Secure Quantum Bit Commitment

Ping Wang[1,2], Yiting Su[1] and Fangguo Zhang[3]

[1] College of Electronics and Information Engineering,
Shenzhen University, Shenzhen 518060, China
wangping@szu.edu.cn, suyiting2020@email.szu.edu.cn
[2] Guangdong Key Laboratory of Intelligent Information Processing,
Shenzhen 518060, China
[3] School of Computer Science and Engineering,
Sun Yat-sen University, Guangzhou 510006, China
isszhfg@mail.sysu.edu.cn

Abstract. Bit commitment (BC) is one of the most important fundamental protocols in secure multi-party computation. However, it is generally believed that unconditionally secure bit commitment is impossible even with quantum resources. In this paper, we design a secure non-interactive bit commitment protocol by exploiting the no-communication theorem of the quantum entangled states, whose security relies on the indistinguishability of whether the Bell states are measured or not. The proposed quantum bit commitment (QBC) is secure against classical adversaries with unlimited computing power, and the probability of a successful attack by quantum adversaries decreases exponentially as n (the number of qubits in a group) increases.

Keywords: bit commitment, quantum bit commitment, no-communication theorem, unconditionally secure, information-theoretically secure

1 Introduction

The concept of bit commitment, first introduced by Blum [4] in 1982, is an important primitive in cryptography that can be used to construct protocols such as zero-knowledge proofs, verifiable secret sharing, and coin tossing. Bit commitment and obvious transfer protocols together form the basis of secure multi-party computation. Numerous complex secure multi-party computation schemes, as well as practical application protocols, can be constructed based on them.

A simple version of the bit commitment is: In the first phase, Alice chooses a bit $x = 0$ (or 1), and sends the corresponding information y to Bob. In the second phase, Alice provides the evidence π, and Bob verifies Alice's choice x according to y and π. The key to the problem is that, on the one hand, Alice cannot modify the value of x once she has chosen the bit, or Alice cannot successfully cheat to make Bob pass the verification if she changes the value of x. On the other hand, Bob cannot get any information about x based on y. The point, therefore, is to

lock Alice's choice and make sure that Bob cannot get any information about Alice's choice based on publicly available information.

Classical bit commitment schemes [4,10] are based on certain complexity-theoretic assumptions and thus invariably make restrictive assumptions on the computational power of the committer (prover) or verifier. No classical bit commitment protocol can achieve unconditional security in terms of both *hiding* and *binding*. Fortunately, the development of quantum information technology has provided new ideas and approaches to cryptography, using properties unique to quantum, such as quantum superposition, quantum entanglement, quantum uncertainty principle, quantum no-cloning theorem, etc., which make it possible for us to design unconditionally secure cryptographic protocols, such as BB84. A cryptosystem is unconditionally secure (often used interchangeably with information-theoretically secure) if it cannot be broken by an adversary with unlimited computational power, and its security is solely based on information theory. Rather than being based on computational complexity theory, such security proofs must be based on information theory (e.g., probability theory) or physical laws. A bit commitment protocol is said to be unconditionally secure if it meets both *hiding* and *binding* requirements and does not make any restrictive assumptions about the attacker's computing power.

Unfortunately, Mayers [15], Lo and Chau [13,14] successfully demonstrated that all the previously proposed quantum bit commitment (QBC) protocols are not unconditionally secure, because the sender, Alice, can almost always successfully cheat by delaying her measurement until she opens her commitment using an Einstein–Podolsky–Rosen (EPR) type of attack. It resulted in a widespread acceptance of the non-existence of unconditionally secure quantum bit commitment [19]. The Mayers–Lo–Chau (MLC) no-go theorem (based on the Hughston–Jozsa–Wootters (HJW) theorem [11,12]) proves that any finite set compatible with a given density operator can be obtained from a fixed initial state by operations on space-like separation systems. The theorem holds true for two systems $\alpha \otimes \beta$ with exactly the same density matrix and tensor into the same subspace. The MLC no-go theorem show that the two basic security requirements (*hiding* and *binding*) of quantum bit commitment are inconsistent.

