Quantum key distribution based on orthogonal states allows secure quantum bit commitment

Guang Ping He

School of Physics and Engineering, Sun Yat-sen University, Guangzhou 510275, People’s Republic of China

E-mail: hegp@mail.sysu.edu.cn

Received 2 June 2011, in final form 18 August 2011
Published 14 October 2011
Online at stacks.iop.org/JPhysA/44/445305

Abstract

For more than a decade, it was believed that unconditionally secure quantum bit commitment (QBC) is impossible. But based on a previously proposed quantum key distribution scheme using orthogonal states, here we build a QBC protocol in which the density matrices of the quantum states encoding the commitment do not satisfy a crucial condition on which the no-go proofs of QBC are based. Thus, the no-go proofs could be evaded. Our protocol is fault-tolerant and very feasible with currently available technology. It reopens the venue for other ‘post-cold-war’ multi-party cryptographic protocols, e.g. quantum bit string commitment and quantum strong coin tossing with an arbitrarily small bias. This result also has a strong influence on the Clifton–Bub–Halvorson theorem which suggests that quantum theory could be characterized in terms of information-theoretic constraints.

PACS numbers: 03.67.Dd, 03.67.Hk, 42.50.Ex, 03.65.Ta, 03.67.Ac, 03.65.Ud, 42.50.St

(Some figures may appear in colour only in the online journal)

1. Introduction

Quantum bit commitment (QBC) is an essential primitive for quantum cryptography. It is the building block for quantum multi-party secure computations and more complicated ‘post-cold-war era’ multi-party cryptographic protocols [1, 2]. The first QBC protocol was proposed along with the very first proposal for quantum key distribution (QKD), i.e. the Bennett–Brassard (BB) 84 protocol [3]. But it was pointed out at the same time that the protocol is insecure against coherent attacks. An improved one was proposed later, known as the Brassard–Crépeau–Jozsa–Langlois (BCJL) 93 protocol [4]. It was accepted as secure for a while until a cheating strategy was found in 1996 [5]. Shortly after, it was further concluded that any QBC protocol cannot be unconditionally secure in principle [6–8]. This result was
called the Mayers–Lo–Chau (MLC) no-go theorem. It was considered as putting a serious
drawback on quantum cryptography. Though the result is widely accepted nowadays, there
is also doubt on the generality of the theoretical model of QBC used in the no-go proof,
as it seems unconvincing that limited mathematical formulation can characterize all possible
protocols [9]. New protocols attempting to evade the no-go theorem were proposed every now
and then [10–28], though most of them turned out to be unsuccessful [29, 30] or at least failed
to gain wide recognition. Nevertheless, these attempts stimulated the research on proving
the no-go theorem in more rigorous forms. The authors of [31–35] reviewed the original no-go
proof with fuller explanations, with some simple examples of insecure protocols given in
[31, 35]. The authors of [33] also extended the proof to cover ideal quantum coin tossing.
More complicated examples on how to apply the no-go proof to break some quantum as well as
classical bit commitment (BC) protocols which looked promising at that time were provided in
[36] and [37], respectively. The authors of [38–40] further studied the security bounds of QBC
quantitatively, with [39] focused on the protocol in [3]. The author of [41, 42] worked on a
similar direction, while focused especially on the class of protocols in [10–14]. Later on, a very
detailed proof was presented both in the Heisenberg picture [43] and the Schrödinger picture
[44], with the intention to achieve a more rigorous bound on the concealment–bindingness
tradeoff that can apply to all conceivable QBC protocols in which both classical and quantum
information are exchanged, including [10, 18–20, 22]. It was also shown that the no-go theorem
remains valid in a world subject to superselection rules [45–47], or for QBC associated with
secret parameters [48, 49], or when the participants are restricted to use Gaussian states and
operations only [50]. Recent efforts also include [51, 52], which proved the no-go theorem
with alternative methods.

As the no-go theorem became well accepted, people started to discuss the possibility of
building BC under various security conditions, e.g. classical BC under relativistic settings
[53, 54] or tamper-evident seals [55], quantum relativistic BC [56, 57] and computationally
secure QBC [58–61]. There are also QBC under experimental limitations, such as individual
measurements [62, 63] or limited coherent measurements [64], misaligned reference frames
[65], limited or noisy quantum storage [66–71], instability of particles [72, 73], Gaussian
operations with non-Gaussian states [74], etc [75, 76]. Some even considered BC in post-
quantum theories [77–80]. Others proposed less secure QBC [81, 82], variations of the
definition of QBC, e.g., cheat-sensitive QBC [83–86], conditionally secure QBC [87], etc
[88–90].

In this paper, we still focus on the original QBC without these conditions. Based on an
existing QKD scheme using orthogonal states [91, 92], we show that it becomes possible to
build a QBC protocol, to which the no-go proofs do not apply. This protocol enables many
other cryptographies, and is readily implementable with currently available technology. We
also address the relationship between this finding and the Clifton–Bub–Halvorson (CBH)
theorem [93] which tries to characterize quantum theory in terms of information-theoretic
constraints.

QKD provides an unconditionally secure method for two remote participants to transmit
secret information against any eavesdropper. Most existing QKD schemes (e.g. [3, 94, 95])
use nonorthogonal states as carriers for the transmitted information. Since quantum mechanics
guarantees that nonorthogonal states cannot be faithfully cloned, any eavesdropping will
inevitably introduce detectable disturbance on the states. Thus, the eavesdropper will be caught
once he gains a non-trivial amount of information. For this reason, it was once believed that
nonorthogonal states are necessary for secure QKD. But Goldenberg and Vaidman managed
to present a scheme based on orthogonal states [91]. This brilliant idea opens yet another path
for adopting more bizarre properties of quantum mechanics for cryptography. We will use it as the base of our current work.

Generally, in both QKD and QBC the two participants are called Alice and Bob. But in our current proposal of QBC, the actions of Bob are more similar to that of the eavesdropper rather than the Bob in QKD. To avoid confusion, in this paper we use the names in the following way. In QKD, the sender of the secret information is called Alice, the receiver is renamed Charlie instead of Bob, and the external eavesdropper is called Eve. In QBC, the sender of the commitment is Alice, the receiver is Bob, and there is no Eve since QBC merely deals with the cheating from internal dishonest participants, instead of external eavesdropping.

2. QKD scheme based on orthogonal states

The QKD scheme proposed in [91] is outlined below. Consider the ideal case where no transmission error occurs in the communication channels. Alice encodes the bit values 0 and 1 she wants to transmit to Charlie, respectively, using two orthogonal states

\[
0 \rightarrow |\psi_0 \rangle \equiv (|a\rangle + |b\rangle)/\sqrt{2}, \\
1 \rightarrow |\psi_1 \rangle \equiv (|a\rangle - |b\rangle)/\sqrt{2}.
\]

Here, $|a\rangle$ and $|b\rangle$ are the localized wave packets of the same qubit. When sending these states to Charlie, two details are important for the security of the scheme. First, $|a\rangle$ and $|b\rangle$ are not sent simultaneously, but separated by a fixed delay time $\tau$. The value of $\tau$ should ensure that $|a\rangle$ reached Charlie’s site before $|b\rangle$ leaves Alice’s site (for simplicity, we do not study the case where $\tau$ is further reduced, even though it may not hurt the security), so that the two wave packets are never present together in the transmission channels. Second, the sending time of each $|\psi_0 \rangle$ and $|\psi_1 \rangle$ is random, and kept secret from Eve until $|a\rangle$ has already arrived.

Figure 1 illustrated the diagram for an experimental implementation of the scheme using a Mach–Zehnder interferometer. Alice prepares $|\psi_0 \rangle$ ($|\psi_1 \rangle$) by sending a single photon from the source $S_0$ ($S_1$), and then splits it into $|a\rangle$ and $|b\rangle$ using the beam splitter $BS_1$. $|a\rangle$ is sent directly to Charlie while $|b\rangle$ is delayed by the storage ring $SR_1$ before sending. At Charlie’s site, $|a\rangle$ is delayed by the storage ring $SR_2$ and then meets $|b\rangle$ at the beam splitter $BS_2$ and interferes. The delay times caused by $SR_1$ and $SR_2$ are tuned equal. Thus, the complete apparatus of Alice and Charlie forms a balanced Mach–Zehnder interferometer, so that $|\psi_0 \rangle$ ($|\psi_1 \rangle$) will always make the detector $D_0$ ($D_1$) click when no eavesdropping occurs, allowing Charlie to decode...
the transmitted bit value. Alice sends Charlie a series of |Ψ₀⟩ and |Ψ₁⟩, and then announces all the sending times and some of the encoded bits for security check. If all announced results match with Charlie’s measurement, the two parties keep the unannounced encoded bits as the secret key. It was shown that the scheme is unconditionally secure [91, 92], since Eve can never access the entire states |Ψ₀⟩ and |Ψ₁⟩, unless she intercepts and delays |a⟩. But then she needs to send Charlie a ‘dummy’ state in advance to escape detection. However, without knowing Alice’s sending time beforehand, Eve can hardly send the dummy state at the proper time. Thus, eavesdropping will be revealed once Alice does not send any state while Charlie’s detectors click after time τ.

3. Our QBC protocol

QBC is a two-party cryptography including two phases. In the commit phase, Alice (the sender of the commitment) decides the value of the bit \( b = 0 \) or \( 1 \) which she wants to commit, and sends Bob (the receiver of the commitment) a piece of evidence, e.g., some quantum states. Later, in the unveil phase, Alice announces the value of \( b \), and Bob checks it with the evidence. An unconditionally secure QBC protocol needs to be both binding (i.e. Alice cannot change the value of \( b \) after the commit phase) and concealing (Bob cannot know \( b \) before the unveil phase) without relying on any computational assumption.

