Can relativistic bit commitment lead to secure quantum oblivious transfer?

Guang Ping He

School of Physics and Engineering, Sun Yat-sen University, Guangzhou 510275, P.R. China

1 Introduction

Besides the well-known quantum key distribution (QKD) [1], bit commitment (BC) and oblivious transfer (OT) are also essential cryptographic primitives. It was shown that OT is the building block of multi-party secure computations and more complicated “post-cold-war era” multi-party cryptographic protocols [2], and quantum OT (QOT) can be obtained basing on quantum BC (QBC) [3]. But it is widely accepted that unconditionally secure QBC is impossible within the quantum framework [4–29]. This result, known as the Mayers-Lo-Chau (MLC) no-go theorem, is considered as putting a serious drawback on quantum cryptography. Obviously, it indicates that QOT built upon QBC cannot be secure either. This stimulated the emergence of many other no-go proofs on quantum two-party secure computations including QOT [30–38].

Nevertheless, Kent showed that BC can be unconditionally secure under relativistic settings [39–42]. Recently, these relativistic BC protocols were implemented experimentally [43,44]. Also, there were many proposals on “practical” QBC, which are secure if the participants are limited by some experimental constraints, such as individual measurements or limited coherent measurements, misaligned reference frames, unstability of particles, Gaussian operations with non-Gaussian states, etc. (see the introduction of reference [45] for a detailed list).

Therefore, it is natural to ask whether these BC protocols can lead to secure QOT. That is, suppose that any setting or constraint required to guarantee the security of the above BC protocols is satisfied, so that the participants can use them as a secure “black box” without caring the internal details of these protocols. Then we put no constraint (except those forbidden by fundamental physics laws) on the participants’ behaviors in other steps of the BC-based QOT. Note that in this scenario, it may not be straight-forward to apply some common methods adopted for proving the impossibility of QBC and related no-go theorems, e.g., replacing any protocol with an ideal model which contains quantum communications and unitary transformations only. This is because now there is the secure “black box” QBC stands in the middle of the QOT process, so that some cheating strategies may be interrupted at this stage. Thus it is important to reexamine whether the no-go proofs of QOT still apply, and if yes, how the cheating is performed.

In this paper, the answer is twofold. On one hand, we will provide a cheating strategy in details, showing that some of the no-go proofs [31–37] remain valid even if QOT is based on secure BC. On the other hand, we found that some other no-go proofs claiming that a dishonest receiver can always decode all transferred bits simultaneously with reliability 100% become invalid in this scenario, because their models of cryptographic protocols are too ideal to cover such a BC-based QOT.
a piece of evidence. Later, in the unveil phase, Charlie announces the value of x, and Diana checks it with the evidence. An unconditionally secure BC protocol needs to be both binding (i.e., Charlie cannot change the value of x after the commit phase) and concealing (Diana cannot know x before the unveil phase) without relying on any computational assumption.

In the quantum case, Charlie’s input can be more complicated. Besides the two classical values 0 and 1, he can commit a quantum superposition or mixture of the states corresponding to x close to 0 by increasing some security parameters of the BC protocol and keeps C to himself. When it is time to unveil, Charlie commits to a probabilistic value distribution (a BC protocol can force Charlie to commit to a probability distribution (p0, p1) which cannot be changed after the commit phase, and (p0 + p1) − 1 can be made arbitrarily close to 0 by increasing some security parameters of the protocol, then it is still considered as unconditionally secure. On the other hand, if a protocol can further force Charlie to commit to a particular classical x, i.e., besides p0 + p1 → 1, both p0 and p1 can only take the values 0 or 1 instead of any value in between, then it is called a bit commitment with a certificate of classicality (BCCC). All the above mentioned BC protocols are not BCCC, and unconditionally secure BCCC seems impossible. Therefore, in the following when speaking of secure BC, we refer to the non-BCCC ones only, except where noted.

OT is also a two-party cryptography. There are two major types of OT in literature. Using Crépeau’s description, they are defined as follows.

**Definition A: All-or-nothing OT (AoN 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 (1-2 OT)**

(B-i) Alice knows two bits b0 and b1.

(B-ii) Bob gets bit b1 and not b_j with Pr(j = 0) = Pr(j = 1) = 1/2.

(B-iii) Bob knows which of b0 or b1 he got.

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

We will study BC-based AoN OT first, and come back to 1-2 OT later.

### 3 Insecurity

According to Yao [3], AoN QOT can be built upon BC as follows.

The BC-based AoN QOT protocol:

1. Let |0⟩ and |1⟩ be two orthogonal states of a qubit, and define |0⟩ ≡ (|0⟩ + |1⟩)/√2, |1⟩ ≡ (|0⟩ − |1⟩)/√2. That is, the state of a qubit is denoted as |a⟩ = a|0⟩ + b|1⟩, where a and b are the basis and y, distinguishes the two states in the same basis. For i = 1, ..., n, Alice randomly picks a_i, g_i ∈ {0, 1} and sends Bob a qubit φ_i = a_i|0⟩ + b_i|1⟩ in the set |a_i⟩. Then Charlie commits (b_i, h_i) to Alice using the BC protocol.