In this paper, we design a secure non-interactive bit commitment protocol. The protocol is secure against classical adversaries with unlimited computational power, and the probability of a successful attack by quantum adversaries (using the MLC-based attack strategy) decreases exponentially as n (the number of quantum bits in a set) increases. Rather than using the quantum entanglement property directly, we generalize the no-communication theorem for the entangled states to the Bell states. The hiding of the protocol relies on the no-communication theorem of the quantum entangled states (also the impossibility of faster-than-light (FTL) communication) and the quantum no-cloning theorem. Moreover, the *binding* of the protocol relies on the non-local effect of entangled systems and the principle of quantum superposition. In fact, we consider the following case: Alice is required to choose either a non-entangled state ($x = 0$) or an entangled state ($x = 1$) as evidence in the first stage. When Alice sends

a non-entangled state to Bob in the first stage, she will not be able to convince Bob that the state of evidence is a subsystem of an entangled state. Meanwhile, when Alice sends an entangled state to Bob in the first stage, she will not be able to convince Bob that these are pure states encoding certain information. Moreover, we make it possible to bind the commitment bit without leaking the value by a subtle connection of binary addition.

To this end, the structure of the paper is as follows: Section 2 will introduce the basic tools used to design the new scheme, and we will extend the no-communication theorem for the entangled states to the Bell states. Section 3 will design a new quantum bit commitment based on the quantum no-cloning theorem, the no-communication theorem, and the quantum entanglement properties. Section 4 will prove and analyze the *hiding* and *binding* properties of the new protocol respectively. Finally, Section 5 concludes the paper.

2 Preliminaries

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

2.1 Quantum Entanglement

In 1935, Schrödinger explicitly mentioned the concept of entanglement in his famous paper on "Schrödinger's cat" [18]. The definition of the quantum entangled state of the two subsystems is: for the quantum system composed of two subsystems p and q, if the state vector of the whole system $|\psi(p,q)\rangle$ cannot be written into the direct product form of the state vector of the subsystem $|\psi(p)\rangle \otimes |\psi(q)\rangle$, the state $|\psi(p,q)\rangle$ is called entangled state, and the two subsystems p and q are called entangled. The two-bit logic gate for quantum computing is usually referred to as the controlled-NOT gate (CNOT).

According to the theory of quantum mechanics, the pair of Bell qubits as a quantum system can be in the following quantum states (called Bell states or EPR pairs): $|\phi_{pq}\rangle = \frac{1}{\sqrt{2}}(|\uparrow\rangle_p |\uparrow\rangle_q + |\downarrow\rangle_p |\downarrow\rangle_q)$. Wherein $|\uparrow\rangle_p$ and $|\downarrow\rangle_p$ represent the spin-up and spin-down eigenstates of qubit p respectively, while $|\uparrow\rangle_q$, $|\downarrow\rangle_q$ represent the spin-up and spin-down eigenstates of qubit q respectively. This is actually a quantum entangled state. For the system of states $|\phi_{pq}\rangle$, it is predicted that the probability of a qubit p (or q) being measured spin up (or down) alone is $1/2$, but once the spin of qubit p is measured spin up (or down), the spin of qubit q must be spin up (or down). That is, the measurement outcomes are correlated. No matter how far apart the two qubits are, they are in this interconnected state, which is the non-local effect (or called the EPR effect) of quantum mechanics. The measurement correlations in the Bell state are stronger than could ever exist between classical systems. Quantum entanglement has wonderful non-classical properties and is an extremely important resource for information processing.

2.2 No-communication Theorem

The Bell states $|\beta_{xy}\rangle \triangleq \frac{1}{\sqrt{2}}(|(0,y)\rangle + (-1)^x|1,\overline{y}\rangle)$ where $\overline{y}$ is the negation of y and $x, y \in \{0,1\}$, are specific quantum states of two qubits that represent the simplest (and maximal) examples of quantum entanglement. Although quantum entanglement shows incredible effects, certain events that are far apart can somehow be correlated, which strongly implies that communication between entangled quantums may be faster than the speed of light, thus making faster-than-light communication possible. However, the no-communication theorem (or no-signaling principle) gives conditions under which FTL communication between two observers is not possible using entanglement. These results can be used to understand so-called paradoxes in quantum mechanics, such as the EPR paradox, or violations of local realism obtained in the tests of Bell's theorem. The no-communication theorem shows that the failure of local realism does not lead to the so-called "spooky communication at a distance". Further, we have the following no-communication Theorem, the proof of which can be referred to [6,9,17].