To make use of the QKD scheme in [91] for QBC, our starting point is to treat Charlie’s site as a part of Alice’s, so that the two parties merge into one. That is, Alice sends out a bit-string encoded with the above orthogonal states, whose value is related to the bit she wants to commit. Then, she receives the states herself. Meanwhile, let Bob take the role of Eve. His action shifts between two modes. In the intercept mode, he applies the intercept–resend attack to read parts of the string. In the bypass mode, he simply does nothing so that the corresponding parts of the states return to Alice intact. Since the eavesdropping on every single bit of the string has a non-trivial probability to escape Alice’s detection, at the end of the process some bits of the string become known to Bob, while Alice does not know the exact position of these bits. Thus, she cannot alter the bit-string freely at a later time, making the protocol binding. On the other hand, Bob cannot eavesdrop the whole string without being detected. Thus, the value of the committed bit can be made concealing by putting a limit on the error rate Bob allowed to make in the protocol.

The rigorous description of our QBC protocol is as follows.

The commit protocol:
1. Bob chooses a binary linear \((n, k, d)\)-code \( C \) and announces it to Alice, where \( n, k, d \) and another parameter \( s \) (\( s \gg n > k > d \)) are agreed on by both Alice and Bob.
2. Alice chooses a nonzero random \( n \)-bit string \( r = (r_1 r_2 \ldots r_n) \in \{0, 1\}^n \) and announces it to Bob. This makes any \( n \)-bit codeword \( c = (c_1 c_2 \ldots c_n) \) in \( C \) sorted into either of the two subsets \( C_{(0)} \equiv \{ c \in C \mid c \circ r = 0 \} \) and \( C_{(1)} \equiv \{ c \in C \mid c \circ r = 1 \} \). Here \( c \circ r \equiv \bigoplus_{i=1}^{n} c_i \land r_i \).
3. Now Alice decides the value of the bit \( b \) that she wants to commit. Then, she chooses a codeword \( c \) from \( C_{(b)} \) randomly.
4. Alice and Bob treat the timeline as a series of discrete time instants \( t_1, t_2, \ldots, t_s \) with equal intervals. Alice encodes each bit of \( c \) as \( c_i \rightarrow |\Psi_{c_i}⟩ = (|a_i⟩ + (-1)^i |b_i⟩)/\sqrt{2} \) and sends them to Bob. The time \( t(i) \) for sending each \( |\Psi_{c_i}⟩ \) is randomly chosen among \( t_1, t_2, \ldots, t_s \), while all \( t(i) \) (\( i = 1, 2, \ldots, n \)) should be chosen in the sequence of \( i \), i.e. there should be \( t(i_1) < t(i_2) \) for any \( i_1 < i_2 \). Also, just as in the QKD scheme in [91], the two wave packets \( |a_i⟩ \) and \( |b_i⟩ \) of the same qubit \( |\Psi_{c_i}⟩ \) are not sent simultaneously. When we say that \( |\Psi_{c_i}⟩ \) is sent at time \( t(i) \), we mean that \( |a_i⟩ \) is sent at time \( t(i) \), while \( |b_i⟩ \) is delayed
and then leaves Alice’s site at time $t(i) + \tau$. The delay time $\tau$ is fixed for all $|\Psi_i\rangle$ and known to Bob.

(5) At each of the time instants $t_1, t_2, \ldots, t_s$, Bob chooses the intercept mode with probability $\alpha$ and the bypass mode with probability $1 - \alpha$.

If he chooses to apply the intercept mode at time $t_j$ ($j \in \{1, 2, \ldots, s\}$), he prepares a qubit in the state $|\Psi_0\rangle = (|a_j\rangle + |b_j\rangle)/\sqrt{2}$, and sends the wave packet $|a_j\rangle$ to Alice at time $t_j$, while $|b_j\rangle$ is temporarily delayed. Meanwhile, Bob adds a delay circuit to the quantum communication channel $A$ (where the wave packets $|a_i\rangle$ come from Alice). At time $t_j + \tau$, he combines the output of this delay circuit with the quantum communication channel $B$ (where the wave packets $|b_i\rangle$ come from Alice) and measures whether Alice has sent him $|\Psi_0\rangle$, $|\Psi_1\rangle$, or nothing at all. If the result of the measurement is $|\Psi_0\rangle$ ($|\Psi_1\rangle$), he leaves his delayed $|b_j\rangle$ unchanged (he introduces a phase shift to change $|b_j\rangle$ into $-|b_j\rangle$) and sends it to Alice. In this case, Bob learned the state Alice sent at time $t_j$ while Alice cannot detect this action with certainty. But if Bob found nothing in his measurement, he measures (or simply discards) $|b_j\rangle$. In this case, Alice’s detectors will click with probability $1/2$ due to the presence of $|a_j\rangle$, revealing that Bob is running the intercept mode.

On the other hand, if Bob chooses to apply the bypass mode at time $t_j$, he simply keeps channel $A$ intact at time $t_j$, and channel $B$ intact at time $t_j + \tau$. Consequently, if a state was sent from Alice at time $t_j$, it will be returned to her detectors as-is at time $t_j + \tau$.

(6) Alice uses the same apparatus that Bob used in the intercept mode to measure the output of the quantum communication channels from Bob. She counts the total number of the states she received from Bob, and denotes it as $n'$. By analyzing step (5) it can be shown that $n' \sim \alpha(s - n)/2 + n$. Thus, Alice can estimate the probability of Bob choosing the intercept mode as $\alpha \sim 2(n' - n)/s - n$. Alice agrees to continue with the protocol if $\alpha \ll 1 - d/n$, which means that the number of $c_i$ known to Bob is $an \ll n - d$.

(7) Alice announces all the time instants $t(i)$ at which she sent $|\Psi_i\rangle$’s ($i = 1, 2, \ldots, n$). Bob checks that he indeed detected some states at each $t(i) + \tau$ and no detection was found at other times, as long as he has chosen the intercept mode at the corresponding time instants. This completes the commit phase.

The unveil protocol:

(8) Alice announces the values of $b$ and $c = (c_1c_2 \ldots c_n)$.

(9) Bob accepts the commitment if $c \oplus r = b$ and $c$ is indeed a codeword from $C$, and every $c_i$ agrees with the state $|\Psi_{c_i}\rangle$ he received in the intercept mode.

The diagram for implementing this protocol using the Mach–Zehnder interferometer is shown in figure 2.

Intuitively, the protocol can achieve the goal of QBC for the following reasons. The binary linear $(n, k, d)$-code $C$ can simply be viewed as a set of classical $n$-bit strings. Each string is called a codeword. This set of strings has two features. (A) Among all the $2^n$ possible choices of $n$-bit strings, only a particular set of the size $\sim 2^k$ is selected to form this set. (B) The distance (i.e. the number of different bits) between any two codewords in this set is not less than $d$. Feature (A) puts a limit on Alice’s freedom on choosing the initial state $|\Psi_0\rangle \equiv |\Psi_{c_1}\rangle \otimes |\Psi_{c_2}\rangle \otimes \cdots \otimes |\Psi_{c_n}\rangle$. Meanwhile, feature (B) guarantees that if Alice wants to change the string $c$ from one codeword into another, she needs to change at least $d$ qubits of $|\Psi_0\rangle$. But the intercept mode in the protocol enables Bob to learn about $an$ bits of the string $c$, while Alice does not know all the positions of these bits in $c$ with certainty. Therefore, when Alice alters the codeword corresponding to $|\Psi_c\rangle$, the probability for her to escape detection will be only at the order of magnitude of $(1 - \alpha)^n$. By increasing $d$, the security of the protocol against Alice’s cheating will be strengthened. On the other hand, feature (A) also guarantees
that the number of different codewords having less than \( n - d \) bits in common increases exponentially with \( k \). That is, as Bob knows only \( \alpha n \ll n - d \) bits of \( c \), the potential choices for \( c \) are too much for him to determine whether \( c \) belongs to the subset \( C(0) \) or \( C(1) \). Thus, his knowledge on the committed bit \( b \) before the unveil phase can be made arbitrarily close to zero by increasing \( k \). Fixing \( k/n \) and \( d/n \) while increasing \( n \) will then result in a protocol secure against both parties. As an example, following the estimation in section 3.2 of [4], a practical choice can be \( k/n = 0.52 \), \( d/n = 0.1 \). The other parameters can be chosen accordingly as \( \alpha = 0.7 \), \( s/n = 10 \) and \( n \geq 1000 \).

Note that when \( n \to \infty \) with \( k/n \), \( d/n \), and \( \alpha \) fixed, the probabilities for Alice and Bob to cheat successfully in our protocol will both drop arbitrarily close to 0, but they never strictly equal 0. As defined in [7, 96], if a protocol can make the probability of successful cheating strictly equal to 0, then it is considered as ‘perfectly secure’. On the other hand, when speaking of ‘unconditionally secure’, it generally implies that the protocol should meet two requirements simultaneously. (I) Theoretically, the security of the protocol must be based directly on fundamental laws of physics (e.g. the validity of the postulates of quantum mechanics or relativity) alone rather than computational assumptions. (II) Quantitatively, the probability of successful cheating does not equal 0, but can be made arbitrarily close to 0 by increasing some security parameters of the protocol. To emphasize the second meaning, some people use the term ‘information-theoretically secure’ interchangeably with ‘unconditionally secure’ [46]. So we can see that our protocol falls into this category. This is already the best we could expect from quantum cryptography so far. For example, the BCJL93 QBC protocol [4] tried to reduce the probability of successful cheating down to exactly the same level (i.e. arbitrarily close but not equal to 0), but was proven a failure by [5]. The authors of [38] also showed that perfectly secure QBC is impossible. The protocols proposed in it are even less secure, as at least one of the probabilities of Alice’s and Bob’s successful cheating can never be made arbitrarily close to 0. In fact, even the well-known BB84 QKD protocol [3] is not perfectly secure. This is because the eavesdropper Eve can always perform the most basic intercept–resend attack. That is, she intercepts any quantum state from the sender, measures it in a basis which she chooses simply by guess and then resends the resultant state to the receiver. While she stands a great chance of being detected whenever her guess is wrong, we can never

![Figure 2. Diagram for the apparatus of the QBC protocol when Bob chooses the intercept mode.](image-url)
neglect the probability that she can be so lucky that she guesses all the bases correctly. Even though this probability is extremely small, and drops arbitrarily close to 0 with the increase of the number of states used in the protocol, still it never strictly equals 0. Nevertheless, QKD is still considered as the most secure communication method of today. Thus, we see that an unconditionally secure protocol is already good enough.

