Unconditionally Secure Quantum Bit Commitment and Quantum Oblivious Transfer

Ping Wang, Yikang Lei and Yiting Su

Shenzhen University, Shenzhen 518060, China
wangping@szu.edu.cn, leiyikang2022@email.szu.edu.cn,
suyiting2020@email.szu.edu.cn
Dec 19, 2023

Abstract. Recently, a novel secure quantum bit commitment (QBC) protocol has been proposed [29]. However, the protocol requires Alice and Bob to share Bell states in advance, making the protocol lacking in practicality. In this paper, we propose two new unconditionally secure quantum bit commitment protocols that do not require pre-shared Bell states based on entangled and non-entangled states, respectively. Their security stems from quantum mechanical properties such as quantum superposition, quantum entanglement, no-cloning theorem, and no-communication theorem. Furthermore, by combining the proposed QBC with Yao's quantum oblivious transfer (QOT) model, we can obtain an unconditionally secure QOT protocol.

Keywords: unconditionally secure, quantum bit commitment, quantum oblivious transfer

1 Introduction

Quantum bit commitment (QBC) and quantum oblivious transfer (QOT) protocols play an important role in the field of cryptography. The quantum bit commitment protocol is a quantum communication protocol implemented based on the principles of quantum mechanics. Bit commitment was first proposed by Wiesner [31], and although his paper was not published until 1983, it is of great importance in quantum information theory. In QBC, Alice first commits a bit value (0 or 1) to Bob and sends the corresponding evidence of this commitment to Bob. After receiving the evidence, Bob does not have access to any information about the commitment value (hiding). In the opening phase, Alice provides Bob with proof of the commitment, and Bob then verifies the validity of the commitment. Once Alice has made a commitment, it cannot be modified (binding). A secure bit commitment protocol would be applicable to the construction of zero-knowledge proofs [32], oblivious transfer protocols [33], and coin flips [26].

Quantum oblivious transfer is a quantum cryptographic protocol that allows for the secure transfer of information between two parties while preserving privacy. It finds important applications in areas such as secure multi-party computation [13], secret sharing [28], digital signatures [16], and signing contracts

[10]. The concept of oblivious transfer was first introduced by Rabin [23] in 1981. In this protocol, Alice sends a message to Bob in a two-party communication, where Bob has a 1/2 probability of accessing the message, but Alice remains completely unaware of whether Bob receives it. Subsequently, a more practical one-out-of-two oblivious transfer scheme was proposed in 1985 [10], which differs from Rabin's initial scheme. In the one-out-of-two oblivious transfer scheme, Alice has two messages, m_1 and m_2, and Bob can access one of them, either m_1 and m_2, without Alice knowing which one Bob has accessed. One of the implementations of the classical one-out-of-two oblivious transfer protocol is based on public-key cryptography, such as RSA and ECC. The security of these cryptosystems relies on the difficulty of integer factorization problems and elliptic curve discrete logarithm problems. However, the emergence of the Shor [25] algorithm demonstrated the ability to solve these problems in quantum polynomial time. Therefore, with the advancement of quantum computing technology, the security of classical public-key cryptography will face significant challenges in the future.

In 1984, Bennett and Brassard proposed the first quantum key distribution protocol known as the BB84 protocol [3], This protocol leveraged the principles of quantum mechanics, specifically the quantum no-cloning theorem and quantum superposition properties, to securely transfer keys between two parties. This marked the formal introduction of cryptography into the quantum era. In 1995, a quantum key distribution protocol requiring only a few tens of bits of EPR particles was proposed [1], enabling a quantum bit commitment scheme. In 1988, Crépeau and Kilian [7] proposed the first quantum all-or-nothing oblivious transfer protocol; followed by Crépeau [6] scheme in 1994 to implement a one-out-of-two type QOT based on QBC. Yao [33] further demonstrated that a secure QOT protocol could be implemented based on a secure QBC.

Information-theoretical security refers to the assumption that an attacker with unlimited computational power cannot obtain information by breaking the protocol. However, subsequent proofs by Mayers [21], Lo, and Chau [19,20] revealed the insecurity of previously proposed QBC schemes, rendering the QOT protocols implemented based on them insecure. This led to the formulation of MLC's no-go theorem, indicating the impossibility of unconditionally secure QBC and QOT. In 1997, Lo [18] proposed Lo's no-go theorem, stating that there is no unconditionally secure oblivious transfer. Despite this, computationally secure QOT protocols have been proposed using the RSA or hash functions [30].

However, based on special relativity, Kent[14,15] has demonstrated that there exist unconditionally secure protocols for bit commitment that take advantage of the principle of special relativity stating that information cannot travel faster than light. Furthermore, Cheung [5] proved that the scope of the no-go theorem is not comprehensive, as not all cases can be exploited by a cheater using a perfect unitary transformation. He [12] also suggests that Lo's no-go theorem is not universally applicable, as BC-based one-out-of-two OT does not align with the OT model defined in Lo's no-go theorem, thus leaving some types of OT outside the scope of Lo's proof. In 2018, Li and Song [27] proposed a novel quantum

one-out-of-two type of oblivious transfer protocol based on the principle that non-orthogonal states cannot be reliably distinguished. They further developed a physically secure quantum bit commitment protocol using this OT scheme. The core idea of MLC's no-go theorem is that Alice can obtain evidence of commitment without performing measurements, allowing her to freely switch the committed value before the opening phase.

In fact, if we let Bob, instead of Alice, prepare the initial states, Alice cannot copy the quantum states she received due to the no-cloning theorem (Alice cannot get the exact information about the quantum states she received), or if we let Alice and Bob use the shared Bell states as the initial states, Alice cannot perform the entanglement attack. In this paper, we design two unconditionally secure bit commitment protocols based on entangled and non-entangled states, respectively, whose frameworks are out of the scope of MLC attacks. Moreover, by improving Yao's QOT model [33] and combining it with the proposed QBC protocol, we can get an unconditionally secure QOT protocol.

The paper is structured as follows: In Section 2, we provide an introduction to the preliminary knowledge that will be utilized in the design of the new protocols. In Section 3, we will describe the two quantum bit commitment schemes based on quantum superposition, quantum entanglement, no-cloning theorem, and no-communication theorem, and we will prove and analyze the *hiding* and *binding* properties of the two protocols, respectively. Section 4 focuses on an enhanced quantum oblivious transfer protocol derived from the proposed unconditionally secure bit commitment scheme. We provide a detailed description of the improved protocol and its security analysis. Finally, in Section 5, we conclude the paper.

2 Preliminaries

In this section, we will introduce the superposition principle, quantum entanglement, the Bell state, and the no-communication theorem as the basic tools that will be used in the proposed protocol.

2.1 Superposition Principle

Schrödinger [24] introduced the concept of the wave function, which aimed to describe certain quantum phenomena and proposed equations that describe the evolution of wave functions in quantum systems. These equations allow for the representation of linear combinations of different eigenstates, known as superposition states. The superposition principle in quantum mechanics states that when a quantum system can exist in multiple possible states, it can simultaneously exist in a linear combination of these states. These possible states are referred to as the eigenstates or ground states of the system. When the quantum system is measured, only one of the eigenstates can be observed, and the corresponding measurement outcome is obtained. Born's rule [4] provides a method to calculate the probability of observing a particular measurement outcome based on

the wave function. It states that the probability of observing a specific measurement outcome is equal to the square of the modulus of the probability amplitude between the eigenstate associated with the observed quantity and the wave function. In the quantum world, a system can exist in multiple possible states simultaneously, which is not possible in the classical world. However, when measured, the system will collapse into one of the states according to the corresponding probability, as determined by the superposition theorem.

2.2 Quantum Entanglement

In the quantum world, there exist states that cannot be directly expressed as a combination of two or more individual states. These states are known as entangled states. In a paper published in 1935 by Einstein et al. [9] proposed a thought experiment that describe a special correlation between two qubits. In this scenario, a measurement taken on one qubit instantly affects the other qubit, even if they are physically separated. This peculiar state between two qubits is referred to as entanglement. Assuming that $|0\rangle, |1\rangle$ denote the possible states of the two qubits, respectively, an entangled state can be represented as $|\Psi\rangle = \alpha|0\rangle + \beta|1\rangle$, where α and β are complex magnitude factors, and $|\alpha|^2 + |\beta|^2 = 1$. Quantum entanglement reflects the non-local nature of quantum mechanics, where the interconnectedness of quantum particles in an entangled state can instantaneously influence other qubits, even when they are spatially separated. In 1964, Bell [2] introduced a special type of quantum state called the Bell state. A Bell state is an entangled state consisting of two qubits and can be represented by the following wave function: $|\Psi\rangle_+ = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$; $|\Psi\rangle_+ = \frac{|00\rangle-|11\rangle}{\sqrt{2}}$; $|\Phi\rangle_+ = \frac{|++\rangle+|--\rangle}{\sqrt{2}}$; $|\Phi\rangle_+ = \frac{|++\rangle-|--\rangle}{\sqrt{2}}$. The nature of the Bell state is revealed in the fact that when the state of one qubit is measured, the state of the other qubit instantaneously collapses to the same or opposite state, regardless of the spatial separation between them. This property of entangled states is utilized in various applications in the field of quantum information.