Theorem 1 (No-communication Theorem). *During measurement of an entangled quantum state, it is not possible for one observer, by making a measurement of a subsystem of the total state, 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'.

The proof proceeds by defining how the total Hilbert space H can be split into two parts, H_a and H_b, describing the subspaces accessible to Alice and Bob. The total state of the system is assumed to be described by a density matrix σ [17]. This appears to be a reasonable assumption, as a density matrix is sufficient to describe both pure and mixed states in quantum mechanics. Another important part of the theorem is that measurement is performed by applying a generalized projection operator P to the state σ. After a measurement by Alice, the state of the total system is said to have collapsed to a state $P(\sigma)$.

The goal of the theorem is to show that Bob cannot distinguish between the pre-measurement state σ and the post-measurement state $P(\sigma)$. This is accomplished mathematically by comparing the traces of σ and $P(\sigma)$, with the trace being taken over the subspace H_a. Because the trace only spans a subspace, it is technically referred to as a partial trace. The assumption that the (partial) trace adequately summarizes the system from Bob's perspective is critical to this step. That is, a partial trace over H_a of the system σ completely describes

everything that Bob has access to, or could ever have access to, measure, or detect. The fact that this trace never changes as Alice performs her measurements is the conclusion of the proof of the no-communication theorem. Simply put, the theorem states that given some initial state, prepared and shared in some way, Bob cannot detect which actions Alice takes.

To facilitate the application of the no-communication theorem, we generalize it to the Bell states. According to the no-communication theorem, we have the following fact: Suppose Alice and Bob each get a qubit from a Bell state, and without further information exchange, neither can tell afterwards whether the other has measured the qubit at hand.

Theorem 2. *Let (p, q) denote a Bell state, where p denotes one qubit of the Bell state and q denotes the other one. Given the qubit p, there is no way to determine afterwards whether q has been measured or not.*

It is clear that Theorem 2 can be seen as a specific instance of Theorem 1, since the qubits owned by Alice and Bob respectively are subsystems of the whole entangled state. In fact, considered from another perspective, if Theorem 2 does not hold, it will immediately lead to FTL communication. Moreover, we have the following corollary.

Corollary 1. *Alice and Bob share n Bell states, i.e., they each take one qubit from each Bell state. Then Alice has two choices, Alice either measures all n qubits in her hand or does not measure any qubit and keep the entangled states. If there is no further information exchange between them, then there is no way for Bob to determine Alice's choice.*

Again, since the qubits owned by Alice and Bob are subsystems of the whole system, it is not possible to determine whether the other has measured the qubits in hand or not, which would otherwise lead to the conclusion that they can communicate by measuring the subsystems, which is contrary to Theorem 1. Furthermore, according to Theorem 2, we have the following indistinguishability theorem. That is, given an unknown state, it is impossible to determine whether it is a subsystem of an entangled state or a non-entangled state.

Theorem 3 (Indistinguishability Theorem). *Let (p, q) denote a Bell state, where p denotes one qubit of the Bell state and q denotes the other one. Let $\{|0\rangle, |1\rangle\}$ denote the computational basis and $\{|+\rangle, |-\rangle\}$ denote the Hadamard basis. Given an unknown quantum state $w \in \{p, q, |0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, it is impossible to determine whether it belongs to the set $\{p, q\}$ or to the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$.*

Obviously, the disproof of Theorem 3 will lead to the disproof of Theorem 2. Furthermore, according to Theorem 3, we have the following corollary.

Corollary 2. *Let $(a_i, b_i) \triangleq \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ $(1 \leq i \leq n)$ denotes n Bell states, 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 $b \triangleq [b_1, b_2, ..., b_n]$. That is, the n Bell states are divided into*

two sets of qubit sequences a and b. Let $c \triangleq [c_1, c_2, ..., c_n]$ denote a qubit sequence, where each c_i is a randomly selected qubit from the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Given an unknown qubit sequence $d \in \{a, c\}$, it is impossible to determine whether $d = a$ or $d = c$.

The bit commitment protocol proposed in this paper essentially relies on Theorem 3 and Corollary 2.