Under practical settings, some steps of our protocol may need minor modifications. For example, the protocol can be made fault-tolerant as long as \( d/n \) is chosen to be much larger than the transmission error rate \( \varepsilon \) of the quantum channels. This is because the distance between any two codewords is not less than \( d \). Even if a dishonest Alice replaces the channels with noiseless ones so that she can alter up to \( \varepsilon n \) bits of the string \( c \) while blaming it on the transmission error, it is still insufficient to change a codeword into another one so that her committed bit \( b \) will not be altered. For this reason, in step (9) Bob can in fact allow the mismatched results between Alice’s announced \( c_i \) and Bob’s received |\( \Psi_1 \rangle \rangle \) to occur with a probability not greater than \( \varepsilon \), thus making the protocol fully functional with noisy channels.

Also, in real settings the physical systems implementing the qubits may have other degrees of freedom, which leave room for some technical cheating strategies. For instance, Alice may send photons with certain polarization or frequency, so that she can distinguish them from the photons Bob sends in the intercept mode. In this case, Bob and Alice should discuss at the beginning of the protocol, to limit these degrees of freedom to a single mode. In step (5) when Bob chooses the intercept mode, he should also measure occasionally these degrees of freedom of some of Alice’s photons, instead of performing the measurement in the original step (5). Then, if Alice wants to send distinguishable photons with a high probability so that they are sufficient for her cheating, she will inevitably be detected.

4. Security

Since the number of potential cheating strategies could be infinite, in this work we do not attempt to prove that our protocol is unconditionally secure against any strategy. What will be shown here is that our protocol is at least not covered by the cheating strategy used in the MLC no-go theorem that makes all previous QBC schemes insecure.

Briefly, the MLC no-go theorem and all its variations [5–8], [31–52] have the following common features.

(i) The reduced model. According to the no-go proofs, any QBC protocol can be reduced to the following model. Alice and Bob together own a quantum state in a given Hilbert space. Each of them performs unitary transformations on the state in turns. All measurements are performed at the very end.

(ii) The coding method. The quantum state corresponding to the committed bit \( b \) has the form

\[
|\psi_b\rangle = \sum_j \lambda_j^{(b)} |e_j^{(b)}\rangle_A \otimes |f_j^{(b)}\rangle_B.
\]

Here, systems \( A \) and \( B \) are owned by Alice and Bob, respectively, \( \{|e_j^{(b)}\rangle_A\} \) is an orthogonal basis of system \( A \) while \( |f_j^{(b)}\rangle_B \) are not necessarily orthogonal to each other.

(iii) The concealing condition. To ensure that Bob’s information on the committed bit is trivial before the unveil phase, any QBC protocol secure against Bob should satisfy

\[
\rho_0^B \simeq \rho_1^B, \tag{3}
\]

where \( \rho_0^B \equiv Tr_A |\psi_0\rangle\langle \psi_0| \) is the reduced density matrix of the state sent to Bob corresponding to Alice’s committed bit \( b \). Note that in some presentation of the no-go proofs (e.g. [38, 40, 43, 50]), this feature was expressed using the trace distance or the fidelity instead of the reduced density matrices, while the meaning remains the same.
(iv) The cheating strategy. As long as equation (3) is satisfied, there exists a local unitary transformation for Alice to map $|\psi_0\rangle$ into $|\psi_1\rangle$ successfully with a high probability [97]. Thus, a dishonest Alice can unveil the state as either $|\psi_0\rangle$ or $|\psi_1\rangle$ at her will with a high probability to escape Bob’s detection. For this reason, a concealing QBC protocol cannot be binding.

The key that makes our protocol evade the no-go proofs is that it does not have the feature (iii). As shown in equation (1), every bit value $c_i$ in our protocol is encoded with orthogonal states. Therefore, the state $|\Psi_i\rangle \equiv |\Psi_{c_1}\rangle \otimes |\Psi_{c_2}\rangle \otimes \cdots \otimes |\Psi_{c_l}\rangle$ corresponding to a codeword $c$ is orthogonal to any other state $|\Psi_{c'}\rangle \equiv |\Psi_{c'_1}\rangle \otimes |\Psi_{c'_2}\rangle \otimes \cdots \otimes |\Psi_{c'_l}\rangle$ corresponding to a different codeword $c'$. Consequently, the two Hilbert spaces supported by the states corresponding to the codeword subsets $C_{(0)}$ and $C_{(1)}$, respectively, are completely orthogonal to each other. Therefore, it is obvious that our protocol satisfies $\rho_{0}^B \perp \rho_{1}^B$ instead of equation (3). Then Alice’s cheating strategy (iv) will no longer apply because the corresponding unitary transformation does not exist without equation (3). Since all existing no-go proofs of unconditionally secure QBC [5–8], [31–52] have the feature $\rho_{0}^B \simeq \rho_{1}^B$, we can see that they all fail to cover our protocol.

Let us elaborate in more detail. The existence of Alice’s cheating strategy in the no-go proofs is backed by the Hughston–Jozsa–Wootters (HJW) theorem [97] basing on Schmidt decomposition. Following the manner of [31], it can be expressed in simple words as follows.

**The HJW theorem:** Let $f_1, f_2, \ldots, f_m$ and $f'_1, f'_2, \ldots, f'_n$ be two sets of possible quantum states with associated probabilities described by an identical density matrix $\rho$. It is possible to construct a composite system $A \otimes B$ such that $B$ alone has the density matrix $\rho$ and such that there exists a pair of measurements $M, M'$ with the property that applying $M$ (respectively $M'$) to $A$ yields an index $j$ of state $f_j$ (respectively $f'_j$) to which $B$ will have collapsed.

Now consider a QBC protocol which requires Alice to encode the committed $b$ in the state

$$|\psi_{b=0}\rangle = \sum_j \lambda_j^{(0)} |e_j^{(0)}\rangle_{A} \otimes |f_j^{(0)}\rangle_{B},$$

or

$$|\psi_{b=1}\rangle = \sum_j \lambda_j^{(1)} |e_j^{(1)}\rangle_{A} \otimes |f_j^{(1)}\rangle_{B},$$

respectively, where the meaning of the notations is the same as that of equation (2). When the concealing condition $\rho_{0}^B \simeq \rho_{1}^B$ is satisfied, according to the HJW theorem there exists another basis $\{|e'_j\rangle_{A}\}$ of system $A$ with which we can rewrite equation (4) as

$$|\psi_{b=0}\rangle = \sum_j \lambda'_j |e'_j\rangle_{A} \otimes |f_j^{(1)}\rangle_{B}. $$

Comparing with equation (5), we can see that $|\psi_{b=0}\rangle$ differs from $|\psi_{b=0}\rangle$ only by a local unitary transformation $U_A$ of Alice which maps $|e_j^{(0)}\rangle_A$ into $|e'_j\rangle_A$. That is, with this transformation, Alice can alter the commitment in the unveil phase by herself. The actual cheating procedure is as follows. Alice always uses $|\psi_{b=0}\rangle$ to execute the commit protocol regardless of the value of $b$. Later, if she wants to unveil $b = 0$, she simply measures system $A$ in the basis $\{|e'_j\rangle_A\}$ to collapse system $B$ into a certain $|f_j^{(0)}\rangle_{B}$ (where $j$ is determined by the quantum uncertainty in the measurement). Else if she wants to unveil $b = 1$, she rotates her basis to $|e_j^{(1)}\rangle_A$ so that the corresponding measurement can collapse system $B$ to a certain $|f_j^{(1)}\rangle_{B}$. Even if she is required to transfer system $A$ to Bob for verification, all she needs to do is to further apply the local unitary transformation $U_A$ on system $A$ to rotate $|e'_j\rangle_A$ into $|e'_j\rangle_A$. Thus, she can always unveil $b = 0$ successfully with the probability 100%, while unveiling $b = 1$ can also be successful.
with a very high probability (which can reach 100% when \( \rho_0^B \) equals \( \rho_1^B \) exactly). Namely, Alice can cheat because there are two different bases for system A, both of which can lead to a legitimate outcome in the unveil phase.

But in our QBC protocol, as the state \( |\Psi_c\rangle \) sent to Bob satisfies \( \rho_0^B \perp \rho_1^B \), \( |\psi_{b=0}\rangle \) can no longer be expressed as the superposition of the components of \( |\psi_{b=1}\rangle \) like equation (6). Consequently, even if Alice introduces an ancillary system \( A \) entangled with many different \( |\Psi_c\rangle \) in the form of equation (2), there will be no alternative basis for Alice to alter her commitment. Instead, unveiling \( b = 0 \) and \( b = 1 \) will be performed in the same basis. This can be seen from the following analysis. Let \( H \) denote the Hilbert space of the composite system \( A \otimes B \) supported by all possible committed states. Let \( H_0 \) (\( H_1 \)) be its subspace supported by all the states encoding \( b = 0 \) (\( b = 1 \)), with \( \{ |g_{j}^{(0)}\rangle_{A\otimes B} \} \) \( \{ |g_{j}^{(1)}\rangle_{A\otimes B} \} \) denoting one of its basis.