2.3 No-communication Theorem

Quantum systems can often be represented as linear combinations of complex numbers, and this form can be used to calculate the probability of a quantum state collapsing to a particular state after a measurement. However, this does not mean that the collapse of the quanta can be controlled and accurately predicted. For example, for two mutually entangled particles, if a measurement is made on one of the particles, the result obtained is unpredictable until the measurement is made. However, immediately after the measurement is made, the quantum state of the other particle collapses to the corresponding state. It is not feasible to try to use this collapse of the quantum state to transfer a message because the collapse of the quantum state is unpredictable, and cannot be manipulated to transfer a specific message by manipulating the collapsed result. The no-communication theorem does not violate the principle of relativity because an

observer cannot use measurements of a part of an entangled quantum system to transmit a message to another observer in an instantaneous or FTL manner. As a corollary, assuming that Alice and Bob have two subsystems of entangled states, it is impossible for one party to get any information about the measurement of the subsystem from the other party through entanglement without additional information exchange. Further, we have the following no-communication theorem, the proof of which can be referred to [8,11,22].

Theorem 1 (No-communication Theorem). *Within the context of quantum mechanics, it is not possible for one observer, by making a measurement of a subsystem of the total state, whether entangled or not, to communicate information to another observer.*

The fundamental assumption underlying the theorem is that a quantum-mechanical system is prepared in an initial state that can be described as a mixed or pure state in a Hilbert space H. The system then evolves over time in such a way that two spatially distinct parts, a and b, are sent to two distinct observers, Alice and Bob, who are free to perform quantum mechanical measurements on their respective portions of the total system (viz, a and b). The question is whether Alice can perform any action on a that would be detectable by Bob observing b. The theorem responds, 'no'.

3 New Quantum Bit Commitment

3.1 Non-entangled States Based QBC

The basic idea of the proposed QBC is as follows: Bob generates a sequence of qubits A and divides them into a series of blocks B, where each qubit is randomly selected from $\{|0\rangle_0, |1\rangle_1, |+\rangle_0, |-\rangle_1\}$, and sends the qubit sequence A to Alice. For each qubit in A, Alice randomly (with equal probability) chooses the standard basis $\{|0\rangle, |1\rangle\}$ or Hadamard basis $\{|+\rangle, |-\rangle\}$ to perform the measurement, and records the measurement result. According to measurement results, Alice obtains two disjoint subsets B_0 and B_1 of the set B. Alice then has two choices (representing the commitments $x = 0$ and $x = 1$, respectively). For $x = 0$, Alice randomly chooses certain blocks from B_0. For $x = 1$, Alice randomly chooses certain blocks from B_1. Alice sends the indexes of the selected blocks to Bob to finish the commitment. Thus, the key to the design is that the sent indexes are able to lock Alice's choice (i.e., commitment), while Bob is unable to distinguish Alice's choice based on the received indexes. Fig. 1 illustrates the framework of the proposed non-entangled states-based quantum bit commitment protocol. In more detail, we describe the protocol as follows.

Commit Phase

Step 1. Let m be an odd number, and n is an integer divisible by m, and denoted as $n = ml$ (e.g., $m = 51$, $n = 5100$ and $l = 100$). Bob generates a qubit sequence $A = (a_1, a_2, \ldots, a_n)$, where each a_i is randomly (with equal probability) chosen from $\{|0\rangle_0, |1\rangle_1, |+\rangle_0, |-\rangle_1\}$. Set $B = \{b_1, b_2, \ldots, b_l\}$, such

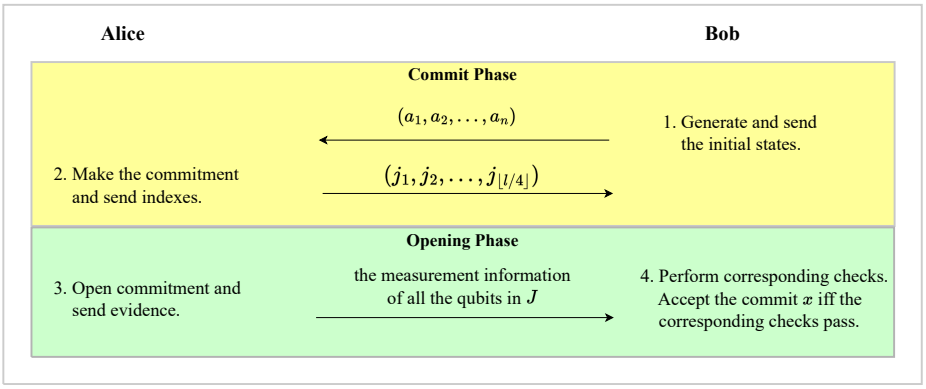

Fig. 1. Framework of The Non-entangled States Based QBC

that $b_i = (a_{m(i-1)+1}, a_{m(i-1)+2}, \ldots, a_{mi})$ with $1 \leq i \leq l$. That is, B divides the qubits in A into l blocks in order. Bob sends A to Alice.

Step 2. For each qubit a_i in A, Alice randomly (with equal probability) chooses the standard basis $\{|0\rangle, |1\rangle\}$ or Hadamard basis $\{|+\rangle, |-\rangle\}$ to perform the measurement (i.e., each qubit corresponds to a different randomly selected basis), and records the measurement basis and measurement result. Denote by p_i the number of 0's measured in block b_i (i.e., the total number of qubits in b_i measured as $|0\rangle_0$ or $|+\rangle_0$) and q_i the number of 1's measured in block b_i (i.e., the total number of qubits in b_i measured as $|1\rangle_1$ or $|-\rangle_1$). Hence, Alice obtains two disjoint subsets B_0 and B_1 of the set B as follows: $B_0 = \{b_i \mid b_i \in B, \text{ and } \frac{|p_i - q_i - 1|}{2} \bmod 2 = 0\} = \{b_i \mid b_i \in B, \text{ and } p_i \bmod 2 = 0\}$, and $B_1 = \{b_i \mid b_i \in B, \text{ and } \frac{|p_i - q_i - 1|}{2} \bmod 2 = 1\} = \{b_i \mid b_i \in B, \text{ and } p_i \bmod 2 = 1\}$. If $|B_0|$ or $|B_1|$ is less than $\lfloor l/4 \rfloor$, Alice aborts the current step and asks Bob to restart the protocol from Step 1. Then, Alice has two choices (representing the commitments $x = 0$ and $x = 1$, respectively). For $x = 0$, Alice randomly (with equal probability) chooses $\lfloor l/4 \rfloor$ blocks from B_0. For $x = 1$, Alice randomly (with equal probability) chooses $\lfloor l/4 \rfloor$ blocks from B_1. Denote the set of selected blocks as $J = \{b_{j_1}, b_{j_2}, \ldots, b_{j_{\lfloor l/4 \rfloor}}\}$ with $j_i \in \{1, 2, \ldots, l\}$. Alice sends the indexes $(j_1, j_2, \ldots, j_{\lfloor l/4 \rfloor})$ to Bob.

This is the end of the commit phase. In fact, the requirement that m be odd is just for analysis simplicity and is not necessary. For the case that m is an even number, we can set $B_0 = \{b_i \mid b_i \in B, \text{ and } \frac{|p_i - q_i|}{2} \bmod 2 = 0\} = \{b_i \mid b_i \in B, \text{ and } p_i \bmod 2 = 0\}$, and $B_1 = \{b_i \mid b_i \in B, \text{ and } \frac{|p_i - q_i|}{2} \bmod 2 = 1\} = \{b_i \mid b_i \in B, \text{ and } p_i \bmod 2 = 1\}$. Notice that if Bob is honest, then Alice has no way to know the exact state of each qubit in the received sequence A. For any qubit a_i, if Alice chooses a measurement basis different from Bob's encoding basis, then the measurement result of a_i has a probability of $1/2$ to be 0 and a probability of $1/2$ to be 1. Therefore, the block to which a_i belongs has a probability of $1/2$ to belong to B_0 and a probability of $1/2$ to belong to B_1. If

the probability that each block belongs to B_0 and the probability that it belongs to B_1 are both 1/2, then Bob cannot distinguish Alice's commitment based on the indexes $(j_1, j_2, \ldots, j_{\lfloor l/4 \rfloor})$.