2. Alice randomly picks a subset R ⊆ {1, ..., n} and tests Bob’s commitment at positions in R. If any i ∈ R reveals a_i = b_i and g_i ≠ h_i, then Alice stops the protocol; otherwise, the test result is accepted.

3. Alice announces the bases a_i (i = 1, ..., n). Let T_k = 0 be the set of all 1 ≤ i ≤ n with a_i = b_i, and T_1 be the set of all 1 ≤ i ≤ n with a_i ≠ b_i. Bob chooses I_0 ⊂ T_0 − R, I_1 ⊂ T_1 − R with |I_0| = |I_1| = 0.24n, and sets {j_0, j_1} = {j_0, j_1} if {j_0, j_1} = {j_0, j_1} at random, then sends {j_0, j_1} to Alice.

4. Alice picks a random s ∈ {0, 1}, and sends s, β_s = b ⊕ g_i to Bob. Bob computes b = β_s ⊕ h_i if j_s = I_0; otherwise does nothing.

Notes: Now suppose that the BC protocol used in this QOT is secure. That is, no matter we use relativistic BC [39–42], or “practical” QBC protocols listed in the introduction of references [45], we assume that all the security requirements (e.g., relativistic settings or experimental limitations) are already met, so that Bob does not have unlimited computational power to cheat within the BC stage. In this case, the validity of the no-go proofs of QOT [30–38] cannot be taken for granted, because all these proofs were derived without implying any limitation on the computational power of the cheater.

Intriguingly, the conclusions of some of the no-go proofs [31–37] remain valid, that unconditionally secure QOT is still impossible in this case. The key reason is that secure BC, being not a BCCC, cannot avoid the participant keeping the commitment at the quantum level instead of taking a fixed classical value. Kent [39] briefly mentioned that it will allow more general coherent quantum attacks to be used on schemes of which BC is a sub-protocol, but no details of the cheating strategy was given. Here we will elaborate how Bob can make use of this feature to break the BC-based QOT protocol.
For each \( \phi_i \) \((i = 1, \ldots, n)\), a dishonest Bob does not pick a classical bit and measure it in step (II). Instead, he introduces two ancillary qubit systems \( B_i \) and \( H_i \) as the registers for the bits \( b_i \) and \( h_i \), and prepares their initial states as \( |B_i\rangle = (|0\rangle_B + |1\rangle_B)/\sqrt{2} \) and \( |H_i\rangle = |0\rangle_H \), respectively. Here \(|0\rangle \) and \(|1\rangle \) are orthogonal. Then he applies the unitary transformation

\[
U_1 \equiv |0\rangle_B \otimes |0\rangle_H \otimes |\phi_i \rangle \otimes |0\rangle \otimes I_H
+ |0\rangle_B \otimes |0\rangle_H \otimes |1\rangle \otimes \sigma_H^{(x)}
+ |1\rangle_B \otimes |1\rangle_H \otimes |0\rangle \otimes I_H
+ |1\rangle_B \otimes |1\rangle_H \otimes |1\rangle \otimes \sigma_H^{(y)}
\]

(2)
on the system \( B_i \otimes \phi_i \otimes H_i \). Here \( I_H \) and \( \sigma_H^{(x)} \) are the identity operator and Pauli matrix of system \( H_i \) that satisfy \( I_H |0\rangle_H = |0\rangle_H \) and \( \sigma_H^{(x)} |0\rangle_H = |1\rangle_H \), respectively. The effect of \( U_1 \) is like running a quantum computer program that if \( |B_i\rangle = |0\rangle_B \), then measures qubit \( \phi_i \) in the basis \( b_i = 0 \), and stores the result \( h_i \) in system \( H_i \). It differs from a classical program with the same function as no destructive measurement is really performed, since \( U_1 \) is not a projective operator. Consequently, the bits \( b_i \) and \( h_i \) are kept at the quantum level instead of being collapsed to classical values.

Bob then commits \((b_i, h_i)\) to Alice at the quantum level. This can always be done in a BC protocol which does not satisfy the definition of BCCC. For example, to commit \( b_i \), Bob further introduces two ancillary systems \( E \) and \( \Psi \) and prepares the initial state as

\[
|E \otimes \Psi\rangle_0 = |\psi_0\rangle_E \otimes |\phi_0\rangle_\Psi
\]