The condition \( \rho_0^B \perp \rho_1^B \) indicates that \( H_0 \) and \( H_1 \) have no overlap at all. Therefore, \( \{ |g_{j}^{(0)}\rangle_{A\otimes B} \} \) and \( \{ |g_{j}^{(1)}\rangle_{A\otimes B} \} \) share no state in common. Any local unitary transformation \( U_A \) on system A by Alice can be extended as \( U \equiv U_A \otimes I_B \), which becomes a unitary transformation on the composite system \( A \otimes B \). Here, \( I_B \) is the identity operator on system B. Obviously any \( U \) in this form cannot map \( \{ |g_{j}^{(0)}\rangle_{A\otimes B} \} \) into \( \{ |g_{j}^{(1)}\rangle_{A\otimes B} \} \). Thus, Alice’s actions for unveiling \( b = 0 \) and \( b = 1 \), respectively, are not related to each other by a local unitary transformation of her own. Instead, the set \( \{ |g_{j}^{(0)}\rangle_{A\otimes B} \} \cup \{ |g_{j}^{(1)}\rangle_{A\otimes B} \} \) forms a single complete orthogonal basis of the global space \( H = H_0 \oplus H_1 \), as either of \( \{ |g_{j}^{(0)}\rangle_{A\otimes B} \} \) and \( \{ |g_{j}^{(1)}\rangle_{A\otimes B} \} \) alone is incomplete. Therefore, when writing out the Schmidt decomposition of the committed state in forms of equations (4) and (5), the states \( |f_{j}^{(0)}\rangle_B \) and \( |f_{j}^{(1)}\rangle_B \) belong to the same basis, instead of two different bases nonorthogonal to each other. As a result, comparing with the description of the HIW theorem, now \( f_1^{(0)}, f_2^{(0)}, \ldots, f_m^{(0)} \) and \( f_1^{(1)}, f_2^{(1)}, \ldots, f_n^{(1)} \) together form a single set of orthogonal quantum states with associated probability described by a density matrix \( \rho \). When constructing a composite system \( A \otimes B \) such that \( B \) alone has a density matrix \( \rho \), the ‘two’ measurements \( M, M' \) (with the property that applying \( M \) (respectively \( M' \)) to \( A \) yields an index \( j \) of the state \( f_j^{(0)} \) (respectively \( f_j^{(1)} \)) to which \( B \) will have collapsed) now both become incomplete measurements on system \( A \). Together they form one single complete measurement set. \( \{ |e_k^{(0)}\rangle_A \} \) and \( \{ |e_k^{(1)}\rangle_A \} \) in equations (4) and (5) now both belong to the same single orthogonal basis of system \( A \) corresponding to this complete measurement. No matter what value Alice wants to unveil, her action is always to perform the measurement in this basis. Which one of the unveiled values will finally be obtained is determined by the form of the state Alice prepared in the commit phase, and the quantum uncertainty in the unveil measurement (if Alice has prepared the state in the form of equation (7), which we will discuss in more detail in the next section). Either way, it is not determined by Alice’s different actions in the unveil phase, as there does not exist a second legitimate action at all. If Alice insists on measuring in a different basis other than \( \{ |e_k^{(0)}\rangle_A \} \cup \{ |e_k^{(1)}\rangle_A \} \), it will not lead to any specific legitimate unveiled outcome with certainty, because it will collapse the state of each qubit she sent to Bob \( \langle \Psi \rangle = \cos \theta |a\rangle + \sin \theta |b\rangle \) (where \( \theta \neq k\pi \pm \pi/4, k \) is an integer) or similar forms, instead of equation (1). Thus, it will only increase the probability for her cheating to be detected. Therefore, we see that the feature \( \rho_0^B \perp \rho_1^B \) eliminates the existence of a second legitimate measurement basis, making Alice’s cheating strategy described in the previous paragraph futile in our protocol.

In fact, similar characters can also be found in a BC protocol proposed by Kent [53], which bases its security on relativity instead of quantum mechanics. As pointed out in the third paragraph of the introduction of [47], ‘Kent’s relativistic BC protocol does not rely on the existence of alternative decompositions of a density operator, and so its security is not challenged by the Mayers–Lo–Chau result’. As our protocol uses orthogonal states to encode
the committed bit, it does not rely on alternative decompositions either. Thus, it can evade the MLC theorem for the same reason.

On the other hand, our protocol is still concealing against Bob despite that $\rho_B^0 \perp \rho_B^1$. The MLC theorem suggests that protocols satisfying this condition cannot be secure, because Bob can always perform a measurement which optimally distinguishes $\rho_B^0$ and $\rho_B^1$, and thus learns the value of $b$ without Alice’s help. But in our protocol, even though $\rho_B^0$ and $\rho_B^1$ are distinguishable theoretically as the states are orthogonal, Bob is unable to perform the corresponding measurement before the unveil phase while escaping Alice’s detection. This is because the protocol puts a limit on the number of qubits that he is allowed to measure, as he is required to apply the intercept mode with probability $\alpha \ll 1 - d/n$ only. So the key question is whether a dishonest Bob can make his intercept mode indistinguishable with the bypass mode to Alice with a probability higher than was evaluated in step (5) of our protocol. This is prevented by two important features of the QKD scheme [91] on which our QBC protocol is based. First, the use of the storage rings ensures the two wave packets of each single qubit of Alice are never presented simultaneously in the quantum channels. This prevents Bob from knowing the arrival of Alice’s qubit in time by measuring channel A alone, as it will disturb the state of the qubit and make the intercept mode lose its advantage of distinguishing Alice’s state. Secondly, Alice’s sending time is random and kept secret until step (7). Therefore, in step (5) Bob has to decide himself whether to send $|\Psi_1\rangle$ into the quantum channels to Alice, before he can be sure whether he will detect a qubit in the quantum channels from Alice. He cannot avoid the case where he sent $|\Psi_0\rangle$ to Alice, while finding out later that Alice has not sent him a qubit at the corresponding time instant. Then, his interception will be revealed once Alice detects $|\Psi_0\rangle$, just as expected in the protocol. Thus, a dishonest Bob intercepting more qubits than allowed will inevitably introduce a very high estimated value of $\alpha$ in step (6), so that the cheating will be revealed.

More generally, if there exists a strategy enabling Bob to intercept most of Alice’s qubit without being detected, then in the QKD scheme [91], an eavesdropper will be able to apply the same strategy to gain a non-trivial amount of information of the secret key while escaping detection too. But there were already many studies on the scheme in [91] proving that it is indeed unconditionally secure [91, 92, 98–100]. Therefore, all these proofs can be regarded as further supports on the security of our protocol.

In short, the use of orthogonal states makes our protocol evade Alice’s cheating strategy suggested by the no-go proofs, while the security against Bob is provided by the security of the QKD scheme on which our QBC protocol is based.

### 5. Limitations and applications

Nevertheless, our protocol has the limitation that it cannot force Alice to commit to a classical bit. Alice can skip step (3). Then in step (4), instead of choosing a particular codeword $c$ and preparing system $B$ to be sent to Bob in the state $|\Psi_c\rangle \equiv |\Psi_{c_1}\rangle \otimes |\Psi_{c_2}\rangle \otimes \ldots \otimes |\Psi_{c_n}\rangle$, she introduces an ancillary system $A$ and prepares the state of the incremented system $A \otimes B$ in an entangled form as

$$|A \otimes B\rangle = \sum_{c \in C} \lambda_c |e_c\rangle \otimes |\Psi_c\rangle$$

$$= \sum_{c \in C_{(0)}} \lambda_c |e_c\rangle \otimes |\Psi_c\rangle + \sum_{c \in C_{(1)}} \lambda_c |e_c\rangle \otimes |\Psi_c\rangle.$$

(7)

Here, $\{|e_c\rangle\}$ is a set of orthogonal states that forms a basis of system $A$. Alice keeps system $A$ at her side unmeasured, and sends system $B$ to Bob to complete the rest of the commit
protocol. By the time she needs to unveil the committed $b$, she completes the measurement on system $A$ and knows which $|\Psi_i\rangle$ system $B$ collapsed to. With this method, she can learn what can be announced as the value of the codeword $c$ (and therefore $b$) without conflicting with Bob’s measurement. As a consequence, her commitment was kept at the quantum level until the unveil phase. But we must note that this problem, according to section III of [96], is not considered a security failure of a quantum BC protocol per se. This is because, as we have shown above, our protocol has the feature $\rho_0^B \perp \rho_1^B$, i.e. all $|\Psi_i\rangle$ corresponding to the codewords $c \in C(0)$ are orthogonal to these corresponding to $c \in C(1)$. Thus, the probability for the state (equation (7)) to be unveiled as $b = 0$ successfully is

$$p_0 = \sum_{c \in C(0)} |\lambda_c|^2,$$

while the probability for it to be unveiled as $b = 1$ is

$$p_1 = \sum_{c \in C(1)} |\lambda_c|^2.$$

The normalization condition for equation (7) gives

$$p_0 + p_1 = 1.$$

Therefore, despite that our protocol cannot force Alice to commit to a particular classical value of $b$, she is forced to commit to a probability distribution $(p_0, p_1)$ once she prepared the state of $A \otimes B$ in step (4). She can no longer change the value of either $p_0$ or $p_1$ later. The final value of the unveiled $b$ is completely out of her control. Instead, it is determined by the quantum uncertainty in her final measurement on system $A$. As stated clearly in [96], when equation (10) is satisfied, the protocol already meets the requirement of what is defined as unconditionally secure QBC. Note that the relativistic BC protocol [53] is well accepted as being unconditionally secure, even though it has exactly the same problem. Most previous QBC protocols are considered insecure because the corresponding $p_0 + p_1$ is larger and cannot be made arbitrarily close to 1. In fact, in some of these protocols (e.g. [3, 4]), $p_0 + p_1$ even reaches or is arbitrarily close to 2. On the other hand, if a protocol can force Alice to commit to a particular classical $b$, i.e. besides $p_0 + p_1 = 1$, both $p_0$ and $p_1$ 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) [96]. Namely, our protocol is a QBC but not a BCCC.