2.3 Quantum Conjugate Coding

Quantum conjugate coding as a cryptographic tool was introduced by Wiesner [20] in the late 1960s, along with two applications: making money that is in principle impossible to counterfeit, and multiplexing two or three messages in such a way that only one can be read. The initial concept of quantum cryptography developed by Bennett and Brassard [2] was also based on this concept.

In order to encode a bit $m_1 \in \{0, 1\}$ into a qubit that can be read or copied reliably only with the help of a key bit $k_1 \in \{0, 1\}$, we generate a qubit with a selected one of the four polarization directions 0, 45, 90 and 135 degrees.

Definition 1 (Quantum Conjugate Encoding [3]). *The quantum encoding $Q_k(m)$ of a message m by a key k of equal length is the train of qubits obtained by applying the above procedure bitwise to m and k.*

Suppose an eavesdropper intercepts and attempts to read a quantum transmission $Q_k(m)$ without being detected. Consider first the case in which the message m and key k are both random, where $m, k \in \{0, 1\}^n$. Not knowing k, the eavesdropper makes the wrong measurement on half the qubits, and thus obtains a message m' differing from m in 1/4 of its bit positions (of course the eavesdropper does not know which ones). Even if k_i is correctly picked and the correct m_i is returned, without knowing m in advance, a random message with random errors still looks random.

3 New Quantum Bit Commitment

Bit commitment was first proposed by Blum [4] in 1982. Bit commitment is a cryptographic task that requires two parties, Alice and Bob, who do not trust each other and do not communicate face-to-face, to make a one-bit ($x = 0$ or 1) commitment from Alice to Bob and reach a consensus between them without the help of a third party. Furthermore, a bit commitment scheme generally has the following properties:

Correctness: If both Alice and Bob execute the protocol honestly, then Bob will receive the committed bit x correctly in the opening phase.

Hiding: Bob should not be able to identify the bit x that Alice committed until she reveals it. If Bob has probability $1/2+\epsilon$ of being able to obtain the correct committed bit x before the opening phase, then ϵ can be made arbitrarily (or exponentially) small by increasing the input size n of the protocol.

Binding: Alice should not be able to alter the value of the bit x once she has committed. The probability of Alice's successful cheating is bounded by ϵ, where ϵ can be made arbitrarily (or exponentially) small by increasing the input size n of the protocol.

We refer to a bit commitment protocol as unconditionally secure if it can satisfy both *hiding* and *binding* without limitations on the computing power of the adversary. Previous classical protocols to tackle this problem were based on unproven assumptions in computational complexity theory, which made them vulnerable to breakthroughs in algorithm design and quantum computers. For quantum bit commitments, based on the MLC attack strategy, Alice prepares suitable entangled quantum states during the commit phase and is always able to change the commitment through the subsystem she accesses during the open phase.

Here, we consider designing a non-interactive quantum bit commitment protocol. The protocol is able to resist classical adversaries with unlimited computing power, and the probability that quantum adversaries can cheat successfully using the MLC attack strategy decreases exponentially as n increases. The basic idea is as follows: Alice generates n Bell states denoted as $(a_i, b_i) = \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ with $1 \leq i \leq n$, where a_i denotes one qubit of the ith Bell state and b_i denotes the other one. Alice has two choices, one (e.g., $x = 0$) is to measure all a_i's of the Bell states, and the other ($x = 1$) is not to measure and keep the entangled states. Alice then keeps all b_i's and sends all a_i's to Bob with $1 \leq i \leq n$. This process is equivalent to: Alice and Bob share n Bell states, i.e., they each take one qubit from each Bell state, and then Alice has two choices, Alice either measures all qubits in her hand or does not measure and keep the entangled states. Therefore, if there is no further information exchange between Alice and Bob, then according to the no-communication theorem, there is no way for Bob to determine Alice's choice.

Furthermore, if Alice chooses $x = 0$, to prevent Alice from denying her choice later, Alice needs to encode certain information into qubits as evidence and send it to Bob. We will show that Alice cannot change the value of x after she has chosen $x = 0$ or 1. Bob cannot obtain any information about x based on the qubits he received. Moreover, he can verify the value of x based on the proofs provided by Alice.