Opening Phase

Step 3. Alice announces the measurement information for all qubits in J as evidence. That is, for each qubit a_i in J, Alice announces what basis was used to measure it, and the corresponding measurement result. Bob checks that the measurement information provided by Alice matches his own records. That is those qubits measured using the same bases as Bob's encoding bases should have the same measurement results. If any check fails, Bob detects that Alice is cheating and terminates the protocol. Otherwise, for each block $b_{j_i} \in J$, Bob gets p_{j_i} and q_{j_i}.

If Alice is committed to $x = 0$, Bob checks whether every block $b_{j_i} \in J$ belongs to B_0, i.e., for every block $b_{j_i} \in J$, Bob checks whether the equation $\frac{|p_{j_i} - q_{j_i} - 1|}{2} \bmod 2 = 0$ (or $p_{j_i} \bmod 2 = 0$ for simplicity) holds. Bob accepts the commitment $x = 0$ if and only if all checks pass.

If Alice is committed to $x = 1$, Bob checks whether every block $b_{j_i} \in J$ belongs to B_1, i.e., for every block $b_{j_i} \in J$, Bob checks whether the equation $\frac{|p_{j_i} - q_{j_i} - 1|}{2} \bmod 2 = 1$ (or $p_{j_i} \bmod 2 = 1$) holds. Bob accepts the commitment $x = 1$ if and only if all checks pass.

This is the end of the opening phase. It is clear that Alice's probability of successful cheating decreases exponentially as the number of blocks increases if she wants to switch between commitment $x = 0$ and commitment $x = 1$.

3.2 Security Analysis

Hiding: In this section, we will show that if Alice behaves as described in the QBC scheme, Bob cannot figure out x through the indexes $(j_1, j_2, \ldots, j_{\lfloor l/4 \rfloor})$. Furthermore, if dishonest Bob employs an entanglement attack and sends Alice the entangled states, he will get nothing according to the no-communication theorem. Details of the entanglement attack will be covered in the entanglement scheme.

For each received qubit, Alice randomly (with equal probability) chooses either the standard basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{|+\rangle, |-\rangle\}$ to perform the measurement. It will inevitably happen that certain qubits encoded with the standard basis are measured with the Hadamard basis, and vice versa. Then, according to the superposition principle, each such measurement leads to a collapse of the quantum state, resulting in 0 with probability 1/2 and 1 with probability 1/2, which neither Alice nor Bob could predict. Moreover, it is these random results that determine whether the block belongs to B_0 or B_1. For the ith block b_i, without loss of generality, suppose that after measurement (the measurement basis of each qubit of this block is the same as the encoding basis with the probability of $(1/2)^m$) Alice obtains $b_i \in B_0$, let $p_i = u$, $q_i = v$, then $\frac{|p_i - q_i - 1|}{2} \bmod 2 = \frac{|u - v - 1|}{2} \bmod 2 = 0$, where $u + v = m$.

If the encoding basis of a particular qubit in block b_i does not match the measurement basis, and the measurement is performed with a 1/2 probability of collapsing to another orthogonal state (e.g., from 0 to 1), the parameters of this block change to $p_i = u-1, q_i = v+1$, which gives $\frac{|(u-1)-(v+1)-1|}{2} \mod 2 = 1$, and Alice finally gets $b_i \in B_1$. It means that any change in measurement (choosing a different basis and collapsing to a different state) may cause the measurement result of a_i to change from 0 to 1 (or from 1 to 0), which is sufficient to change the collection to which the block belongs, changing it from B_0 to B_1 (or from B_1 to B_0). Therefore, the probability that this block belongs to B_0 is $Pr(b_i \in B_0) = 1/2 + (1/2)^{m+1}$; the probability that it belongs to B_1 is $Pr(b_i \in B_1) = 1/2 - (1/2)^{m+1}$. Moreover, $\epsilon = (1/2)^{m+1}$ can be made arbitrarily (or exponentially) small by increasing the input size m of the protocol. Therefore, it is impossible to distinguish Alice's commitment from the indexes $(j_1, j_2, \ldots, j_{\lfloor l/4 \rfloor})$ sent by Alice alone.

In summary, based on the superposition principle, a dishonest Bob has no strategy to determine whether any block will belong to B_0 or B_1, therefore the protocol satisfies the hiding requirement.

Binding: In this section, we will show that once Alice has made her commitment, i.e., announced the indexes $(j_1, j_2, \ldots, j_{\lfloor l/4 \rfloor})$, she will not be able to successfully cheat Bob later.

Based on the superposition principle, Alice has no strategy to determine whether any block will belong to B_0 or B_1 before she has measured the qubits. In other words, whether a particular block b_i belongs to B_0 or B_1 is unpredictable (because Alice is unaware of the qubit's initial state, and Bob is unaware of Alice's measurement basis). Furthermore, each block b_i belongs to either B_0 or B_1, and $Pr(b_i \in B_0) = Pr(b_i \in B_1) = 1/2$. If in the commit phase, Alice randomly selects $\lfloor l/4 \rfloor$ blocks (without measurement) as evidence of commitment, then in the opening phase, the probability of success $\frac{7}{8}^{\lfloor l/4 \rfloor}$ decreases exponentially as l increases, regardless of whether Alice claims to be committed to 0 or 1. Similarly, if Alice chooses to measure some of the qubits and some of the qubits remain entangled for the chosen blocks, then, this strategy makes Alice's probability of successfully switching commitment values in the opening phase decrease exponentially as l increases, and the probability of being detected as cheating is non-negligible. Hence, Alice should measure the qubits before making a commitment.

Suppose Alice performs the measurement honestly. For the case of $x = 0$, Alice selects $\lfloor l/4 \rfloor$ blocks from B_0 at random and sends the indexes. In the opening phase, dishonest Alice seeks to convince Bob that $x = 1$, and she can only cheat by misrepresenting a particular measurement (e.g., from 0 to 1, or from 1 to 0) because it is unpredictable whether a given qubit a_i belongs to 0 or 1 with the incompatible measurement basis. Alice has no idea which qubit of any block b_{j_i} selects the measurement basis that happens to be the same as Bob's encoding basis, and she can only cheat by randomly selecting one qubit a_l of this block. Assume that the measurement basis is $k' = 0$ and the measurement result is $r' = 0$, and she will announce that $k'_c = 1 \neq k'$, $r'_c = 1 \neq r'$, because this

has a higher probability of successful cheating (compared to $k'_c = 0$, $r'_c = 1$). As previously stated, this block will belong to B_1, with the number of forged $p'_{j_i} = u - 1$, $q'_{j_i} = v + 1$. The probability that Bob will accept this block (i.e., that the qubit a_l will be accepted) is $Pr(k \neq k'_c) + Pr(k = k'_c) \times Pr(r = 1 | k = k'_c) = 3/4$, where k, r are Bob's records on qubit a_l. In conclusion, for each block $b_{j_i} \in B_x$, the probability that Alice will convince Bob that $b_{j_i} \in B_{1-x}$ is $3/4$. Therefore, for all blocks in J, the probability of successfully cheating is $\frac{3}{4}^{\lfloor l/4 \rfloor}$. Similarly, if Alice commits to $x = 1$, the probability of successfully convincing Bob that $x = 0$ is $\frac{3}{4}^{\lfloor l/4 \rfloor}$. The probability of Alice's successful cheating is bounded by $\epsilon = \frac{3}{4}^{\lfloor l/4 \rfloor}$, where ϵ can be made arbitrarily (or exponentially) small by increasing l.

In short, the probability of Alice's cheating success decreases exponentially as l increases. Therefore, the protocol satisfies the binding requirement.

3.3 Generality of The Impossibility Proof

The well-known proof of the impossibility of unconditionally secure QBC was supposed to be general. However, in this section, we will show that it is not general. In fact, in the generality proof of the impossibility of secure quantum bit commitment [20], the authors use a simplified version of Yao's model [33]. It is this simplified version that makes the proof not general.

The authors propose the following attack for the simplified version on page 181 of [20]: "Consider more closely the situation at the end of step (b), the commit phase. Let $|0\rangle_{\text{com}}$ and $|1\rangle_{\text{com}}$ denote the state of $H = H_A \otimes H_B \otimes H_C$ at that time corresponding to the two possible values of b, respectively. In order that Alice and Bob can follow the procedures, they must know the exact forms of all the unitary transformations involved. Therefore, Alice must be capable of computing the two states $|0\rangle_{\text{com}}$ and $|1\rangle_{\text{com}}$." That is, Alice can obtain $|0\rangle_{\text{com}}$ and $|1\rangle_{\text{com}}$ (two states corresponding to the two possible values of b) just by certain unitary transformations without any measurement, so all measurements can be delayed to the opening phase and Alice can always switch her commitment in the opening phase. However, this attack relies on the assumption that all measurements can be postponed to the opening phase.