The difference between QBC and BCCC makes it important to re-examine the relationship between BC and other cryptographic tasks at the quantum level. For example, though BC and oblivious transfer (OT) [2, 101] are equivalent at the classical level, our QBC protocol may not lead to unconditionally secure quantum OT (QOT) [1, 102], at least, not in the traditional way described in these references. Note that there are many variations of OT [2], e.g. 1-out-of-2 OT [102, 103]. Here, we use the original one [1, 101] (also called all-or-nothing OT) as an example. It is defined as the following process. Alice wants to transfer a secret bit $b \in \{0, 1\}$ to Bob. At the end of the protocol, either Bob could learn the value of $b$ with the reliability (which means the probability for Bob’s output $b$ to be equal to Alice’s input) 100%, or he has zero knowledge on $b$. Each case should occur with the probability 1/2, and which one finally occurs is out of their control. Meanwhile, Alice should learn nothing about which case takes place. According to section 2 of [1], QOT can be built upon BC as follows.

The $QOT$ protocol:

(1) Let $|0, 0\rangle$ and $|0, 1\rangle$ be two orthogonal states of a qubit, and define $|1, 0\rangle \equiv (|0, 0\rangle + |0, 1\rangle)/\sqrt{2}$, $|1, 1\rangle \equiv (|0, 0\rangle - |0, 1\rangle)/\sqrt{2}$. That is, the state of a qubit is denoted as $[a_i, g_i]$, where $a_i$ represents the basis and $g_i$ distinguishes the two states in the same basis. For
i = 1, \ldots, n, Alice randomly picks \(a_i, g_i \in \{0, 1\}\) and sends Bob a qubit \(\phi_i\) in the state \(|a_i, g_i\rangle\).

(II) For \(i = 1, \ldots, n\), Bob randomly picks a basis \(b_i \in \{0, 1\}\) to measure \(\phi_i\) and records the result as \(|b_i, h_i\rangle\). Then, he commits \((b_i, h_i)\) to Alice using the BC protocol.

(III) Alice randomly picks a subset \(R \subseteq \{1, \ldots, n\}\) and tests Bob’s commitment at positions in \(R\). If any \(i \in R\) reveals \(a_i = b_i\) and \(g_i \neq h_i\), then Alice stops the protocol; otherwise, the test result is accepted.

(IV) Alice announces the bases \(a_i (i = 1, \ldots, n)\). Let \(T_0\) be the set of all \(1 \leq i \leq n\) with \(a_i = b_i\), and \(T_1\) be the set of all \(1 \leq i \leq n\) with \(a_i \neq b_i\). Bob chooses \(I_0 \subseteq T_0 - R, I_1 \subseteq T_1 - R\) with \(|I_0| = |I_1| = 0.24n\), and sends \(|I_0, I_1\rangle\) in random order to Alice.

(V) Alice picks a random \(s \in \{0, 1\}\), and sends \(s, \beta_s = b \bigoplus_{i \in I_s} g_i\) to Bob. Bob computes

\[ b = \beta_s \oplus h_i \text{ if } I_s \subseteq T_0, \text{ otherwise does nothing.} \]

If QBC instead of BCCC is used as the BC protocol in step (II), Bob can make use of its limitation to enable a so-called honest-but-curious attack \([104–107]\), as shown below. For each \(\phi_i (i = 1, \ldots, n)\), Bob does not pick a classical \(b_i\) and measure it in step (II). Instead, he introduces two ancillary qubit systems \(B_i\) and \(H_i\) as storage for the bits \(b_i\) and \(h_i\), and prepares their initial states as \(|B_i\rangle = (|0\rangle + |1\rangle)/\sqrt{2}\) and \(|H_i\rangle = |0\rangle_{H_i}\), respectively. Here \(|0\rangle\) and \(|1\rangle\) are orthogonal. Then, he applies the unitary transformation

\[ U_1 \equiv |0\rangle_B |0\rangle |0\rangle_\phi (0, 0) \otimes I_H + |0\rangle_B |0\rangle |0\rangle_\phi (0, 1) \otimes \sigma_H^{(x)} \]

\[ + |1\rangle_B |1\rangle |0\rangle_\phi (1, 0) \otimes I_H + |1\rangle_B |1\rangle |1\rangle_\phi (1, 1) \otimes \sigma_H^{(x)} \]  

(11)
on the incremented system \(B_i \otimes \phi \otimes H_i\). Here, \(I_H\) and \(\sigma_H^{(x)}\) are the identity operator and the 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 \(|B_i\rangle = |0\rangle_B\) (\(|B_i\rangle = |1\rangle_B\)), then measures qubit \(\phi_i\) in the basis \(h_i = 0, b_i = 1\), and stores the result \(h_i\) in system \(H_i\). It is different 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 QBC protocol which does not satisfy the definition of BCCC. For example, to commit \(b_i\) in our QBC protocol, Bob further introduces two ancillary systems \(E\) and \(\Psi\) and prepares the initial state as

\[ |E \otimes \Psi\rangle_0 = N \sum_{c \in C_{00}} |e_c\rangle \otimes |\Psi_c\rangle, \]

(12)
where \(N\) is the normalization constant. Let \(U_{E \otimes \Psi}\) be a unitary transformation on \(E \otimes \Psi\) which can map each \(|e_c\rangle \otimes |\Psi_c\rangle (c \in C_{00})\) into a \(|e_c\rangle \otimes |\Psi_c\rangle (c \in C_{11})\), i.e. it satisfies \(U_{E \otimes \Psi} |E \otimes \Psi\rangle_0 = N \sum_{c \in C_{00}} |e_c\rangle \otimes |\Psi_c\rangle\). Bob applies the unitary transformation

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

(13)
on the incremented 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 \(B_i \otimes \phi \otimes H_i \otimes E \otimes \Psi\) will be very similar to equation (7) if we view \(B_i \otimes \phi \otimes H_i \otimes E\) as system \(A\). Then, Bob can follow the process after equation (7) (note that now Bob becomes the sender of the commitment while Alice becomes the receiver) 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 remaining \((b_i, h_i)\) (\(i \neq R\)) are still kept at the quantum level. After Alice announces 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 \(T_i\) for each \(i \in T_0 \cup T_1 - R\) initialized in the state \(|T_i\rangle = |0\rangle_T\). Then, he applies the unitary transformation

\[
U_3 = |0\rangle_S \langle 0| \otimes |a_i\rangle_B \otimes I_T + |0\rangle_S \langle 0| \otimes |a_i\rangle_B (\langle a_i| \otimes \sigma^{(i)}_T)
\]

\[
\quad + |1\rangle_S \langle 1| \otimes |a_i\rangle_B \otimes \sigma^{(i)}_T + |1\rangle_S \langle 1| \otimes |a_i\rangle_B (\langle a_i| \otimes I_T) \quad (14)
\]

on the incremented system \(S' \otimes B_i \otimes T_i\). Here, \(I_T\) and \(\sigma^{(i)}_T\) are the identity operator and the Pauli matrix of system \(T_i\), that satisfy \(I_T|0\rangle_T = |0\rangle_T\) and \(\sigma^{(i)}_T|0\rangle_T = |1\rangle_T\), respectively. The effect of \(U_3\) is to compare \(a_i\) with \(b_i\) and store the result (\(a_i \neq b_i\) or \(s'\) in \(T_i\)). Bob then measures all \(T_i\) \((i \in T_0 \cup T_1 - R)\) in the basis \(|0\rangle_T, |1\rangle_T\), takes \(T_0(T_1)\) as the set of all \(1 \leq i \leq n\) with \(|T_i\rangle = |0\rangle_T\) \((|T_i\rangle = |1\rangle_T\) instead of how they are defined in step (IV) and finishes the rest parts of the QOT protocol.