(3)
Let \( U_{E \otimes \Psi} \) be a unitary transformation on \( E \otimes \Psi \) satisfying \( U_{E \otimes \Psi} |\psi_0\rangle_E \otimes |\phi_0\rangle_\Psi = |\psi_1\rangle_E \otimes |\phi_1\rangle_\Psi \). Here \(|\psi_0\rangle_\Psi\), \(|\phi_0\rangle_\Psi\), \(|\psi_1\rangle_\Psi\), and \(|\phi_1\rangle_\Psi\) have the same meanings as in equation (1), and \(|\psi_0\rangle_E\), \(|\psi_1\rangle_E\), \(|\phi_0\rangle_E\), and \(|\phi_1\rangle_E\) are orthogonal. Bob applies the unitary transformation

\[
U_2 \equiv |0\rangle_B \otimes I_{E \otimes \Psi} \otimes |1\rangle_B \otimes |I_{E \otimes \Psi}\rangle
\]

(4)
on system \( B_i \otimes E \otimes \Psi \), where \( I_{E \otimes \Psi} \) is the identity operator of system \( E \otimes \Psi \). As a result, we can see that the final state of \( B_i \otimes \phi_i \otimes H_i \otimes E \otimes \Psi \) will be very similar to equation (1) if we view \( B_i \otimes \phi_i \otimes H_i \otimes E \) as system \( C \). Then Bob can follow the process after equation (1) (note that now Bob plays the role of Charlie) to complete the commitment of \( b_i \) without collapsing it to a classical value. He can do the same to \( h_i \).

Back to step (III) of the QOT protocol. Whenever \((b_i, h_i)\) \((i \in R)\) are picked to test the commitment, Bob simply unveils them honestly. Since these \((b_i, h_i)\) will no longer be useful in the remaining steps of the protocol, it does not hurt Bob's cheating. Note that the rest \((b_i, h_i)\) \((i \notin R)\) are still kept at the quantum level. After Alice announced all bases \( a_i \) \((i = 1, \ldots, n)\) in step (IV), Bob introduces a single global control qubit \( S' \) for all \( i \), initialized in the state \(|S'\rangle = (|0\rangle_S + |1\rangle_S)/\sqrt{2} \), and yet another ancillary system \( \Gamma_i \) for each \( i \in T_0 \cup T_1 \) initialized in the state \(|\Gamma_i\rangle = |0\rangle_{\Gamma_i} \). Then he applies the unitary transformation

\[
U_3 \equiv |0\rangle_S \otimes (|0\rangle_B \otimes |a_i\rangle_B \otimes I_{\Gamma_i})
+ |0\rangle_S \otimes (|0\rangle_B \otimes \overline{|a_i\rangle_B \otimes I_{\Gamma_i}})
+ |1\rangle_S \otimes (|1\rangle_B \otimes |a_i\rangle_B \otimes \sigma_{\Gamma_i}^{(x)})
+ |1\rangle_S \otimes (|1\rangle_B \otimes \overline{|a_i\rangle_B \otimes I_{\Gamma_i}})
\]

(5)
on the incremented system \( S' \otimes B_i \otimes \Gamma_i \). Here \( I_{\Gamma_i} \) and \( \sigma_{\Gamma_i}^{(x)} \) are the identity operator and Pauli matrix of system \( \Gamma_i \) that satisfies \( I_{\Gamma_i} |0\rangle_{\Gamma_i} = |0\rangle_{\Gamma_i} \) and \( \sigma_{\Gamma_i}^{(x)} |0\rangle_{\Gamma_i} = |1\rangle_{\Gamma_i} \), respectively. The effect of \( U_3 \) is to compare \( a_i \) with \( b_i \) and store the result \((a_i \neq b_i) \iff s' = 1\) in \( \Gamma_i \). Then Bob measures all \( \Gamma_i \) \((i \in T_0 \cup T_1 \) \) in the basis \(|\{0\}_{\Gamma_i}, |1\rangle_{\Gamma_i}\rangle \), takes \( T_0 (T_1) \) as the set of all \( i \leq l \leq n \) with \(|\Gamma_i\rangle = |0\rangle_{\Gamma_i} \) \((|\Gamma_i\rangle = |1\rangle_{\Gamma_i}\rangle \) instead of how they were defined in step (IV), and always sets \( J_0 \equiv T_0 - R, J_1 \equiv T_1 - R \) to finish the rest parts of the QOT protocol.

With this method, the relationship between \( J_0, J_1 \) and \( J_0, J_1 \) are kept at the quantum level. Since \( J_0 (J_1) \) denotes the set corresponding to \( a_i = b_i \) \((a_i \neq b_i) \), we can see that \( U_3 \) makes \( J_0 = J_0, J_1 = J_1 \) when \( s' = 0 \), while \( J_0 = J_1 \) \( \iff s' = 1 \). As \( S' \) was initialized as \(|S'\rangle = (|0\rangle_S + |1\rangle_S)/\sqrt{2} \), the actual result of step (IV) can be described by the entangled state

\[
|\psi_b\rangle = (|0\rangle_S \otimes |J_0 = J_0 \land J_1 = J_1\rangle)
+ |1\rangle_S \otimes |J_0 = J_1 \land J_1 = J_0\rangle)/\sqrt{2}
\]

(6)
Here \( E_i' \) stands for all the ancillary systems Bob introduced in the process of committing \((b_i, h_i)\). \(|J_0 = J_0 \land J_1 = J_1\rangle \) denotes the state of system \( B_i \otimes \phi_i \otimes H_i \otimes E_i' \), in which the subsystems \( B_i \) and \( H_i \) contain the correct \( b_i \) and \( h_i \) corresponding to \( J_0 = J_0 \land J_1 = J_1 \). The meaning of \(|J_0 = J_1 \land J_1 = J_0\rangle \) is also similar.