Regarding the reason for simplification, there is an explanation on pages 179-180 as follows: "Second, in Yao's model, the user D does two things in each round of the communication: D carries out a measurement on the current mixed state of the portion of the space, $H_D \otimes H_C$, in his/her control and then performs a unitary transformation on $H_D \otimes H_C$. In our model, the measurement step has been eliminated." Moreover, regarding the reason why the measurement step can be eliminated, the authors explain that: "Essentially, we give Alice and Bob quantum computers and quantum storage devices. Therefore, they can execute a quantum bit commitment scheme by unitary transformations." This does not make sense. In fact, based on the quantum superposition principle, the measurement is uncertain and irreversible, while the unitary transformation is reversible.

There is an implicit requirement for using the simplified version of Yao's model, i.e., if Alice can get evidence of commitment without the measurement (i.e., can delay the measurement), then the simplified version will perfectly match such a case. However, there are possible schemes (e.g., the proposed scheme) where Alice cannot get valid evidence of commitment without the measurement (That is, not in all cases, Alice can delay the measurement), otherwise, allowing Bob to detect Alice cheating with a probability close to 1 in the opening phase. The inability to delay the measurement makes it impossible for Alice to switch the commitment in the opening phase.

For our proposed scheme, Alice needs to announce the indexes of $\lfloor l/4 \rfloor$ blocks in the commit phase. If Alice does not measure any qubit in the commit phase, there is no way for Alice to get $\lfloor l/4 \rfloor$ blocks to pass Bob's check in the opening phase. If Alice chooses $x = 0$ in the commit phase, because the probability that each block belongs to B_0 and B_1 is $1/2$ for Alice, then there is no way for Alice to get all $\lfloor l/4 \rfloor$ blocks to pass Bob's check with $x = 1$ (the same is true for choosing $x = 1$ at commitment and claiming $x = 0$ at the opening phase), unless Alice can know the exact status of every qubit she received, which clearly contradicts the no-cloning theorem. Because Bob sends Alice some BB84 states and Bob does not keep any quantum state, no matter non-entangled or entangled. Therefore, Alice's attempted entanglement attack strategy is invalid in this case.

3.4 Entangled States Based QBC

In the above non-entangled states based QBC scheme, each qubit in the sequence A generated by Bob is randomly chosen from $\{|0\rangle_0, |1\rangle_1, |+\rangle_0, |-\rangle_1\}$. If we replace these random quantum states with entangled states (e.g., Bell states), then we will obtain a similar QBC scheme. The key to the design is that Alice needs to provide the appropriate information (i.e., the indexes) to corroborate that she has made the commitment and that she cannot change it, while the scheme ensures that Bob cannot obtain any information about x from the indexes. The framework of the proposed entangled states based quantum bit commitment protocol is shown in Fig. 2. The detailed steps are as follows.

Commit Phase

Step 1. Let m be an odd number, and n is an integer divisible by m, and denoted as $n = ml$ (e.g., $m = 51$, $n = 5100$ and $l = 100$). Assume Alice and Bob share n Bell states, denoted as $(a_i, b_i) \triangleq \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ with $1 \leq i \leq n$, where a_i denotes one qubit of the ith Bell state and b_i denotes the other one. Let $A \triangleq (a_1, a_2, ..., a_n)$ and $B \triangleq (b_1, b_2, ..., b_n)$. Alice keeps the qubit sequence A and Bob keeps B. Set $C = \{c_1, c_2, \ldots, c_l\}$ and $D = \{d_1, d_2, \ldots, d_l\}$, such that $c_i = (a_{m(i-1)+1}, a_{m(i-1)+2}, \ldots, a_{mi})$ and $d_i = (b_{m(i-1)+1}, b_{m(i-1)+2}, \ldots, b_{mi})$ with $1 \leq i \leq l$. That is, C divides the qubits in A into l blocks in order, and D divides the qubits in B into l blocks in order. Bob sends A to Alice.

Step 2. For each qubit a_i in A, Alice randomly chooses the standard basis $\{|0\rangle, |1\rangle\}$ or Hadamard basis $\{|+\rangle, |-\rangle\}$ to perform the measurement (i.e., each qubit corresponds to a different randomly selected basis), and records

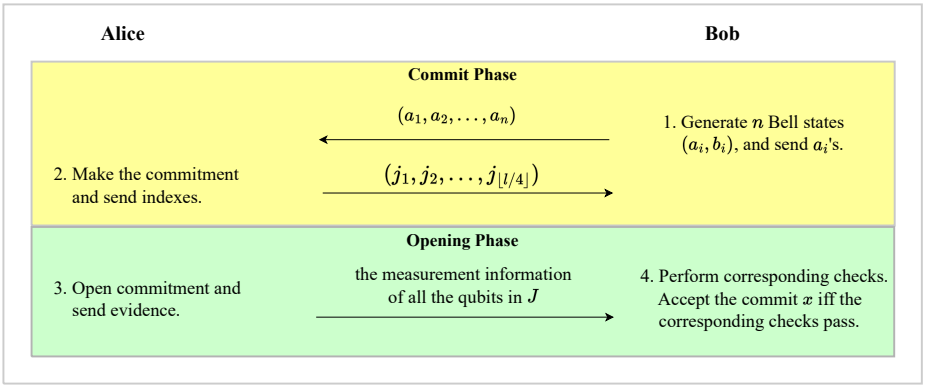

Fig. 2. Framework of The Entangled States Based QBC

the measurement basis and measurement result (i.e., if the measurement result of a_i is $|0\rangle$ or $|+\rangle$, it is recorded as 0; if the measurement result of a_i is $|1\rangle$ or $|-\rangle$, it is recorded as 1). Denote by p_i the total number of 0's measured in block c_i, and q_i the total number of 1's measured in block c_i. Hence, Alice obtains two disjoint subsets C_0 and C_1 of the set C as follows: $C_0 = \{c_i \mid c_i \in C, \text{ and } \frac{|p_i - q_i - 1|}{2} \bmod 2 = 0\} = \{c_i \mid c_i \in C, \text{ and } p_i \bmod 2 = 0\}$, and $C_1 = \{c_i \mid c_i \in C, \text{ and } \frac{|p_i - q_i - 1|}{2} \bmod 2 = 1\} = \{c_i \mid c_i \in C, \text{ and } p_i \bmod 2 = 1\}$. Then, Alice has two choices (representing the commitment $x = 0$ and $x = 1$, respectively). For $x = 0$, Alice randomly chooses $\lfloor l/4 \rfloor$ blocks from C_0. For $x = 1$, Alice randomly chooses $\lfloor l/4 \rfloor$ blocks from C_1. Denote the set of selected blocks as $J = \{c_{j_1}, c_{j_2}, \ldots, c_{j_{\lfloor l/4 \rfloor}}\}$ with $j_i \in \{1, 2, \ldots, l\}$. Alice sends the indexes $(j_1, j_2, \ldots, j_{\lfloor l/4 \rfloor})$.

This is the end of the commit phase. Likewise, the requirement that m be odd is just for analysis simplicity and is not necessary. For the case that m is an even number, we can set $C_0 = \{c_i \mid c_i \in C, \text{ and } \frac{|p_i - q_i|}{2} \bmod 2 = 0\} = \{c_i \mid c_i \in C, \text{ and } p_i \bmod 2 = 0\}$, and $C_1 = \{c_i \mid c_i \in C, \text{ and } \frac{|p_i - q_i|}{2} \bmod 2 = 1\} = \{c_i \mid c_i \in C, \text{ and } p_i \bmod 2 = 1\}$. According to the no-communication theorem, Bob does not get any information from Alice's measurement behavior.

Opening Phase

Step 3. Alice announces the measurement information for all qubits in J as evidence. That is, for each qubit a_i in J, Alice announces what basis was used to measure it, and the corresponding measurement result. Bob measures each qubit b_i in $\{d_{j_1}, d_{j_2}, \ldots, d_{j_{\lfloor l/4 \rfloor}}\}$ with the corresponding basis provided by Alice, such that a_i and b_i were measured using the same basis. Bob checks that the measurement results match the information provided by Alice, i.e., the two qubits in each pair (a_i, b_i) measured with the same basis should have the same result. If any check fails, Bob detects that Alice is cheating and terminates the game. Otherwise, for each block $c_{j_i} \in J$, Bob gets p_{j_i} and q_{j_i}.