Let $|0\rangle, |+\rangle, |1\rangle, |-\rangle$ be the four states of light polarization of angles $0°, 45°, 90°, 135°$. For simplicity, we denote these four states as $|0,0\rangle, |1,0\rangle, |0,1\rangle, |1,1\rangle$. If the key bit is 0, then the qubit is polarized computationally at 0 or 90 degrees according to whether the message bit is 0 or 1. If the key bit is 1, then the qubit is polarized Hadamardly at 45 or 135 degrees according to the message bit. The framework of the proposed non-interactive quantum bit commitment protocol is shown in Fig. 1. For the sake of simplicity, we suppose that the quantum operations and communications are error-free in the proposed protocol. In more detail, we describe the protocol as follows.

Commit Phase

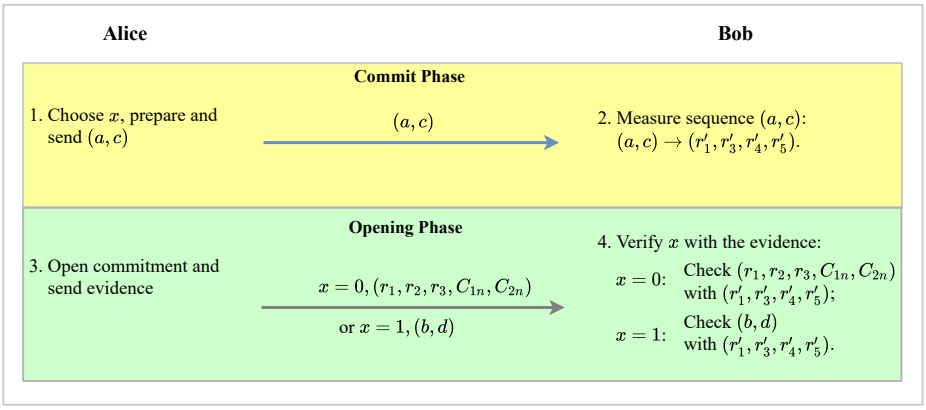

Fig. 1. The Framework of the New Bit Commitment Protocol

Alice has two choices: commit to $x = 0$ or commit to $x = 1$. We refer to these two commitments as *Non-Entanglement Commitment* (e.g., $x = 0$) and *Entanglement Commitment* ($x = 1$), respectively. Alice needs to complete different procedures under the two different commitments. We describe the steps for each of these two commitments, respectively, as follows.

Non-Entanglement Commitment ($x = 0$):

1) Alice generates three n-bit ($n > 1$, e.g. $n = 1000$) random numbers: $r_1 \triangleq r_{11}r_{12}...r_{1n}$, $r_2 \triangleq r_{21}r_{22}...r_{2n}$ and $r_3 \triangleq r_{31}r_{32}...r_{3n}$. Let $r_4 \triangleq r_{41}r_{42}...r_{4n} = r_2+r_3+C_{1n}$ and $r_5 \triangleq r_{51}r_{52}...r_{5n} = r_1+r_2+C_{2n}$, i,e., $r_1+r_4+C_{2n} = r_3+r_5+C_{1n}$, where $+$ denotes the full adder (with respect to $+$, assume r_{21} is the highest bit and r_{2n} is the lowest bit), and C_{1n} (*also* C_{2n}) can be either 0 or 1 with an equal probability of 1/2. As shown in the Fig. 2.

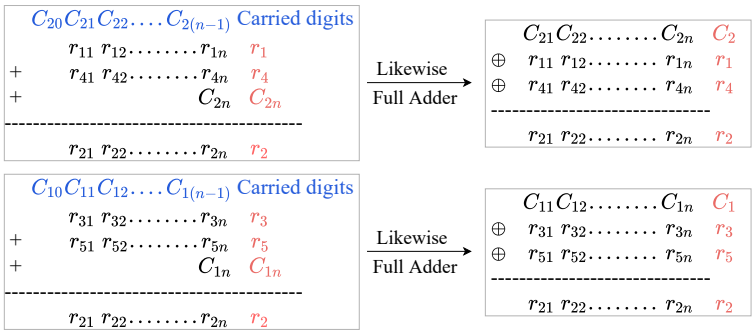

Fig. 2. Derived Form with Carry Digits

2) $\underset{i=1}{\overset{n}{DO}}$ Alice picks the bit r_{4i} and makes a qubit a_i with polarization $|r_{1i}, r_{4i}\rangle$.