After Alice announced \( s \) and \( b \) in step (V), the systems under Bob's possession can be viewed as

\[
|\psi_b\rangle = (|s\rangle_S \otimes |J_s = J_0 \rangle \land |\overline{s}\rangle_S \otimes \overline{|\text{fail}|})/\sqrt{2}
\]

(7)
It means that if Bob measures system \( S' \) in the basis \(|0\rangle_S \land |1\rangle_S\rangle \) and the result \(|s\rangle_S \) satisfies \( s' = s \), then he is able to measure the rest systems and get all the correct \( h_i \) to decode the secret bit \( b \) unambiguously; else if the result satisfies \( s' \neq s \), then he knows that he fails to decode \( b \). Now the most tricky part is, as the value of \( s' \) was kept at the quantum level before system \( S' \) is measured, at this stage a dishonest Bob can choose not to measure \( S' \) in the basis \(|0\rangle_S \land |1\rangle_S\rangle \). Instead, by denoting \(|b\rangle \equiv |s\rangle_S \otimes |J_s = J_0\rangle \land |\overline{s}\rangle_S \otimes \overline{|\text{fail}|} \), equation (7) can be treated as \(|\psi_b\rangle = (|b\rangle + |\overline{b}\rangle)/\sqrt{2} \), where \(|b\rangle \equiv (1 \ 0 \ 0 \ 1)^T, |b\rangle \equiv (0 \ 1 \ 0 \ 1)^T, \text{ and } |\overline{s}\rangle \equiv (0 \ 0 \ 0 \ 1)^T \) are mutually orthogonal. Then according to equation (33) of reference [33], Bob can distinguish them using the positive
This allows Bob’s decoded $b$ to match Alice’s actual input with reliability $(1 + \sqrt{3}/2)/2$ \cite{33}. On the contrary, when Bob executes the QOT protocol honestly, in 1/2 of the cases he can decode $b$ with reliability 100%; in the rest 1/2 cases he fails to decode $b$, he can guess the value randomly, which results in a reliability of 50%. Thus the average reliability in the honest case is $100%/2 + 50%/2 = 75% < (1 + \sqrt{3}/2)/2$. Note that in the above dishonest strategy, in any case Bob can never decode $b$ with reliability 100%. Therefore it is debatable whether it can be considered as a successful cheating, as the strategy does not even accomplish what an honest Bob can do. That is why it is called honest-but-curious adversary \cite{34,35}, i.e., in some sense it may still be regarded as honest behavior instead of full cheating. Nevertheless, it provides Bob with the freedom to choose between accomplishing the original goal of QOT or achieving a higher average reliability, which could leave rooms for potential problems when building even more complicated cryptographic protocols upon such a BC-based QOT.

The above cheating strategy is basically the same we proposed in Section 5 of reference \cite{45}, which was applied to show why the specific QBC protocol in the same reference cannot lead to secure QOT. But here we can see that its power is not limited to the QBC protocol in reference \cite{45}. Especially, Bob’s steps related with equations (3) and (4) will always be valid as long as the BC protocol used in QOT is not a BCCC, as they do not involve the details of the BC process. Thus we reach a much general result, that any BC (except BCCC) cannot lead to unconditionally secure AoN QOT using Yao’s method \cite{3}. It covers not only unconditionally secure QBC (regardless whether it exists or not), but also relativistic BC (both classical \cite{39,40} and quantum ones \cite{41,42}) and practically secure QBC (e.g., those listed in the introduction of reference \cite{45}), even if all the requirements for them to be secure are already met. In this sense, QOT is more difficult than QBC, in contrast to the classical relationship that OT and BC are equivalent.

This result shows that the original security proof of BC-based QOT \cite{3} is not general. The proof claimed that as long as the BC protocol is unconditionally secure, then the QOT protocol built upon it will be unconditionally secure too. But now we can see that it may still be valid for BCCC-based QOT, but fails to cover all unconditionally secure BC.

Now consider 1-2 OT. It can be built upon BC in much the same way as the above BC-based AoN QOT protocol, except that step (V) should be modified into:

(V') Alice sends $\beta_0 = \sum_{i \in J_0} g_i$ and $\beta_1 = \sum_{i \in J_1} g_i$, to Bob. Bob computes $b_0 = \sum_{i \in J_0} h_i$ if $J_0 = I_0$, or $b_1 = \sum_{i \in J_1} h_i$ if $J_1 = I_0$.