If Alice's commitment is $x = 0$, Bob checks whether every block $c_{j_i} \in J$ belongs to C_0, i.e., for every block $c_{j_i} \in J$, Bob checks whether the equation $\frac{|p_{j_i} - q_{j_i} - 1|}{2} \bmod 2 = 0$ (or $p_{j_i} \bmod 2 = 0$) holds. Bob accepts the commitment $x = 0$ if and only if all checks pass.

If Alice's commitment is $x = 1$, Bob checks whether every block $c_{j_i} \in J$ belongs to C_1, i.e., for every block $c_{j_i} \in J$, Bob checks whether the equation $\frac{|p_{j_i} - q_{j_i} - 1|}{2} \bmod 2 = 1$ (or $p_{j_i} \bmod 2 = 1$) holds. Bob accepts the commitment $x = 1$ if and only if all checks pass.

This is the end of the opening phase. In fact, similar to [29], we can require Alice and Bob to share n Bell states in advance, rather than Bob sending Alice n qubits. In such a case, the protocol starts from Step 2, and we can easily analyze that any attempted entanglement attack by Alice or Bob becomes impossible. The security proof of this protocol actually gives a new version of the proof of BQP $\neq$ QMA. However, to make the protocol more practical, our analysis below does not require Alice and Bob to share n Bell states beforehand. It is clear that, according to the quantum entanglement property, the probability that Alice wants to switch her commitment without being detected decreases exponentially as n/m increases.

3.5 Security Analysis

Hiding: In this section, we will show that if Alice behaves as described in the QBC scheme, Bob cannot figure out x through the qubit sequence B and the indexes $(j_1, j_2, \ldots, j_{\lfloor l/4 \rfloor})$.

On the one hand, according to the no-communication theorem, Bob learns nothing about Alice's operations (measurements). Therefore, Bob gets no information about x based on the qubit sequence B alone.

On the other hand, for each qubit a_i, Alice randomly (with equal probability) chooses either the standard basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{|+\rangle, |-\rangle\}$ to perform the measurement. Then, based on the superposition principle (i.e., $(a_i, b_i) = \frac{|00\rangle + |11\rangle}{\sqrt{2}} = \frac{|{+}{+}\rangle + |{-}{-}\rangle}{\sqrt{2}}$), each such measurement leads to a collapse of the quantum state, resulting in 0 with probability 1/2 and 1 with probability 1/2, which neither Alice nor Bob could predict.

Furthermore, considering any qubit a_k in the ith block $c_i = (a_{m(i-1)+1}, a_{m(i-1)+2}, \ldots, a_{mi})$, Alice's measurement of a_k has a 1/2 probability of getting 0 and a 1/2 probability of getting 1. Assuming that other qubits in c_i have been measured except a_k, then switching the measurement result of a_k from 0 to 1, or from 1 to 0, both would lead to c_i switching between C_0 and C_1. Any qubit a_k in a Bell state is measured with a 1/2 probability of collapsing to another orthogonal state (switching between 0 and 1), which in turn switches c_i between C_0 and C_1. The probability that c_i belongs to C_0 or C_1 is $Pr(c_i \in C_0) = Pr(c_i \in C_1) = 1/2$. Therefore, Bob can't distinguish the commitment based on the indexes $(j_1, j_2, \ldots, j_{\lfloor l/4 \rfloor})$ alone.

Furthermore, based on the Bell state entanglement property, after Alice performs the measurement, Bob has exactly the same set of qubit blocks as

$J = \{c_{j_1}, c_{j_2}, \ldots, c_{j_{\lfloor l/4 \rfloor}}\}$, noted as $J' = \{d_{j_1}, d_{j_2}, \ldots, d_{j_{\lfloor l/4 \rfloor}}\}$, where d_{j_i} has exactly the same quantum states as c_{j_i}. There are two strategies for a dishonest Bob to develop his analysis. First, he randomly selects the standard basis or the Hadamard basis to measure each qubit in block $d_{j_i} \in J'$ and records the number of blocks belonging to set $D_0 = \{d_i \mid d_i \in D, \text{ and } \frac{|p_i - q_i - 1|}{2} \bmod 2 = 0\}$ and $D_1 = \{d_i \mid d_i \in D, \text{ and } \frac{|p_i - q_i - 1|}{2} \bmod 2 = 1\}$, respectively. Suppose the set $D_{x'}$ contains more blocks, then Bob is biased to believe that Alice is committed to x'. For each block d_{j_i}, it belongs to set D_x with probability 1 only if Bob has chosen the complete consistent measurement bases with Alice; otherwise, it belongs to both sets with probability 1/2. Therefore, the probability that each block d_{j_i} belongs to D_x is $Pr(d_{j_i} \in D_x) = 1/2 + 1/2^{(m+1)}$; and the probability that it belongs to another set is $Pr(d_{j_i} \in D_{1-x}) = 1/2 - 1/2^{(m+1)}$. Moreover, $\epsilon = 1/2^{(m+1)}$ can be made arbitrarily small by increasing the input size m of the game. On the other hand, Bob may choose one basis to measure all qubits in J', e.g., choose the standard basis (or Hadamard basis) to measure. In such case, the probability that each block d_{j_i} belongs to D_x is also $Pr(d_{j_i} \in D_x) = 1/2 + 1/2^{(m+1)}$, because Alice chooses the measurement bases randomly, and each block also has a $1/2^{(m+1)}$ probability of consistent with the combination of bases chosen by Bob.

Secondly, considering a dishonest Bob measuring all the qubits in J' with the Breidbart basis, which is the best option for an attacker to obtain the key in BB84 [17]. For the ith block c_{j_i}, we denote the m results from Alice as bit-string $r = r_1 r_2 ... r_m$. And the m results of d_{j_i} from Bob as bit-string $r' = r'_1 r'_2 ... r'_m$. It is possible to conclude that the block d_{j_i} belongs to the same set D_x if two bit-strings have an even number of bits that take different values in them, where $Pr(r'_i = r_i) = \cos^2(\pi/8) = p_b$, $Pr(r'_i \neq r_i) = 1 - p_b = q_b$. Therefore, the probability that each block d_{j_i} belongs to D_x is $Pr(d_{j_i} \in D_x) = \frac{1}{2} + \epsilon$, where

$$\epsilon = \frac{1}{2}\Big(\sum_{k=0}^{(m-1)/2} \mathrm{C}_m^{2k} p_b^{2k} q_b^{m-2k} - \sum_{k=0}^{(m-1)/2} \mathrm{C}_m^{2k+1} p_b^{2k+1} q_b^{m-2k-1}\Big).$$

The above probability formula represents the difference between the even number and the odd number of k in the Bernoulli trials. Clearly, ϵ can be made arbitrarily small by increasing m.

As the density matrices of the two commitments are not identical, there exists a POVM measure that allows Bob to distinguish them with a non-zero probability ϵ and consequently learn the value x chosen by Alice. The probability that Bob never distinguishes x is $(1-\epsilon)^{\lfloor l/4 \rfloor}$. As mentioned above, ϵ can be made arbitrarily small by increasing m, which means that although the density matrices of the two quantum states of the two commitments are not identical, they can be approximated rapidly as m increases. Therefore, the probability of Bob successfully distinguishing between the two commitments is $1-(1-\epsilon)^{\lfloor l/4 \rfloor}$. In this equation, as long as the number of blocks l is fixed, then as m increases, ϵ converges to 0 and the probability of successful distinction will eventually converge to 0 infinitely. Fortunately, in our proposed game, l can be fixed, since

the number of blocks that can prevent Alice from successfully cheating does not need to be infinite.

In summary, based on the principle of superposition, the probability that a dishonest Bob can derive the value of x through the qubit sequence B and the indexes can be arbitrarily small as m increases. Therefore, the protocol satisfies the hiding requirement.

Binding: In this section, we will show that once Alice has made her commitment, i.e., announced the indexes $(j_1, j_2, \ldots, j_{\lfloor l/4 \rfloor})$, she will not be able to successfully cheat Bob later.

To begin with, we analyze the feasibility of entanglement attacks. For any block c_i, if Alice measures $\frac{|p_i - q_i - 1|}{2} \bmod 2 = 0$, the qubits in Bob's block d_i must also collapse to a state corresponding to $\frac{|p_i - q_i - 1|}{2} \bmod 2 = 0$, provided Bob applies the same measurement bases to these qubits as Alice. Although Bob does not know Alice's measurement bases, he can exhaust the states satisfying $\frac{|p_i - q_i - 1|}{2} \bmod 2 = 0$ under all possible combinations of measurement bases and get the density matrix corresponding to these states with equal probability of occurrence, denoted as ρ_0. Similarly, he can also get the density matrix ρ_1 corresponding to $\frac{|p_i - q_i - 1|}{2} \bmod 2 = 1$.

