i\rangle_A \otimes |j_2\rangle_B). \quad \text{(A8)}$$

Due to the requirement (b) in definition D, the reduced density matrices in Alice's hand for the two cases $j=j_1$ and $j=j_2$ must be the same, i.e.,

$$\rho_{j_1}^{Alice} = \mathrm{Tr}_B|v_{j_1}\rangle\langle v_{j_1}| = \mathrm{Tr}_B|v_{j_2}\rangle\langle v_{j_2}| = \rho_{j_2}^{Alice}. \quad \text{(A9)}$$

Equivalently, $|v_{j_1}\rangle$ and $|v_{j_2}\rangle$ have the same Schmidt decomposition

$$|v_{j_1}\rangle = \sum_k a_k|\alpha_k\rangle_{AD} \otimes |\beta_k\rangle_B \quad \text{(A10)}$$

and

$$|v_{j_2}\rangle = \sum_k a_k|\alpha_k\rangle_{AD} \otimes |\beta'_k\rangle_B. \quad \text{(A11)}$$

Now consider the unitary transformation U^{j_1,j_2} that rotates $|\beta_k\rangle_B$ to $|\beta'_k\rangle_B$. Notice that it acts on H_B alone and yet, as can be seen from Eqs. (A10) and (A11), it rotates $|v_{j_1}\rangle$ to $|v_{j_2}\rangle$, i.e.,

$$|v_{j_2}\rangle = U^{j_1,j_2}|v_{j_1}\rangle. \quad \text{(A12)}$$

Since

$${}_D\langle i|v_j\rangle = \frac{1}{\sqrt{n}}|v_{ij}\rangle \quad \text{(A13)}$$

[see Eqs. (A2), (A7), and (A8)], by multiplying Eq. (A12) by ${}_D\langle i|$ on the left, one finds that

$$|v_{ij_2}\rangle = U^{j_1,j_2}|v_{ij_1}\rangle. \quad \text{(A14)}$$

Taking the trace of $|v_{ij_2}\rangle\langle v_{ij_2}|$ over H_A and using Eq. (A14), Eq. (A4) can be obtained.

Note that all these equations are just those presented in the Lo's proof [7]. We now consider protocol P, where Alice's input i is dependent of Bob's input j. In the above proof, all i in the equations should be replaced by $i(j)$ from the very beginning. Consequently, Eq. (A13) becomes

$${}_D\langle i(j)|v_j\rangle = \frac{1}{\sqrt{n}}|v_{i(j)j}\rangle. \quad \text{(A15)}$$

In this case multiplying Eq. (A12) by ${}_D\langle i_2|$ ($i_2 \equiv i(j_2)$ for short) on the left cannot give Eq. (A14) any more. Instead, the result is

$$|v_{i_2j_2}\rangle = U^{j_1,j_2}U^{i_1,i_2}|v_{i_1j_1}\rangle, \quad \text{(A16)}$$

where $U^{i_1,i_2} \equiv {}_D|i_2\rangle\langle i_1|_D$. Then Eq. (A4) is replaced by

$$U^{j_1,j_2}U^{i_1,i_2}\rho^{i_1,j_1}(U^{j_1,j_2}U^{i_1,i_2})^{-1} = \rho^{i_2,j_2}. \quad \text{(A17)}$$

Note that U^{i_1,i_2} is the unitary operation on Alice's side. This implies that without Alice's help, Bob cannot change the density matrix he has from ρ^{i_1,j_1} to ρ^{i_2,j_2}. That is why Bob's cheating strategy fails in protocol P.

[1] S. Wiesner, SIGACT News **15**, 78 (1983).
[2] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing* (IEEE, New York, 1984), p. 175.
[3] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[4] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[5] D. Mayers, Phys. Rev. Lett. **78**, 3414 (1997).
[6] H.-K. Lo and H. F. Chau, Phys. Rev. Lett. **78**, 3410 (1997).
[7] H.-K. Lo, Phys. Rev. A **56**, 1154 (1997).
[8] J. Kilian, in *Proceedings of 1988 ACM Annual Symposium on Theory of Computing* (ACM, New York, 1988), pp. 20.
[9] M. Rabin, technical report TR-81, Aiken Computation Laboratory, Harvard University, 1981.
[10] S. Even, O. Goldreich, and A. Lempel, *Advances in Cryptology: Proceedings of Crypto '82*, edited by D. Chaum, R. L. Rivest, and A. T. Sherman (Plenum, New York, 1982), pp. 205.
[11] C. Crepeau, in *Advances in Cryptology: Proceedings of Crypto '87*, edited by C. Pomerance (Springer-Verlag, Berlin, 1988), Vol. 293, pp. 350.
[12] G. P. He and Z. D. Wang, Phys. Rev. A **73**, 012331 (2006).
[13] A. Kent, Phys. Rev. Lett. **90**, 237901 (2003).
[14] T. Short, N. Gisin, and S. Popescu, e-print quant-ph/0504134.
[15] H. Buhrman, M. Christandl, F. Unger, S. Wehner, and A. Winter, e-print quant-ph/0504133.