With this method, the divisions of \(I_0, I_1\) are kept at the quantum level. Let \(I_m, (I_\mu)\) denote the set corresponding to \(a_i = b_i \neq h_i\). We can see that \(U_3\) makes \(I_0 = I_m, I_1 = I_\mu\) when \(s' = 0\), while \(I_0 = I_\mu, I_1 = I_m\) when \(s' = 1\). Since \(S'\) was initialized as \(|s'\rangle = (|0\rangle_S + |1\rangle_S)/\sqrt{2}\), the actual result of step (IV) can be described by

\[
|S' \otimes \left( \bigotimes_i B_i \otimes \phi_i \otimes H_i \otimes E'_i \right) \rangle \rightarrow |\Phi_0\rangle = (|0\rangle_S \otimes |I_0 = I_m \vee I_1 = I_\mu\rangle)
\]

\[
\quad + |1\rangle_S \otimes |I_0 = I_\mu \vee I_1 = I_m\rangle)/\sqrt{2}, \quad (15)
\]

where \(E'_i\) stands for all the ancillary systems Bob introduced in the process of committing \((b_i, h_i)\). Suppose that Bob announces \([I_0, I_1]_\mu\) in their original order to Alice. i.e. he never announces them in the order \([I_1, I_0]\). After Alice announces \(s\) and \(\beta_i\) in step (V), the systems under Bob’s possession can be viewed as

\[
|\Phi_b\rangle = (|s\rangle_S \otimes |I_0 = I_m\rangle + |\neg s\rangle_S \otimes |\text{fail}\rangle)/\sqrt{2}. \quad (16)
\]

It means that if Bob measures system \(S'\) in the basis \(|0\rangle_S, |1\rangle_S\) and the result \(|s'\rangle_S\) satisfies \(s' = s\), then he is able to measure the rest of the systems and 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, that at this stage a dishonest Bob can choose not to measure \(S'\) in the basis \(|0\rangle_S, |1\rangle_S\). Instead, by denoting \(|b\rangle \equiv |s\rangle_S \otimes |I_0 = I_m\rangle\), and \(|?\rangle \equiv |\neg s\rangle_S \otimes |\text{fail}\rangle\), equation \((16)\) becomes \(|\Phi_b\rangle = (|b\rangle + |?\rangle)/\sqrt{2}\) where \(|b = 0\rangle = (1 \ 0 \ 0)^T\), \(|b = 1\rangle = (0 \ 1 \ 0)^T\), and \(|?\rangle = (0 \ 0 \ 1)^T\) are mutually orthogonal. Then, according to equation (33) of [104], Bob can distinguish them using the positive operator-valued measure (POVM) \((E_0, I - E_0)\), where

\[
E_0 = \frac{1}{6} \begin{bmatrix}
2 + \sqrt{3} & -1 & 1 + \sqrt{3} \\
-1 & 2 - \sqrt{3} & 1 - \sqrt{3} \\
1 + \sqrt{3} & 1 - \sqrt{3} & 2
\end{bmatrix}. \quad (17)
\]

This allows Bob’s decoded \(b\) to match Alice’s actual input with reliability \((1 + \sqrt{3}/2)/2\). 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 other 1/2 cases, where 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 successful cheating, as the strategy does not even accomplish what
an honest Bob can do. That is why it is called *honest*-but-curious behavior [105, 106]. The existence of this loophole may actually come from the fact that in the literature, there is a lack of a self-consistent definition of OT specifically made for the quantum case. That is, the goal ‘reaching reliability 100% and 50% with equal probabilities’ may conflict with ‘reaching a maximal average reliability 75% with probability 100% ‘ by nature, so that it seems unrealistic to require a protocol to satisfy both goals simultaneously. Therefore, it is somewhat unfair to consider it as a limitation on the power of quantum cryptography itself. Nevertheless, as this honest-but-curious behavior provides Bob with the freedom to choose between accomplishing the original goal of QOT and achieving a higher average reliability, it may leave rooms for potential problems when we want to build even more complicated cryptographic protocols upon such a QBC-based QOT.

Despite this limitation, our QBC protocol can still be used to build many other ‘post-cold-war era’ multi-party quantum cryptographic protocols. For example, since it makes committing a single bit possible, then repeating the protocol many times immediately enables quantum bit string commitment (QBSC) [108]. Also, building quantum strong coin tossing (QCT, a.k.a. quantum coin flipping) [3] with an arbitrarily small bias is straightforward. Alice and Bob first execute our commit protocol. Then, Bob announces a random bit $x$ classically. Finally, Alice unveils her committed bit $b$, and the two parties accept $y \equiv b \oplus x$ as the coin tossing result. It is trivial to show that even if Alice kept $b$ at the quantum level until the unveil phase by using the state equation (7), she cannot bias the final $y$ since she cannot change the probabilities $p_0, p_1$. Note that these results suggest that all the existing no-go proofs of QBSC (e.g. [109, 110]) and QCT (e.g. [33, 111–114]) are incorrect. This is not surprising because all these no-go proofs are also based on some conditions similar to $\rho_B^0 \simeq \rho_B^1$, or even built directly on top of the no-go theorem of QBC, which are all inapplicable to our case.

### 6. Feasibility

Our protocol is very feasible. The QKD scheme [91] we based on was already experimentally implemented recently [99]. By comparing figures 1 and 2 it can clearly be seen that our QBC protocol can be implemented with exactly the same devices as in [99]. Thus, the QBSC and QCT protocols built upon our QBC protocol are also straightforward with currently available technology. Moreover, as mentioned in section 3, the protocol can easily be made fault-tolerant against noisy quantum channels. Therefore it is extremely practical.

Comparing with the unconditionally secure BC protocols based on relativity [53, 54, 56, 57], our protocol reaches the same security level, while the implementation is more convenient. This is because in all these relativistic BC, both Alice and Bob must have agents to help them carry out the protocols. Therefore, it is in fact no longer a two-party cryptography, as BC should have been. Also, Alice and Bob must be separated from their agents by a distance on the relativistic scale, i.e. they need to be so far apart that they cannot exchange information in time. All these requirements obviously limit the application of their protocols.

In [100], a variation of the QKD scheme in [91] was proposed, which replaced the symmetric (equal transmissivity and reflectivity) beam splitters $BS_1$ and $BS_2$ in figure 1 of our paper with asymmetric ones. The advantage is that the sending time of the qubits no longer needs to be random. The same idea may also apply to our protocol to bring the same advantage.

However, it is important to note that the beam splitters can be half-silvered mirrors or similar types, but must not be polarizing beam splitters. This is because the QKD scheme [91] we based on will become insecure if polarizing beam splitters are used. Let $|H\rangle$ ($|V\rangle$) denote the horizontally (vertically) polarized state that will always be transmitted (reflected) by polarizing beam splitters. Eve can simply use the same device of Charlie to measure all
states that come from Alice. Then, depending on which one of her detectors clicks, she can send $|H\rangle$ ($|V\rangle$) to Charlie through channel B (in figure 1) only, let alone channel A. This can make Charlie’s detector $D_1$ ($D_0$) click with certainty, so that Charlie always receives the same result as hers and therefore her cheating can be covered. But if half-silvered mirrors or similar types of beam splitters are used, when Eve sends a state to Charlie through channel B alone, both of Charlie’s detectors $D_1$ and $D_0$ will have non-vanishing probabilities to click so that Eve cannot control the result with certainty. Then, the eavesdropping will not be successful, just as shown in the security proof in [91].

7. Relationship with the CBH theorem

The above result is also useful for developing understanding of fundamental theories. The CBH theorem [93] is an attractive attempt to raise some information-theoretic constraints to the level of fundamental laws of nature, from which quantum theory can be deduced. These constraints were suggested to be three ‘no-go’s’, which are (I) the impossibility of superluminal information transfer, (II) the impossibility of perfectly broadcasting an unknown state and (III) the impossibility of unconditionally secure BC. It was worked out in [93] that these three constraints can jointly entail three definitive physical characteristics of quantum theory, i.e. kinematic independence (a.k.a. microcausality), noncommutativity and nonlocality. Meanwhile, to show that these three characteristics and the above three information-theoretic constraints are exactly equivalent, it is necessary to prove conversely that the three characteristics can entail the three constraints. This was only partly accomplished in [93]. It was demonstrated that the first two characteristics can entail constraints (I) and (II). What was left undone is the derivation of constraint (III). Note that some people believe that the problem was solved later by [47]. But in fact the no-go proof of QBC in [47] was also based on the condition $\rho_B^0 \simeq \rho_B^1$, which fails to cover our protocol. Thus, the derivation of constraint (III) is still incomplete. In our understanding, this situation is yet further evidence indicating that the MLC no-go theorem of unconditionally secure QBC is not a necessary deduction of quantum mechanics. In fact, the reason why the MLC theorem was included in the three constraints, simply put, is because it can entail nonlocality. As can be seen from features (ii) and (iv) in the above brief review of the MLC theorem, Alice can cheat in QBC only when she has the capability to manipulate entangled states. That is, the MLC theorem can be valid only if the physical world allows entanglement, which is a typical example of nonlocality. However, our QBC protocol also entails nonlocality. According to [98], equation (1) can be rewritten using the standard notations of quantum optics as

$$|\Psi_0\rangle = \frac{|0\rangle|1\rangle + |1\rangle|0\rangle}{\sqrt{2}},$$

$$|\Psi_1\rangle = \frac{|0\rangle|1\rangle - |1\rangle|0\rangle}{\sqrt{2}},$$

(18)

where the first and second kets refer to the two quantum communication channels, and the 0 and 1 inside the kets refer to the photon number. This indicates that Alice’s transmitted states in fact contain single-photon nonlocality. The resultant QBC can be executed only when Alice has the capability to create such nonlocality. Otherwise, if Alice merely sends both wave packets of a photon simultaneously into the quantum communication channels, i.e. nonlocality is not fully utilized, then Bob can easily intercept, clone and resend all these orthogonal states without being detected. That is, our result indicates that QBC can be unconditionally secure only if there is nonlocality in the physical world. This somewhat clarifies why most previously proposed QBC protocols (e.g. [3, 4]) are insecure. In these protocols, if Alice wants to commit honestly, then sending Bob pure states unentangled with any system at Alice’s side is already sufficient. Nonlocality is not entailed when these protocols are supposed to be executed honestly. Thus, it
is not surprising that a dishonest party who is capable of manipulating entangled states can gain more advantages than is allowed in these protocols. On the contrary, in our protocol Alice who only sends unentangled pure states will no longer be considered as honest. Nonlocality becomes a must. Thus, we can see that no matter if the MLC theorem is correct or our QBC protocol could indeed be unconditionally secure, nonlocality is entailed in both cases. Therefore, we tend to believe that the (im)possibility of unconditionally secure QBC is irrelevant to the goal of characterizing quantum theory in terms of information-theoretic constraints. To complete the CBH theorem, we may need to seek for another information-theoretic principle as the third constraint.