As the density matrices of the two commitments are not identical, there exists a POVM measure that allows Bob to distinguish them with a non-negligible probability and consequently learn the value x chosen by Alice. Therefore, if Alice is able to perform some local unitary operations to switch between ρ_0 and ρ_1 as she wishes, then Bob can succeed in distinguishing x. That is, if Alice can switch between ρ_0 and ρ_1 by local unitary operations then Bob can know whether Alice wants to send him a 0 or a 1 by POVM measurements without further information exchange, which is a clear violation of the no FTL principle. So it can be concluded that Alice can not perform some local unitary operations to switch between ρ_0 and ρ_1 as she wishes.

In the next section, we analyze the feasibility of non-entanglement attacks. Based on the superposition principle, Alice has no strategy to determine whether any block c_i belongs to C_0 or C_1 before measuring all its qubits. In other words, whether a particular block c_i belongs to C_0 or C_1 is unpredictable (since measuring a qubit of a Bell state will randomly get 0 with 1/2 probability and 1 with 1/2 probability). Moreover, each block c_i belonging to C_0 or C_1 is independent and $Pr(c_i \in C_0) = Pr(c_i \in C_1) = 1/2$. If in the commit phase, Alice chooses to keep the entangled states without measuring qubits, i.e., randomly selects $\lfloor l/4 \rfloor$ blocks as evidence of commitment, then in the opening phase, the probability of success $\frac{3}{4}^{\lfloor l/4 \rfloor}$ decreases exponentially as l increases, regardless of whether Alice claims to be committed to 0 or 1. Similarly, if Alice chooses to measure some of the qubits and some of the qubits remain entangled for the chosen blocks, then, this strategy makes Alice's probability of successfully switching commitment values in the opening phase decrease exponentially as l increases, and the probability of being detected as cheating is non-negligible. Hence, Alice should measure the qubits before making a commitment.

For the case of $x = 0$, Alice selects $\lfloor l/4 \rfloor$ blocks from C_0 at random (with equal probability) and sends the indexes. In the opening phase, dishonest Alice seeks to convince Bob that $x = 1$, and she can cheat by misrepresenting a particular measurement (e.g., from 0 to 1, or from 1 to 0) because for a given qubit a_i, it is unpredictable whether 0 or 1 will be obtained with the incompatible measurement basis. For any block c_{j_i}, Alice will choose a qubit (e.g., a_l) of this block at random to cheat. Without loss of generality, suppose that the measurement basis of a_l is $k = 0$, and the measurement result is $r = 0$, and then she will announce that $k_c = 1 \neq k, r_c = 1 \neq r$. Then the probability that this block is accepted by Bob (i.e., the probability that the qubit b_l will be accepted) is 1/2 (e.g., $Pr(r' = 1|k' = k_c \neq k) = 1/2$), where k', r' are Bob's records on qubit b_l. In conclusion, for each block $c_{j_i} \in C_x$, the probability that Alice will convince Bob that $c_{j_i} \in C_{1-x}$ is 1/2. Therefore, for all blocks in J, the probability of successfully cheating is $\frac{1}{2}^{\lfloor l/4 \rfloor}$. Similarly, if Alice commits to $x = 1$, the probability of successfully convincing Bob that $x = 0$ is $\frac{1}{2}^{\lfloor l/4 \rfloor}$. The probability of Alice's successful cheating is bounded by $\epsilon = \frac{1}{2}^{\lfloor l/4 \rfloor}$, where ϵ can be made arbitrarily (or exponentially) small by increasing l.

Furthermore, considering the following cheating strategy: Alice chooses u C_0 blocks and v C_1 blocks in the commit phase, where $u + v = \lfloor l/4 \rfloor$. Then the probability that Alice will successfully claim commitment $x = 0$ is $1/2^v$, and the probability that she will successfully claim commitment $x = 1$ is $1/2^u$ in the opening phase. Therefore, Alice should take $u = v = \lfloor l/8 \rfloor$ if she wishes to maximize the possibility of switching commitments between 0 and 1 at will in the opening phase. The probability of success is $1/2^{\lfloor l/8 \rfloor}$ for both. The probability of success decreases exponentially as l increases, regardless of whether Alice claims to be committed to 0 or 1.

In short, the probability of Alice's cheating success decreases exponentially as l increases. Therefore, the protocol satisfies the binding requirement.

4 Improved Quantum oblivious Transfer

4.1 QOT Based on QBC

The basic idea of Yao's QOT model [33] is as follows: Alice generates n qubits, randomly chosen from the set $\{|0\rangle_0, |1\rangle_1, |+\rangle_0, |-\rangle_1\}$, and sends them to Bob. Bob randomly performs measurements using either the standard basis $\{|0\rangle, |1\rangle\}$ or the Hadamard base $\{|+\rangle, |-\rangle\}$, records the measurement results, and commits to the results. After Bob completes the measurement, Alice randomly selects R qubits for inspection. Bob publicly discloses the corresponding information to allow Alice to verify that he has honestly measured all the qubits. Once the inspection is passed, Alice also reveals the measurement information of the remaining qubits to Bob. Bob categorizes the index values of the qubits into two groups by comparing whether the measurement bases at the corresponding positions match Alice's measurements, and he sends these two categories of index

values to Alice in any order he chooses. Depending on Alice's selection, Bob has a 1/2 probability of obtaining the message.

By improving this QOT model, we can obtain an unconditionally secure quantum one-out-of-two oblivious transfer scheme using the proposed bit commitment protocol. Fig. 3 illustrates the framework of the proposed quantum oblivious transfer protocol. In more detail, we describe the protocol as follows (each step may cover several steps in the framework).

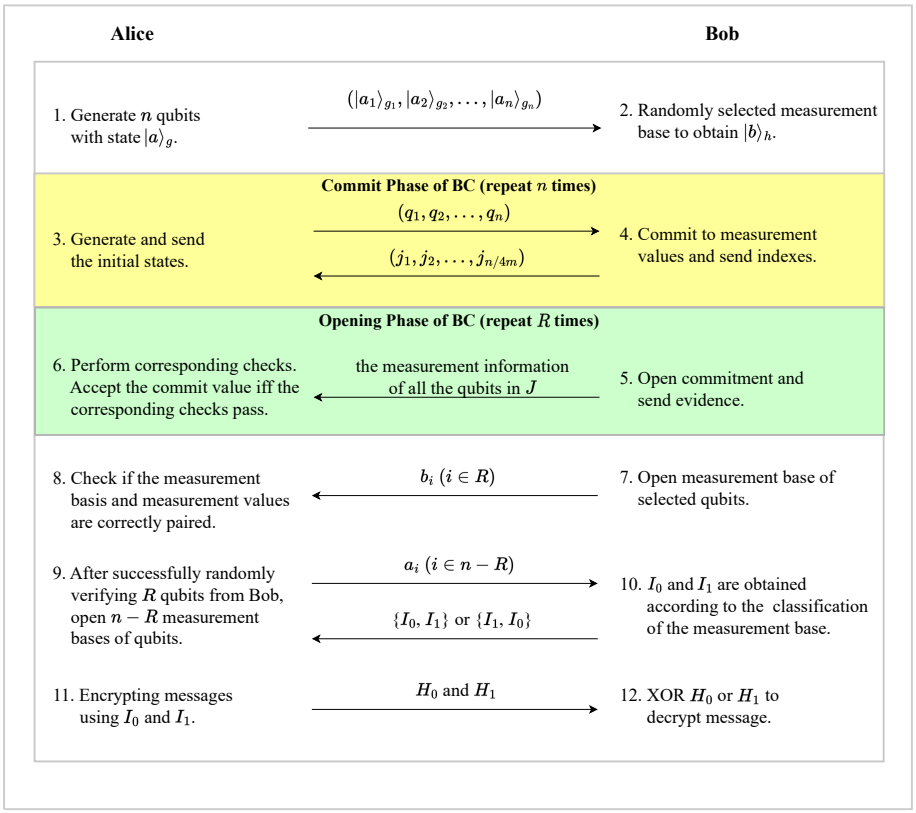

Fig. 3. Framework of The QOT based on QBC

Step 1. Alice begins by preparing n qubits with state $|a\rangle_g$. Where a represents the measurement basis (either the standard basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{|+\rangle, |-\rangle\}$) and g represents the measurement value (0 or 1), there are four possible states i.e., $\{|0\rangle_0, |1\rangle_1, |+\rangle_0, |-\rangle_1\}$. Each qubit owned by Alice is denoted as $|a_i\rangle_{g_i}$, where i ranges from 1 to n. Alice owns the set of measurement bases a and the set of measurement values g. She then sends the n qubits to Bob, and honest Bob needs to perform measurements on these qubits without having access to information other than these n qubits.