3) $\underset{i=1}{\overset{n}{DO}}$ Alice picks the bit r_{5i} and makes a qubit c_i with polarization $|r_{3i}, r_{5i}\rangle$.

4) Let $(a, c) \triangleq [a_1, a_2, ..., a_n, c_1, c_2, ..., c_n]$. Alice sends (a, c) as the commitment information to Bob via the quantum channel.

Entanglement Commitment ($x = 1$):

1) Alice generates 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 $b \triangleq [b_1, b_2, ..., b_n]$. Generates another n Bell states denoted as $(c_i, d_i) \triangleq \frac{|00\rangle+|11\rangle}{\sqrt{2}}$ with $1 \leq i \leq n$. Let $c \triangleq [c_1, c_2, ..., c_n]$ and $d \triangleq [d_1, d_2, ..., d_n]$.

2) Let $(a, c) \triangleq [a_1, a_2, ..., a_n, c_1, c_2, ..., c_n]$. Alice sends (a, c) as the commitment information to Bob via the quantum channel.

Subsequently, once Bob receives the qubit sequence of (a, c), he randomly selects the computational basis or the Hadamard basis for each received qubit to perform the measurement and records the measurement results. The specific steps are as follows.

1) Bob generates two n-bit random numbers $r'_1 \triangleq r'_{11}r'_{12}...r'_{1n}$ and $r'_3 \triangleq r'_{31}r'_{32}...r'_{3n}$.

2) $\underset{i=1}{\overset{n}{DO}}$ Bob measures a_i with the computational basis if $r'_{1i} = 0$, otherwise Bob measures a_i with the Hadamard basis. Record $r'_{4i} = 0$ if the measurement result belongs to $\{|0\rangle, |+\rangle\}$, and record $r'_{4i} = 1$ if the measurement result belongs to $\{|1\rangle, |-\rangle\}$.

3) $\underset{i=1}{\overset{n}{DO}}$ Bob measures c_i with the computational basis if $r'_{3i} = 0$, otherwise Bob measures c_i with the Hadamard basis. Record $r'_{5i} = 0$ if the measurement result belongs to $\{|0\rangle, |+\rangle\}$, and record $r'_{5i} = 1$ if the measurement result belongs to $\{|1\rangle, |-\rangle\}$.

4) Let $r'_2 \triangleq r'_{41}r'_{42}...r'_{4n}$ and $r'_5 \triangleq r'_{51}r'_{52}...r'_{5n}$. Therefore, Bob gets the quadruple (r'_1, r'_3, r'_4, r'_5).

This is the end of the commit phase. Concerning the polarization bases chosen independently by Alice and Bob, the protocol requires that they follow the randomization principle.

Opening Phase

According to Alice's *Non-Entanglement Commitment* ($x = 0$) and *Entanglement Commitment* ($x = 1$), correspondingly, we will describe two different cases in the opening phase: *Non-Entanglement Check* and *Entanglement Check*, respectively. The specific steps are as follows.

Non-Entanglement Check ($x = 0$):

1) Alice opens her commitment $x = 0$ to Bob by sending him the quadruple $(r_1, r_2, r_3, C_{1n}, C_{2n})$.

2) Bob computes $r_4 \triangleq r_{41}r_{42}...r_{4n} = r_2 + r_3 + C_{1n}$ and $r_5 \triangleq r_{51}r_{52}...r_{5n} = r_1 + r_2 + C_{2n}$. Bob will accept the choice $x = 0$ only if the two quadruples (r_1, r_3, r_4, r_5) and (r'_1, r'_3, r'_4, r'_5) meet both of the following two requirements:

2.1) For all i, $r'_{4i} = r_{4i}$ if $r'_{1i} = r_{1i}$;
2.2) For all i, $r'_{5i} = r_{5i}$ if $r'_{3i} = r_{3i}$.

Entanglement Check ($x = 1$):

1) Alice opens her commitment $x = 1$ by sending qubit sequence $(b, d) \triangleq [b_1, b_2, ...b_n, d_1, d_2, ..., d_n]$ to Bob.