Bob can also apply the above cheating strategy, so that the result of step (IV) is still described by equation (6). After Alice announced $\beta_0$ and $\beta_1$ in step (V’), if Bob wants to decode $b_0$, he can treat the right-hand side of equation (6) as

$$|\Phi_b\rangle = (|0\rangle_{SR} \otimes |J_0 = I_0\rangle + |1\rangle_{SR} \otimes |\text{fail}\rangle)/\sqrt{2},$$

else if he wants to decode $b_1$, he can treat it as

$$|\Phi_b\rangle = (|0\rangle_{SR} \otimes |\text{fail}\rangle + |1\rangle_{SR} \otimes |J_1 = I_0\rangle)/\sqrt{2}. $$

Comparing these two equations with equation (7), we can see that they both have the form $|\Phi_b\rangle = (|b\rangle + |\bar{b}\rangle)/\sqrt{2}$. Thus Bob can still apply the POVM described by equation (8) to decode the bit he wants. Consequently, he can decode one of $b_0$ and $b_1$ at his choice with reliability $(1 + \sqrt{3}/2)/2$. Again, despite that the value is higher than the average reliability of the honest behavior, in the current case Bob can never decode the bit with reliability 100%. Thus it still belongs to the honest-but-curious adversaries. Also, it is important to note that the POVM $(E_0, I - E_0)$ is a two-value measurement that can obtain one bit of information only, and the POVMs corresponding to equation (9) and equation (10) are not the same. Therefore Bob can pick only one of them to increase the average reliability of one of $b_0$ and $b_1$, instead of decoding both bits simultaneously.

From the above cheating strategies, we can see that Bob’s key idea is to keep introducing quantum entanglement to the system, which enables him to keep more and more data at the quantum level, so that he can have the freedom on choosing different measurements at a later time. This gives yet another example showing the power of entanglement in quantum cryptography.

4 Security

The above honest-but-curious adversaries indicate that the BC-based QOT protocol is not unconditionally secure, which is in agreement with the conclusion of the no-go proofs of QOT \cite{31–37}. Nevertheless, we will show below that this protocol is secure against the cheating strategy in other no-go proofs \cite{30,38}.

In Lo’s no-go proof \cite{30}, the following definition of 1-2 OT was proposed.

Definition C: Lo’s 1-2 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 $f(m_0, m_{\bar{j}}, j = 1) = m_{\bar{j}}$.

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

It was introduced as a special case of the ideal one-sided two-party quantum secure computations, defined in Lo’s proof as follows.
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 $f(i, j)$.

Lo’s proof [30] showed that any protocol satisfying Definition D is insecure, because Bob can always learn all $f(i, j)$ ($j \in \{1, 2, \ldots, m\}$). As a corollary, secure 1-2 OT satisfying Definition C is impossible, as Bob can always learn both $m_0$ and $m_1$.

This result is surprising. As shown in the previous section, other no-go proofs [31–37] claimed that QOT is insecure, merely because Bob can increase the average reliability of the decoded value of one of $m_0$ and $m_1$. It is never indicated in references [31–37] that he can decode both of them simultaneously. Thus the cheating strategy in Lo’s proof [30] seems more powerful.

However, it will be shown below that Lo’s proof is not sufficiently general to cover all kinds of QOT. We must notice that Definition C is not rigorously equivalent to Definition B. An important feature of Definition C is that all Alice’s (Bob’s) input to the entire protocol is merely $I \supset i$ (or $J \supset j$), and $I$, $J$ are independent of each other. But in general, seldom any protocol satisfies these requirement. That is, let us denote all Alice’s (Bob’s) input to a protocol as $I$ ($J$). In Definition C there is $I \supset i$, $J \supset j$, and $I$, $J$ are independent. But most existing quantum cryptographic protocols generally have $I \supset i$, $J \supset j$ and $I$, $J$ are dependent of each other.

For example, in the well-known Bennett-Brassard 1984 (BB84) QKD protocol [1], though the aim of Alice and Bob is to share a secret key $k$, the protocol cannot be modeled as a simple box to which Alice inputs $k$, then Bob gets the output $k$. Instead, more inputs of both participants have to be involved. Alice should first input some quantum states (denoted as input $i_1$), and Bob inputs and announces his measurement bases (input $j_1$). Then Alice tells Bob which bases are correct (input $i_2$), followed by a security check in which Bob reveals some measurement results (input $j_2$), and Alice verifies whether these results are correct or not (input $i_3$). Alice also reveals some results for Bob to verify … Finally they obtain $k$ from the remaining unannounced measurement results. Obviously Alice cannot determine $i_2$ without knowing $j_1$. Bob’s $j_2$ will be affected by Alice’s $i_1$, …, the final key $k$ is also affected by the $i$’s and $j$’s. Thus we see that in the BB84 protocol, the inputs $I = \{i_1, i_2, \ldots\}$ and $J = \{j_1, j_2, \ldots\}$ are dependent of each other. For an eavesdropper, even though parts of $I$ and $J$ are revealed, it is still insufficient to decode $k$.