Step 2. Bob randomly selects a measurement basis (either the standard basis $\{|0\rangle, |1\rangle\}$ or the Hadamard basis $\{|+\rangle, |-\rangle\}$) for each qubit. The set of randomly chosen measurement bases is denoted as b. Corresponding to each measurement basis, Bob obtains a set of measurement values, denoted as h. Therefore, Bob can represent the states of the n qubits as $|b\rangle_h$, where $|b_i\rangle_{h_i}$ denotes the state of the ith qubits owned by Bob (for $i = 1, ..., n$). After all measurements are completed, Bob needs to commit to each value in his set of measurements h using the previously described non-entangled states based quantum bit commitment scheme. Bob then sends the evidence of his committed values to Alice.

Step 3. Alice randomly selects a subset of R qubits from $|b\rangle_h$ for inspection. Bob provides the proof of the bit commitment for the measured values corresponding to the selected qubits to Alice. Once Alice approves all the commitment results, the next step of verification is carried out. Bob discloses to Alice the measurement bases he used for the selected qubits. Alice then selects the corresponding measurement bases a_i $(i \in R)$ and values g_i $(i \in R)$ in $|a\rangle_g$. If Alice finds that, under $a_i = b_i$ for all $(i \in R)$, it also holds that $g_i = h_i$ for all $(i \in R)$, then Alice considers that Bob has honestly measured all the qubits.

Step 4. After confirming that Bob has measured all n qubits honestly, Alice reveals her remaining set of measurement bases a_i $(i \in n - R)$ to Bob. Bob then separates the indexes of the remaining qubits into two sets: I_0 and I_1. In I_0, Bob includes the indexes of qubits that have the same measurement bases as Alice at the corresponding positions, while in I_1, Bob includes the indexes of qubits that have different measurement bases. Subject to the satisfaction that the sets I_0 and I_1 have the same number of elements, the sum of the numbers of elements of I_0 and I_1 should be made as close as possible to $n - R$.

Step 5. Bob randomly chooses the order of I_0 and I_1 to send to Alice, either as $\{I_0, I_1\}$ or $\{I_1, I_0\}$. If Bob sends $\{I_0, I_1\}$, Alice can get the set $K_0 = g_i$ $(i \in I_0)$, and the set $K_1 = g_i$ $(i \in I_1)$. Alice then applies a hash function to K_0 and K_1, resulting in the output values H_0 and H_1 respectively. Next, Alice uses H_0 to encrypt the message m_0, obtaining the ciphertext C_0 as $C_0 = H_0 \oplus m_0$; Similarly, she uses H_1 to encrypt the message m_1, obtaining the ciphertext C_1 as $C_1 = H_1 \oplus m_1$. Then, Alice sends C_0, C_1, and the hash function to Bob. Bob can compute m_0 by performing $m_0 = C_0 \oplus H(K_0)$, but since he does not have access to K_1, he cannot obtain m_1, and vice versa.

Description of the QBC section of the QOT. The specific steps to use the quantum bit commitment protocol in a quantum oblivious transfer protocol are as follows: Bob treats each of his measurement values h_i as a commitment, where each measurement value has an associated index value $(j_1, j_2, \ldots, j_{\lfloor l/4 \rfloor})$ as evidence. This allows us to obtain the set $E = (evidence_1, evidence_2, \ldots, evidence_n)$. Bob announces the set E to Alice, who then selects R elements from it, denoted as $(evidence_{i_1}, evidence_{i_2}, \ldots, evidence_{i_R})$, while keeping the commitment values secret. In the opening phase, Bob publicly reveals his commitment values and provides proof of his commitment values to Alice. Alice can then verify the va-

lidity of the commitments and determine whether Bob has honestly revealed his measurement results.

4.2 Security Analysis

The selection of commitment value: The choice of making a bit commitment for the measurements in Step 2 is to address the possibility of cheating by Bob. If Bob chooses to make a bit commitment for his own set of n measurement bases, let's say committing 0 for the standard basis and 1 for the Hadamard basis. Even if Alice verifies that Bob's commitments for the measurement bases are correct, she cannot trust Bob completely. This is because a dishonest Bob may simply claim that he has chosen those measurement bases and assign a random set of bases, making honest commitments according to the BC protocol without actually performing the measurements. Then, after Alice verifies Bob's committed bases, she proceeds to check each selected pair of measurement bases and their corresponding measurement results, ensuring that for every $a\lfloor i\rfloor = b\lfloor i\rfloor$, there exists $g\lfloor i\rfloor = h\lfloor i\rfloor$, for $(i \in R)$ exist. At this point, the dishonest Bob could selectively measure only the R qubits using the committed measurement bases, while leaving the remaining $n - R$ qubits unmeasured. This would enable Bob to pass Alice's checks and make her believe that he has indeed measured all n qubits. Later, when Alice announces the measurement bases for the remaining $n - R$ qubits, Bob can measure the remaining qubits using the announced bases and obtain the same measurement results as Alice, thereby gaining access to all of Alice's information.

Therefore, to prevent possible cheating by Bob, it is necessary to have Bob commit to the measurement values. Bob will make a bit commitment for each of his qubits' measurement results (the commitment value is bound to the measurement result but not revealed during the commitment phase; a commitment value of 0 represents a measurement result of 0, and a commitment value of 1 represents a measurement result of 1). Bob publicly reveals the evidence for the commitment values of each measurement result $(evidence_1, evidence_2, \ldots, evidence_R)$, but Alice cannot obtain any information about the commitment values from the evidence. After Alice randomly selects R qubits, she requires Bob to disclose the proof information $(proof_1, proof_2, \ldots, proof_R)$. If all the R commitment values are correct, Alice proceeds to the next verification step, where Bob publicly announces the R selected measurement bases. In the sets of R pairs $(b\lfloor i\rfloor, h\lfloor i\rfloor)$ for Bob and $(a\lfloor i\rfloor,\ g\lfloor i\rfloor)$ for Alice, if there exists $a\lfloor i\rfloor = b\lfloor i\rfloor$ and $g\lfloor i\rfloor \neq h\lfloor i\rfloor$, $(i \in R)$, it indicates that Bob did not measure honestly. However, if for every $a\lfloor i\rfloor = b\lfloor i\rfloor$, there exists $g\lfloor i\rfloor = h\lfloor i\rfloor$, $(i \in R)$, the verification is successful, and Alice can trust that Bob indeed measured all n qubits. Subsequently, Alice announces her remaining $n - R$ measurement bases to Bob to proceed with the oblivious transfer protocol. If the dishonest Bob randomly assigns a set of measurement results and makes commitments without actually measuring, Bob will not know the correct measurement bases. Therefore, when Alice checks the R pairs of measurement bases and results, Bob cannot ensure that his declared

measurement bases, which are the same as Alice's, have the same measurement results because the committed measurement results cannot be altered.

Improvements: In order to address another potential cheating method by Bob, an improvement is introduced in Step 5, and the proposed method and its purpose will now be described. After Alice believes that Bob has honestly measured all the qubits, Alice will disclose her remaining $n - R$ measurement bases to Bob. Bob compares Alice's announced measurement bases with his own and calculates the number of bases that are the same and different at the same index positions, denoted as s_0 and s_1, respectively. let $s = \min(s_0, s_1)$. This allows Bob to obtain two sets, I_0 and I_1, where $a\lfloor i \rfloor = b\lfloor i \rfloor$ for $i \in I_0 = (i_1, \ldots, i_s)$ and $a\lfloor j \rfloor \neq b\lfloor j \rfloor$ for $j \in I_1 = (j_1, \ldots, j_s)$. Indeed, it can be noted that once Alice discloses her measurement bases, the classification and division of the sets I_0 and I_1 are entirely determined by Bob himself. Therefore, Bob may not necessarily categorize them honestly. One possible cheating method is for Bob to evenly distribute sets I_0 and I_1 into subsets $\bar{I}_0$ and $\bar{I}_1$, respectively, such that $\bar{I}_0$ and $\bar{I}_1$ each contain half of I_0 and I_1. Bob then sends $\bar{I}_0$ and $\bar{I}_1$ to Alice. In this case, if the measurement results K_0 and K_1 are directly used to encrypt the information m_0 and m_1, for example, $C_0 = K_0 \oplus m_0$; $C_1 = K_1 \oplus m_1$, Bob can use $\bar{I}_0$ and $\bar{I}_1$ to obtain half of the correct results from the sets of measurement values K_0 and K_1. Bob can then partially decrypt C_0 and C_1 to obtain partial information from m_0 and m_1. Therefore, to prevent Bob from cheating in this way, the measurement results cannot be used directly as keys to encrypt the information.