8. Summary

We show that if a formerly proposed QKD scheme based on orthogonal states [91] is secure, it can be used to build a QBC protocol which remains concealing while the reduced density matrix $\rho_B^0$ of the state Bob received satisfies $\rho_B^0 \perp \rho_B^1$. Thus, it evades the MLC no-go theorem [5–8], [31–52] which is valid for the case $\rho_B^0 \simeq \rho_B^1$ only. The resultant QBC protocol is not a bit commitment with a certificate of classicality; thus, it cannot lead to unconditionally secure quantum oblivious transfer in the traditional way. But it can lead to quantum bit string commitment and quantum strong coin tossing. This finding suggests that a different principle other than the MLC no-go theorem is needed for the CBH theorem to completely characterize quantum theory in terms of information-theoretic constraints.

Acknowledgments

The work was supported in part by the NSF of China under grant no 10975198, the NSF of Guangdong province under grant no 9151027501000043 and the Foundation of Zhongshan University Advanced Research Center.

References

[1] Yao A C C 1995 Security of quantum protocols against coherent measurements Proc. 26th Symp. on the Theory of Computing (New York: ACM) p 67
[2] Kilian J 1988 Founding cryptography on oblivious transfer Proc. 1988 ACM Annu. Symp. on Theory of Computing (New York: ACM) p 20
[3] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution and coin tossing Proc. IEEE Int. Conf. on Computers, Systems, and Signal Processing (New York: IEEE) p 175
[4] Brassard G, Crépeau C, Jozsa R and Langlois D 1993 A quantum bit commitment scheme provably unbreakable by both parties Proc. 34th Annu. IEEE Symp. on Foundations of Computer Science (Los Alamitos, CA: IEEE) p 362
[5] Mayers D 1996 The trouble with quantum bit commitment arXiv: quant-ph/9603015v3
[6] Mayers D 1996 Unconditionally secure quantum bit commitment is impossible Proc. 4th Workshop on Physics and Computation (New England Complex System Institute, Boston, MA) p 226
[7] Mayers D 1997 Unconditionally secure quantum bit commitment is impossible Phys. Rev. Lett. 78 3414
[8] Lo H-K and Chau H F 1997 Is quantum bit commitment really possible? Phys. Rev. Lett. 78 3410
[9] Yuen H P 2008 Impossibility proofs and quantum bit commitment arXiv:0808.2040v1
[10] Yuen H P 2000 Unconditionally secure quantum bit commitment is possible arXiv:quant-ph/0006109v7
[11] Yuen H P 2000 Anonymous-key quantum cryptography and unconditionally secure quantum bit commitment arXiv:quant-ph/0009113v1
[12] Yuen H P 2001 Unconditional security in quantum bit commitment arXiv:quant-ph/0106001v1
[13] Yuen H P 2001 How unconditionally secure quantum bit commitment is possible arXiv:quant-ph/0109055v2
[14] Yuen H P 2002 Quantum bit commitment and unconditional security arXiv:quant-ph/0207089v3
[15] Yuen H P 2002 Why there is no impossibility theorem on secure quantum bit commitment arXiv:quant-ph/0210206v1
[16] Yuen H P 2003 A simple unconditionally secure quantum bit commitment protocol via quantum teleportation arXiv:quant-ph/0305142v3
[17] Yuen H P 2003 Another simple unconditionally secure quantum bit commitment protocol—beating entanglement with entanglement arXiv:quant-ph/0305143v3
[18] Yuen H P 2003 How to build unconditionally secure quantum bit commitment protocols arXiv:quant-ph/0305144v3
[19] Yuen H P 2005 Unconditionally secure quantum bit commitment arXiv:quant-ph/0505132v1
[20] Yuen H P 2007 QBC3: an unconditionally secure quantum bit commitment protocol arXiv:0702074v4
[21] Mitra A 2000 Unconditionally secure quantum bit commitment is simply possible arXiv:physics/0007089v3
[22] Cheung C-Y 2001 Quantum bit commitment can be unconditionally secure arXiv:quant-ph/0112120v3
[23] Srikanth R 2001 Securing quantum bit commitment through reverse quantum communication arXiv:quant-ph/0112172v2
[24] Srikanth R 2004 Quantum bit commitment with a composite evidence Phys. Scr. 70 343 (arXiv:quant-ph/0306155v4)
[25] Shimizu K and Imoto N 2002 Communication channels analogous to one out of two oblivious transfers based on quantum uncertainty Phys. Rev. A 66 052316
[26] Shimizu K and Imoto N 2003 Communication channels analogous to one out of two oblivious transfers based on quantum uncertainty: II. Closing EPR-type loopholes Phys. Rev. A 67 034301
[27] Yang L and Li B 2006 Unconditionally secure quantum bit commitment protocols based on correlation immune Boolean function arXiv:quant-ph/0607089v6
[28] Prasath S E and Panigrahi P K 2009 One way quantum bit commitment through classical correlation arXiv:0909.3117v1
[29] Srikanth R 2003 private communication
[30] Yuen H P 2003 private communication
[31] Crépeau C 1996 What is going on with quantum bit commitment? Proc. Pragocrypt ’96: 1st Int. Conf. on the Theory and Applications of Cryptology (Prague: Czech Technical University Publishing House)
[32] Chau H F and Lo H-K 1998 Making an empty promise with a quantum computer Fortsch. Phys. 46 507 (arXiv:quant-ph/9709053v2)
[33] Lo H-K and Chau H F 1998 Why quantum bit commitment and ideal quantum coin tossing are impossible Physica D 120 177
[34] Brassard G, Crépeau C, Mayers D and Salvail L 1998 The security of quantum bit commitment schemes Proc. Randomized Algorithms, Satellite Workshop of 23rd Int. Symp. on Mathematical Foundations of Computer Science
[35] Bub J 2001 The quantum bit commitment theorem Found. Phys. 31 735
[36] Brassard G, Crépeau C, Mayers D and Salvail L 1997 A brief review on the impossibility of quantum bit commitment arXiv:quant-ph/9712023v1
[37] Brassard G, Crépeau C, Mayers D and Salvail L 1998 Defeating classical bit commitments with a quantum computer arXiv:quant-ph/9806031v1
[38] Spekkens R W and Rudolph T 2001 Degrees of concealment and bindiness in quantum bit commitment protocols Phys. Rev. A 65 012310
[39] Spekkens R W and Rudolph T 2002 Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol Quant. Inf. Comput. 2 66 (arXiv:quant-ph/0107042v2)
[40] Chailloux A and Kerenidis I 2011 Optimal bounds for quantum bit commitment arXiv:1102.1678v1
[41] D’Ariano G M 2002 The quantum bit commitment: a finite open system approach for a complete classification of protocols arXiv:quant-ph/0209149v1
[42] D’Ariano G M 2002 The quantum bit commitment: a complete classification of protocols Proc. QCM&C (Boston, MA: Rinton Press) (arXiv:quant-ph/0209150v1) (shortened version of arXiv:quant-ph/0209149)
[43] D’Ariano G M, Kretschmann D, Schlingemann D and Werner R F 2007 Reexamination of quantum bit commitment: the possible and the impossible Phys. Rev. A 76 032328 (arXiv:quant-ph/0605224v2)
[44] Chiribella G, D’Ariano G M, Perinotti P, Schlingemann D M and Werner R F 2009 A short impossibility proof of quantum bit commitment arXiv:0905.3801v1
[45] Mayers D 2002 Superselection rules in quantum cryptography arXiv:quant-ph/0212159v2
[46] Kitaev A, Mayers D and Preskill J 2004 Superselection rules and quantum protocols Phys. Rev. A 69 052326
[47] Halvorson H 2004 Remote preparation of arbitrary ensembles and quantum bit commitment J. Math. Phys. 45 4920 (arXiv:quant-ph/0310001v2)
[48] Cheung C-Y 2005 Secret parameters in quantum bit commitment protocol Proc. ERATO Conference on Quantum Information Science (Tokyo) (arXiv:quant-ph/0508180v2)
[49] Cheung C-Y 2006 Insecurity of quantum bit commitment with secret parameters arXiv:quant-ph/0601206v1
[50] Magnin L, Magniez F, Leverrier A and Cerf N J 2010 Strong no-go theorem for Gaussian quantum bit commitment Phys. Rev. A 81 010302(R) (arXiv:0905.3419v2)
[51] Chiribella G, D’Ariano G M and Perinotti P 2010 Probabilistic theories with purification Phys. Rev. A 81 062348 (arXiv:0908.1583v5)
[52] Li Q, Li C Q, Long D-Y, Chan W H and Wu C-H 2011 On the impossibility of non-static quantum bit commitment between two parties arXiv:1101.5684v1
[53] Kent A 1999 Unconditionally secure bit commitment Phys. Rev. Lett. 83 1447
[54] Kent A 2005 Secure classical bit commitment using fixed capacity communication channels J. Cryptol. 18 313 (arXiv:quant-ph/9906103v7)
[55] Moran T and Naor M 2005 Basing cryptographic protocols on tamper-evident seals Proc. ICALP 2005 (Lecture Notes in Computer Science vol 3580) ed L Caires, G F Italiano, L Monteiro, C Palamidessi and M Yung (Berlin: Springer) p 285
[56] Kent A 2011 Unconditionally secure bit commitment with flying qudits arXiv:1101.4620v3
[57] Kent A 2011 Unconditionally secure bit commitment by transmitting measurement outcomes arXiv:1101.4620v3
[58] Yu B, Zhou Z W, Li J and Guo G C 2002 Secure bit commitment based on quantum one-way function Proc. SPIE 4917 92
[59] Tanaka K 2003 Quantum bit-commitment for small storage based on quantum one-way permutations New Generat. Comput. 21 339
[60] Chailloux A, Kerenidis I and Rosgen B 2010 Quantum commitments from complexity assumptions arXiv:1010.2793v2
[61] Yang L, Xiang C and Li B 2010 Qubit-string-based bit commitment protocols with physical security arXiv:1011.5099v2
[62] Brassard G and Crépeau C 1991 Quantum bit commitment and coin tossing protocols Advances in Cryptology: CRYPTO ’90 ( Lecture Notes in Computer Science vol 537) ed A J Menezes and S A Vanstone (Berlin: Springer) p 99
[63] Shimizu K and Imoto N 2002 Fault-tolerant simple quantum-bit commitment unbreakable by individual attacks Phys. Rev. A 65 032324
[64] Salvail L 1998 Quantum bit commitment from a physical assumption Advances in Cryptology: CRYPTO ’98 ( Lecture Notes in Computer Science vol 1462) (Berlin: Springer) p 338
[65] Harrow A, Oliveira R and Terhal B M 2006 Quantum bit commitment with misaligned reference frames Phys. Rev. A 73 032311
[66] Damgård I, Fehr S, Salvail L and Schaffner C 2005 Cryptography in the bounded quantum-storage model 2005 Proc. FOCS, 46th Annu. IEEE Symp. on Foundations of Computer Science (Piscataway, NJ: IEEE) p 449 (arXiv:quant-ph/0508222v2)
[67] Damgård I B, Fehr S, Renner R, Salvail L and Schaffner C 2007 A tight high-order entropic quantum uncertainty relation with applications Advances in Cryptology: CRYPTO 2007 ( Lecture Notes in Computer Science vol 4622) (Berlin: Springer) (arXiv:quant-ph/0612014v2)
[68] Wehner S and Wullschleger J 2008 Composable security in the bounded-quantum-storage model Proc. ICALP 2008 ( Lecture Notes in Computer Science vol 5126) (Berlin: Springer) p 604 (arXiv:0709.0492v1)
[69] Ramos R V and Mendonca F A 2008 Quantum bit commitment protocol without quantum memory arXiv:0801.0690v1
[70] Koenig R, Wehner S and Wullschleger J 2009 Unconditional security from noisy quantum storage arXiv:0906.1030v4
[71] Wehner S, Curty M, Schaffner C and Lo H-K 2010 Implementation of two-party protocols in the noisy-storage model Phys. Rev. A 81 052336 (arXiv:0911.2302v2)
[72] Cheung C Y 2006 Secure quantum bit commitment using unstable qubits arXiv:quant-ph/0603154v3
[73] Cheung C Y 2009 Unconditionally secure quantum bit commitment using neutron double-slit interference arXiv:0910.2645v4
[74] Mandilara A and Cerf N J 2011 Quantum bit commitment under Gaussian constraints arXiv:1105.2140v1
[75] Langford N K, Dalton R B, Harvey M D, O’Brien J L, Pryde G J, Gilchrist A, Bartlett S D and White A G 2004 Measuring entangled qutrits and their use for quantum bit commitment Phys. Rev. Lett. 93 053601
[76] Mendonca F A and Ramos R V 2007 Quantum bit string commitment protocol using polarization of mesoscopic coherent states arXiv:quant-ph/0703080v1
[77] Buhrman H, Christandl M, Unger F, Wehner S and Winter A 2006 Implications of superstrong nonlocality for cryptography Proc. R. Soc. A 462 1919 (arXiv:quant-ph/0504133v3)
[78] Short T, Gisin N and Popescu S 2005 The physics of no-bit-commitment: generalized quantum non-locality versus oblivious transfer arXiv:quant-ph/0504134v1
[79] Barnum H, Dahlsten O C O, Leifer M and Toner B 2008 Nonclassicality without entanglement enables bit commitment Proc. IEEE Information Theory Workshop (Piscataway, NJ: IEEE) p 386 (arXiv:0803.1264v1)