This is also the case for OT. Alice and Bob generally need to send quantum states, perform operations and exchanges lots of information throughout the entire protocol.

All these {e.g., Alice’s $(a_1, g_1)$, $R$, $\beta_0$, $\beta_1$ and Bob’s $(b_1, h_1)$, $(j_0, j_1)$} in the protocol in Sect. 3 should be treated as parts of their inputs. Consequently, there is $I \supset i$ and $J \supset j$. Definition B requires that Alice has zero knowledge about $j$. But it does not necessarily imply that she has zero knowledge about $J$. Therefore $I$ and $J$ can be dependent of each other. Indeed, step (V‘) of the BC-based 1-2 QOT protocol in Section 3 clearly shows that $I$ includes not only the secret bits $b_0$ and $b_1$, but also depends on how Bob selects $J_0$ and $J_1$ in step (IV). Meanwhile, Bob’s announcing $J_0$ and $J_1$ does not necessarily reveal his choice of $j$. Therefore, comparing with Definitions C and D, the BC-based 1-2 QOT protocol cannot be viewed as an ideal 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’ 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, BC-based 1-2 QOT does not satisfy Definition C.

With this feature, the cheating strategy in Lo’s proof can be defeated, as it was pointed out in reference [48] which will be reviewed below. According to Lo’s strategy, Bob can cheat in 1-2 OT satisfying Definition C, because he can change the value of $j$ from $j_1$ to $j_2$ by applying a unitary transformation to his own quantum machine alone. This enables him to 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, in a protocol described by the function $f(I(m_0, m_1, J), J)$, a value in the form $f(I(m_0, m_1, J), J)$ (with $J(k)$ denoting Bob’s input corresponding to $j_k$) will be 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. Thus the BC-based 1-2 QOT protocol is immune to this cheating.

Now we prove it in a more rigorous mathematical form, following the procedure in the appendix of reference [48]. According to the cheating strategy in Lo’s proof as shown in Section III of reference [30], 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.

$$|u\rangle_{fin} = U |u\rangle_{in}. \quad (11)$$

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

$$|u^{h}\rangle_{fin} = |v_{ij}\rangle \equiv U (|i\rangle_A \otimes |j\rangle_B). \quad (12)$$

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

$$\rho^{j_2} = Tr_A |v_{ij}\rangle \langle v_{ij}|. \quad (13)$$

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

$$U^{j_1, j_2} \rho^{j_1} (U^{j_1, j_2})^{-1} = \rho^{j_2} \quad (14)$$

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 equation is derived as follows [30].

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

$$\frac{1}{\sqrt{n}} \sum_i |i\rangle_D \otimes |i\rangle_A. \quad (15)$$

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

$$|u\rangle_{in} = \frac{1}{\sqrt{n}} \sum_i |i\rangle_D \otimes |i\rangle_A \otimes |j_1\rangle_B. \quad (16)$$

At the end of the protocol, it follows from equations (11) and (16) that the total wave function of the combined system $D, A,$ and $B$ is

$$|v_{j_1}\rangle_{in} = \frac{1}{\sqrt{n}} \sum_i |i\rangle_D \otimes U(|i\rangle_A \otimes |j_1\rangle_B). \quad (17)$$

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

$$|v_{j_2}\rangle_{in} = \frac{1}{\sqrt{n}} \sum_i |i\rangle_D \otimes U(|i\rangle_A \otimes |j_2\rangle_B). \quad (18)$$

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.,

$$\rho_{j_1}^{Alice} = \text{Tr}_B |v_{j_1}\rangle \langle v_{j_1}| = \text{Tr}_B |v_{j_2}\rangle \langle v_{j_2}| = \rho_{j_2}^{Alice}. \quad (19)$$

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

$$|v_{j_1}\rangle = \sum_k a_k |\alpha_k\rangle_A \otimes |\beta_k\rangle_B \quad (20)$$

and

$$|v_{j_2}\rangle = \sum_k a_k |\alpha_k\rangle_A \otimes |\beta_k\rangle_B. \quad (21)$$

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 equations (20) and (21), it rotates $|v_{j_1}\rangle$ to $|v_{j_2}\rangle$, i.e.

$$|v_{j_2}\rangle = U^{j_1,j_2} |v_{j_1}\rangle. \quad (22)$$

Since

$$D \langle i | v_j \rangle = \frac{1}{\sqrt{n}} |v_{ij}\rangle \quad (23)$$

(see Eqs. (12), (17), and (18)), by multiplying equation (22) by $D \langle i |$ on the left, one finds that

$$|v_{ij}\rangle = U^{j_1,j_2} |v_{ij'}\rangle. \quad (24)$$

Taking the trace of $|v_{ij}\rangle \langle v_{ij}|$ over $H_A$ and using equation (24), equation (14) can be obtained.