Therefore, in Step 5, Alice's two sets of measurement results K_0 and K_1 are first hashed using a hash function to obtain H_0 and H_1, respectively, which are then used to encrypt the information m_0 and m_1. The purpose of this is to ensure that only with completely correct measurement results K_0 and K_1 can the information be obtained. If Bob categorizes the sets I_0 and I_1 dishonestly, he will not obtain completely correct K_0 and K_1, resulting in incorrect hash values. The choice of the hash function is illustrated using SHA-256 as an example. Assuming Bob obtains $\bar{K}_0$ and $\bar{K}_1$ using $\bar{I}_0$ and $\bar{I}_1$, he would need to pad $\bar{K}_0$ and $\bar{K}_1$ with $s/2$ bits each and exhaustively enumerate $2^{s/2}$ times to obtain all possible combinations. Then, decryption can be performed using the hash values. In this process, a large amount of readable plaintext may be obtained, and Bob will not be able to determine which plaintext is the actual message.

Soundness and security: Lo's no-go theorem states that unilateral quantum secure computation is impossible, and as a consequence, quantum one-out-of-two oblivious transfer is also impossible. However, recent findings [12] have shown that in Lo's definition of the one-out-of-two QOT model, Alice and Bob's inputs are mutually independent. In the proposed improved QOT scheme based on quantum bit commitment, Alice and Bob's inputs are correlated. The prepared n qubits, randomly selected R qubits, and H_0 and H_1 can all be considered as Alice's inputs, while Bob's inputs are the measurement bases chosen for the n qubits and either $\{I_0, I_1\}$ or $\{I_1, I_0\}$. It is evident that I_0 and I_1 depend to some extent on the indices of the R qubits randomly chosen by Alice, and H_0

and H_1 are also related to Bob's inputs. Therefore, the QOT scheme based on QBC can circumvent the implications of Lo's no-go theorem.

Based on the analysis of the QOT scheme above, it can be observed that before the disclosure phase, Bob can only honestly measure all the qubits, otherwise he will fail Alice's verification. However, the keys used by Alice to encrypt the information come from the measurement results of the remaining unverified qubits, and Alice is unaware of the information in the remaining unverified $n-R$ qubits. Thus, she has no knowledge of where the correct index set of $\{I_0, I_1\}$ or $\{I_1, I_0\}$ sent by Bob will be, and consequently, she does not know which message Bob will receive. If Bob honestly divides I_0 and I_1, Alice can only guess with a probability of $1/2$ which message Bob has obtained. Before disclosing her measurement bases, Alice randomly selects R qubits for verification, so prior to the disclosure phase, Bob cannot obtain any information from Alice other than knowing which qubits are being verified. If dishonest Bob wants to obtain both messages from Alice after the disclosure phase, the most likely approach is to include $s/2$ correct index positions in both I_0 and I_1. When Alice sends the hash function, Bob would need to exhaustively try all possible inputs (K_0 and K_1) of the hash function to decrypt Alice's two messages. The number of exhaustive trials would be $2\times 2^{s/2}=2^{s/2+1}$. Therefore, the difficulty for Bob to obtain the information would exponentially increase with the number of qubits, and there would be a large number of readable plaintexts that would make it impossible for Bob to determine the correct information. Hence, the introduction of a hash function ensures that Bob cannot obtain the two messages after encryption.

5 Conclusion

We propose two unconditionally secure QBC protocols, based on non-entangled states and based on entangled states, respectively. The hiding of the protocols relies on the no communication theorem and the quantum superposition principle; the binding of the protocols relies on the Bell state effect, the quantum superposition principle, and the inability to achieve the FTL nature of information exchange. Hiding and binding together constitute the unconditional security of the protocol. An unconditionally secure QOT protocol is also described based on the improvement of the model proposed by Yao and the proposed QBC.

References

1. M. Ardehali. A quantum bit commitment protocol based on epr states. *arXiv preprint quant-ph/9505019*, 1995.
2. J. S. Bell. On the einstein podolsky rosen paradox. *Physics Physique Fizika*, 1(3):195, 1964.
3. C. H. Bennett and G. Brassard. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, New York, 1984.
4. M. Born. Quantenmechanik der stoßvorgänge. *Zeitschrift für physik*, 38(11-12):803–827, 1926.

5. C. Y. Cheung. Quantum bit commitment can be unconditionally secure. *arXiv preprint quant-ph/0112120*, 2001.
6. C. Crépeau. Quantum oblivious transfer. *Journal of Modern Optics*, 41(12):2445–2454, 1994.
7. C. Crépeau and J. Kilian. Achieving oblivious transfer using weakened security assumptions. In *Proceedings of 29th Annual Symposium on Foundations of Computer Science*, pages 42–52. IEEE Computer Society, 1988.
8. P. H. Eberhard and R. R. Ross. Quantum field theory cannot provide faster-than-light communication. *Foundations of Physics Letters*, 2(2):127–149, 1989.
9. A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, 1935.
10. S. Even, O. Goldreich, and A. Lempel. A randomized protocol for signing contracts. *Communications of the ACM*, 28(6):637–647, 1985.
11. G. C. Ghirardi, R. Grassi, A. Rimini, and T. Weber. Experiments of the epr type involving cp-violation do not allow faster-than-light communication between distant observers. *EPL (Europhysics Letters)*, 6(2):95, 1988.
12. G. He. Can relativistic bit commitment lead to secure quantum oblivious transfer? *The European Physical Journal D*, 69:1–8, 2015.
13. M. Keller, E. Orsini, and P. Scholl. Mascot: faster malicious arithmetic secure computation with oblivious transfer. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 830–842, 2016.
14. A. Kent. Unconditionally secure bit commitment. *Physical Review Letters*, 83(7):1447, 1999.
15. A. Kent. Secure classical bit commitment using fixed capacity communication channels. *Journal of Cryptology*, 18(4):313–335, 2005.
16. N. Lee and T. Hwang. On the security of fair blind signature scheme using oblivious transfer. *Computer Communications*, 22(3):287–290, 1999.
17. D. Liu, C. Pei, D. Quan, B. Han, and N. Zhao. A new attack strategy for bb84 protocol based on, breidbart basis. In *2009 Fourth International Conference on Communications and Networking in China*, pages 1–3. IEEE, 2009.
18. H. K. Lo. Insecurity of quantum secure computations. *Physical Review A*, 56(2):1154, 1997.
19. H. K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78:3410–3413, 1997.
20. H. K. Lo and H. F. Chau. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D: Nonlinear Phenomena*, 120(1-2):177–187, 1998.
21. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78:3414–3417, 1997.
22. A. Peres and D. R. Terno. Quantum information and relativity theory. *Reviews of Modern Physics*, 76(1):93–123, 2004.
23. M. Rabin. How to exchange secrets with oblivious transfer. *Technical Report Tech. Memo TR-81, Aiken Computation Laboratory*, 1981.
24. E. Schrödinger. Quantisierung als eigenwertproblem. *Annalen der physik*, 385(13):437–490, 1926.
25. P. W. Shor. Algorithms for quantum computation: discrete logarithms and factoring. In *Proceedings 35th Annual Symposium on Foundations of Computer Science*, pages 124–134, 1994.
26. J. Silman, A. Chailloux, N. Aharon, I. Kerenidis, S. Pironio, and S. Massar. Fully distrustful quantum bit commitment and coin flipping. *Physical review letters*, 106(22):220501, 2011.

27. Y. Song and L. Yang. Practical quantum bit commitment protocol based on quantum oblivious transfer. *Applied Sciences*, 8(10):1990, 2018.
28. T. Tassa. Generalized oblivious transfer by secret sharing. *Designs, Codes and Cryptography*, 58:11–21, 2011.
29. P. Wang and Y. Su. Bqp $\neq$ qma, Cryptology ePrint Archive, Paper 2023/703, 2023. https://ia.cr/2023/703.
30. P. Wang, R. Zhang, G. Jiang, and Z. Sun. Computationally secure quantum oblivious transfer. *Advanced Quantum Technologies*, 2100125, 2021.
31. S. Wiesner. Conjugate coding. *Sigact News*, 15:78–88, 1983.
32. J. Yan, J. Weng, D. Lin, and Y. Quan. Quantum bit commitment with application in quantum zero-knowledge proof. In *Algorithms and Computation: 26th International Symposium, ISAAC 2015, Nagoya, Japan, December 9-11, 2015, Proceedings 26*, pages 555–565. Springer, 2015.
33. A. C.-C. Yao. Security of quantum protocols against coherent measurements. In *Proceedings of the twenty-seventh annual ACM symposium on Theory of computing*, pages 67–75, 1995.