[80] Winkler S, Wolf S and Wullschleger J 2008 Bit commitment from non-sampling correlations arXiv:0811.3589v2

[81] Dumais P, Mayers D and Salvail L 2000 Perfectly concealing quantum bit commitment from any quantum one-way permutation Advances in Cryptology: EUROCRYPT ’00 (Lecture Notes in Computer Science vol 1807) (Berlin: Springer) p 305

[82] Silman J, Chailloux A, Aharon N, Kerenidis I, Pironio S and Massar S 2011 Fully distrustful quantum bit commitment and coin flipping Phys. Rev. Lett. 106 220501 (arXiv:1101.5086v2)

[83] Hardy L and Kent A 2004 Cheat sensitive quantum bit commitment and coinflipping Phys. Rev. Lett. 92 157901 (arXiv:quant-ph/0409143v5)

[84] Aharonov D, Ta-Shma A, Vazirani U V and Yao A C 2000 Quantum bit escrow Proc. 32nd Annua. Symp. on Theory of Computing (New York: ACM) 705 (arXiv:quant-ph/0004017v1)

[85] Ishizaka S 2008 Dilemma that cannot be resolved by biased quantum coin flipping Phys. Rev. Lett. 100 070501 (arXiv:quant-ph/0703099v5)

[86] Shimizu K, Fukasaka H, Tamaki K and Imoto N 2011 Cheat-sensitive commitment of a classical bit coded in a block of m×n round-trip qubits Phys. Rev. A 84 022308

[87] DrVincenzo D P, Leung D W and Terhal B M 2002 Quantum data hiding IEEE Trans. Inf. Theory 48 580 (arXiv:quant-ph/0103098v1)

[88] Wang L-C, Cao Z-F, Cao F, Qian H-F and Bao H-Y 2008 Biased bit commitment and applications J. Inf. Sci. Eng. 24 444

[89] Choi J W, Hong D, Chang K-Y and Chi D P 2009 Non-static quantum bit commitment arXiv:0901.1178v4

[90] Kossbiha T and Odara T 2011 Non-interective stastically-hiding quantum bit commitment from any quantum one-way function arXiv:1102.3441v1

[91] Goldenberg L and Vaidman L 1995 Quantum cryptography based on orthogonal states Phys. Rev. Lett. 75 1239

[92] Goldenberg L and Vaidman L 1996 Reply to ‘Quantum cryptography with orthogonal states?’ Phys. Rev. Lett. 77 3265

[93] Clifton R, Bub J and Halvorson H 2003 Characterizing quantum theory in terms of information-theoretic constraints Found. Phys. 33 1561 (arXiv:quant-ph/0211089v2)

[94] Ekert A K 1992 Quantum cryptography based on Bell’s theorem Phys. Rev. Lett. 67 661

[95] Bennett C H 1992 Quantum cryptography using any two nonorthogonal states Phys. Rev. Lett. 68 3121

[96] Kent A 2000 Unconditionally secure commitment of a certified classical bit is impossible Phys. Rev. A 61 042301 (arXiv:quant-ph/9911087v2)

[97] Hughstont L P, Joza R and Wootters W K 1993 A complete classification of quantum ensembles having a given density matrix Phys. Lett. A 183 14

[98] Peres A 1996 Quantum cryptography with orthogonal states? Phys. Rev. Lett. 77 3264

[99] Avella A, Brida G, Degiovanni I P, Genovesi M, Gramegna M and Tramai P 2010 Experimental quantum-cryptography scheme based on orthogonal states Phys. Rev. A 82 062309

[100] Koashi M and Imoto N 1997 Quantum cryptography based on split transmission of one-bit information in two steps Phys. Rev. Lett. 79 2383

[101] Rabin M O 1981 How to exchange secrets by oblivious transfer Technical Report TR-81 Aiken Computation Laboratory, Harvard University (available online at http://eprint.iacr.org/2005/187.pdf)

[102] Crépeau C 1994 Quantum oblivious transfer J. Mod. Opt. 41 2445

[103] Crépeau C and Kilian J 1988 Achieving oblivious transfer using weakened security assumptions Proc. 29th Symp. on Foundations of Computer Science (New York: IEEE) p 42

[104] Colbeck R 2007 Impossibility of secure two-party classical computation Phys. Rev. A 76 062308 (arXiv:0708.2845v2)

[105] Salvail L, Schaffner C and Sotakova M 2009 On the power of two-party quantum cryptographyASIACRYPT (Lecture Notes in Computer Science vol 5912) (Berlin: Springer) p 70 (arXiv:0902.4036v2)

[106] Salvail L and Sotakova M 2009 Two-party quantum protocols do not compose securely against honest-but-curious adversaries arXiv:0906.1671v2

[107] Colbeck R 2009 Quantum and relativistic protocols for secure multi-party computation PhD Thesis University of Cambridge (arXiv:0911.3814v1)

[108] Kent A 2003 Quantum bit string commitment Phys. Rev. Lett. 90 237901

[109] Buhrman H, Christandl M, Hayden P, Lo H-K and Wehner S 2006 Security of quantum bit string commitment depends on the information measure Phys. Rev. Lett. 97 250501 (arXiv:quant-ph/0609237v2)

[110] Buhrman H, Christandl M, Hayden P, Lo H-K, and Wehner S 2008 Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment Phys. Rev. A 78 022316 (arXiv:quant-ph/0504078v2)
[111] Ambainis A 2004 A new protocol and lower bounds for quantum coin flipping J. Comput. Syst. Sci. 68 398 (arXiv:quant-ph/0204022v1) (earlier version in Proc. STOC’01)

[112] Kitaev A 2003 A negative result about quantum coin flipping Lecture delivered at the 2003 Annu. Quantum Information Processing (QIP) Workshop (Berkeley, CA: Mathematical Sciences Research Institute) (unpublished) (available online at http://www.msri.org/publications/video/index05.html)

[113] Nayak A and Shor P 2003 Bit-commitment-based quantum coin flipping Phys. Rev. A 67 012304

[114] Hanggi E and Wullschleger J 2011 Tight bounds for classical and quantum coin flipping Proc. TCC 2011 (Brown University) p 468 (arXiv:1009.4741v2)