Equations (11)–(24) are exactly those presented in Lo’s proof [30]. We now consider the BC-based 1-2 QOT protocol. Since it has the feature that 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, equation (23) becomes

$$D \langle I(J) | v_j \rangle = \frac{1}{\sqrt{n}} |v_{IJ}\rangle. \quad (25)$$

In this case, multiplying equation (22) by $D \langle I(2) | (I(2) \equiv I(J(2))$ for short) on the left cannot give equation (24) any more. Instead, the result is

$$|v_{IJ}\rangle = U^{I(1),J(2)} U^{I(1),J(2)} |v_{IJ(1)}\rangle, \quad (26)$$

where $U^{I(1),J(2)} \equiv D \langle I(2) | \langle I(1) |_D$. Then equation (14) is replaced by

$$U^{I(1),J(2)} U^{I(1),J(2)} \rho^{I(1),J(1)} (U^{I(1),J(2)} U^{I(1),J(2)})^{-1} = \rho^{I(2),J(2)}. \quad (27)$$

Note that $U^{I(1),J(2)}$ is the unitary operation on Alice’s side. This implies that without Alice’s help, Bob cannot change the density matrix he has from $\rho^{I(1),J(1)}$ to $\rho^{I(2),J(2)}$. That is why Bob’s cheating strategy fails.

In brief, Lo’s no-go proof on ideal one-sided two-party secure computations [30] cannot cover the above BC-based 1-2 QOT, because the proof studied merely the protocols in which the inputs of the participants are independent. As we mentioned, even the BB84 protocol does not satisfy this requirement, while it can still be used as a black box to build more sophisticated protocols, e.g., quantum secret sharing. Thus we see that black box protocols do not necessarily require independent inputs of the participants. The model used in Lo’s proof is too ideal, so that many useful protocols in quantum cryptography are not covered.

Similarly, a recent no-go proof on two-sided two-party secure computations [38] is also based on a model of protocols with independent inputs. Moreover, the proof contains a logical loophole on the use of the security definition [49]. Therefore its conclusion is not sufficiently general either.

5 Summary and discussions

We elaborated how Bob can make use of quantum entanglement to break the above BC-based QOT and achieve a higher average reliability of the decoded value of the transferred bit, even under certain practical settings in which the no-go proofs for secure QBC become invalid. Meanwhile, we also showed that BC-based QOT, though not unconditionally secure, can defeat certain kinds of cheating which attempt to decode all transferred bits simultaneously with reliability 100%. Thus it is still valuable for building some “post-cold-war era” quantum cryptographies.
This insecurity proof is valid as long as the secure BC used in the QOT protocol is not BCCC. It covers relativistic BC [39–42], as well as many practically secure QBC [50–52], conditionally secure QBC [53], computationally secure QBC [54–56], cheat-sensitive QBC [57–62], and some other types of protocols [45,63–65]. Nevertheless, when Bob is limited to bounded or noisy quantum storages, secure QOT can be made possible in practice with two approaches. On one hand, with this technological constraint BCCC can be obtained [66–74]. This is because Bob can no longer keep system $C$ in equation (1) (which represents the systems $B_i \otimes \phi_i \otimes H_i \otimes E_i$ mentioned below equation (4) or $B_i \otimes \phi_i \otimes H_i \otimes E_i$ in Eq. (6)) perfectly in the entangled form shown by these equations once the protocol lasts too long or requires too much quantum storages. Thus BC-based QOT protocol in Section 3 can be secure at least against the insecurity proof in this paper. On the other hand, bounded or noisy storages can also force Bob to measure the quantum states he receives, as long as the QOT protocol involves too much qubits or the time interval between each step is sufficiently long. BC is no longer needed to convince Alice that Bob has already completed the measurements. Then there can be QOT protocols not based on BC, which are proven to be practically secure [68–71,75–77].

We should also note that, even without the assumption of such technological limitations, our above insecurity proof does not mean that all QOT must not be unconditionally secure in principle. This is because the existing method [3] is not necessarily the only way to build OT from BC. Further more, there is no evidence indicating that OT has to be built upon BC. Therefore, it is still worth questioning whether other kinds of unconditionally secure OT exist, especially relativistic OT.

The work was supported in part by the NSF of Guangdong province.

References

1. C.H. Bennett, G. Brassard, in Proceedings of IEEE Int. Conf. Computers, Systems, and Signal Processing, Bangalore, India (IEEE, New York, 1984), p. 175
2. J. Kilian, in Proceedings of ACM Annual Symposium on the Theory of Computing, 1988 (ACM, New York, 1988), p. 20
3. A.C.C. Yao, in Proceedings of the 26th Symposium on the Theory of Computing (ACM, New York, 1995), p. 67
4. D. Mayers, arXiv:quant-ph/9603015v3
5. D. Mayers, in Proceedings of the Fourth Workshop on Physics and Computation (New England Complex System Inst., Boston, 1996), p. 226
6. D. Mayers, Phys. Rev. Lett. 78, 3414 (1997)
7. H.-K. Lo, H.F. Chau, Phys. Rev. Lett. 78, 3410 (1997)
8. C. Crépeau, in Proceedings of Pragocrypt ’96: 1st International Conference on the Theory and Applications of Cryptology (Czech Technical University Publishing House, Prague, 1996)
9. H.-K. Lo, H.F. Chau, Physica D 120, 177 (1998)
10. H.F. Chau, H.-K. Lo, Fortsch. Phys. 46, 507 (1998)
11. G. Brassard, C. Crépeau, D. Mayers, L. Salvail, arXiv:quant-ph/9712023v1
12. G. Brassard, C. Crépeau, D. Mayers, L. Salvail, arXiv:quant-ph/9806031v1
13. G. Brassard, C. Crépeau, D. Mayers, L. Salvail, in Proceedings of Randomized Algorithms, Satellite Workshop of 23rd International Symposium on Mathematical Foundations of Computer Science (1998)
14. J. Bub, Found. Phys. 31, 735 (2001)
15. R.W. Spekkens, T. Rudolph, Phys. Rev. A 65, 012310 (2001)
16. R.W. Spekkens, T. Rudolph, Quantum Inf. Comput. 2, 66 (2002)
17. G.M. D’Ariano, arXiv:quant-ph/0209149v1
18. G.M. D’Ariano, in Proceedings of QCM&BC (Rinton press, Boston, 2002). Shortened version of arXiv:quant-ph/0209149
19. D. Mayers, arXiv:quant-ph/0212159v2
20. H. Halvorson, J. Math. Phys. 45, 4920 (2004)
21. A. Kitaev, D. Mayers, J. Preskill, Phys. Rev. A 69, 052326 (2004)
22. C.-Y. Cheung, in Proceedings of ERATO Conference on Quantum Information Science 2005 (Tokyo, 2005), arXiv:quant-ph/0508180v2
23. C.-Y. Cheung, arXiv:quant-ph/0601206v1
24. G.M. D’Ariano, D. Kretschmann, D. Schlingemann, R.F. Werner, Phys. Rev. A 76, 032328 (2007)
25. L. Magnin, F. Magniez, A. Leverrier, N.J. Cerf, Phys. Rev. A 81, 010302(R) (2010)
26. G. Chiribella, G.M. D’Ariano, P. Perinotti, D.M. Schlingemann, R.F. Werner, Phys. Lett. A 377, 1076 (2013)
27. G. Chiribella, G.M. D’Ariano, P. Perinotti, Phys. Rev. A 81, 062348 (2010)
28. Q. Li, C.Q. Li, D.-Y. Long, W.H. Chan, C.-H. Wu, QIP 11, 519 (2012)
29. A. Chailloux, I. Kerenidis, arXiv:1102.1679v1
30. H.-K. Lo, Phys. Rev. A 56, 1154 (1997)
31. T. Rudolph, arXiv:quant-ph/0202143v1
32. R. Colbeck, arXiv:0911.3814v2
33. R. Colbeck, Phys. Rev. A 76, 062308 (2007)
34. L. Salvail, C. Schaffner, M. Sotokawa, ASIACRYPT 2009, Lecture Notes in Computer Science (Springer-Verlag, 2009), Vol. 5912, p. 70
35. L. Salvail, M. Sotokawa, arXiv:0906.1671v2
36. A. Chailloux, I. Kerenidis, J. Sikora, arXiv:1007.1875v1
37. S. Winkler, J. Wullschleger, in Advances in Cryptology: CRYPTO 2010, Lecture Notes in Computer Science, edited by T. Rabin (Springer-Verlag, 2010), Vol. 6223, p. 707
38. H. Buhrman, M. Christandl, C. Schaffner, Phys. Rev. Lett. 109, 160501 (2012)
39. A. Kent, Phys. Rev. Lett. 83, 1447 (1999)
40. A. Kent, J. Cryptol. 18, 313 (2005)
41. A. Kent, New J. Phys. 13, 113015 (2011)
42. A. Kent, Phys. Rev. Lett. 109, 130501 (2012)
43. Y. Liu et al., Phys. Rev. Lett. 112, 010504 (2014)
44. T. Lunghi et al., Phys. Rev. Lett. 111, 180504 (2013)
45. G.P. He, J. Phys. A: Math. Theor. 44, 445305 (2011)
46. A. Kent, Phys. Rev. A 61, 042301 (2000)
47. C. Crépeau, in Advances in Cryptology: CRYPTO ’87, Lecture Notes in Computer Science, edited by C. Pomerance (Springer-Verlag, 1988), Vol. 293, p. 350
48. G.P. He, Z.D. Wang, Phys. Rev. A 73, 044304 (2006)