2) $\underset{i=1}{\overset{n}{DO}}$ Bob measures b_i with the computational basis if $r'_{1i} = 0$, otherwise Bob measures b_i with the Hadamard basis. Record $r''_{4i} = 0$ if the measurement result belongs to $\{|0\rangle, |+\rangle\}$, and record $r''_{4i} = 1$ if the measurement result belongs to $\{|1\rangle, |-\rangle\}$.

3) $\underset{i=1}{\overset{n}{DO}}$ Bob measures d_i with the computational basis if $r'_{3i} = 0$, otherwise Bob measures d_i with the Hadamard basis. Record $r''_{5i} = 0$ if the measurement result belongs to $\{|0\rangle, |+\rangle\}$, and record $r''_{5i} = 1$ if the measurement result belongs to $\{|1\rangle, |-\rangle\}$.

4) Let $r''_4 \triangleq r''_{41}r''_{42}...r''_{4n}$ and $r''_5 \triangleq r''_{51}r''_{52}...r''_{5n}$. Bob will accept the choice $x = 1$ only if the quadruple $(r'_4, r''_4, r'_5, r''_5)$ meets both of the following two requirements:
4.1) For all i, $r''_{4i} = r'_{4i}$;
4.2) For all i, $r''_{5i} = r'_{5i}$.

This is the end of the opening phase, and also the end of the whole bit commitment protocol. We will show that Bob can not obtain anything about x before the opening phase. One key point is that, with the help of C_{1n} ($also\ C_{2n}$), each bit of C_1 ($also\ C_2$) can be either 0 or 1 with the same probability of 1/2, so C_1 ($also\ C_2$) is a totally random number for Bob. Hence, the mutual information of r_4 and r_5 is 0. Moreover, Alice can not tamper with x, once the commit phase is finished. In particular, we will analyze the new protocol from three perspectives: *Correctness*, *Hiding* and *Binding*, respectively.

As mentioned above, if Alice chooses $x = 0$, to prevent Alice from denying her choice later, she needs to encode certain information into qubits as evidence and send it to Bob. The main ideas of the protocol: Let's suppose that the protocol is directly disclosed $r_2 = F(r_1, r_4)$ (disguised r_2 is disclosed in the choice of $x = 1$), such that the protocol is *binding*, but not sufficiently *hiding*. To achieve the goal that r_2 is committed by Alice and is unknown to Bob, we adopt the strategy of encoding certain information $r_2 = F(r_3, r_5)$ into the auxiliary sequence c. Based on the quantum no-cloning theorem, Bob knows nothing about C_2 where $C_{2i} = f(r_{1(i+1)}, r_{4(i+1)}, r_{2(i+1)}) = r_{1i} \oplus r_{4i} \oplus r_{2i}$. That is, Bob is not sure about the connection between b_i and b_{i+1} ($also\ c_i$ and c_{i+1}). Given this, Bob could analyze only for each quantum pair $[b_i, c_i]$.

Correctness: *If Alice and Bob behave as described in this protocol, Bob will always receive the correct commitment bit in the opening phase.* For different commitment bits, Alice needs to provide different validation information in the opening phase. When Alice commits $x = 0$, she needs to provide a $3n + 2$-bit string to Bob for the *Non-Entanglement Check*. But while committing $x = 1$, she needs to provide a $2n$-qubit state to Bob for the *Entanglement Check*.

On the one hand, Alice can provide proof to convince Bob $x = 0$ if she had previously chosen $x = 0$. In this QBC protocol, when Alice chooses $x = 0$, then the requirement $r_4 = r_2 + r_3 + C_{1n}, r_5 = r_1 + r_2 + C_{2n}$ needs to be met. As Bob receives the qubit a_i (or c_i), he decides, randomly for each qubit and independently of Alice, whether to measure the qubit with computational basis or Hadamard basis. In general, Bob obtains the same measurement result from half the qubits he detects, those for which he guessed the correct polarization basis. Therefore, Alice can always convince Bob that $x = 1$ if she publishes the proof $(r_1, r_2, r_3, C_{1n}, C_{2n})$ honestly.

On the other hand, Alice can provide proof to convince Bob $x = 1$ if she had previously chosen $x = 1$. Let (p, q) denote a Bell state, where p denotes one qubit of the Bell state and q denotes the other one. On the theory of quantum mechanics, the Bell state as a quantum system can be in the following quantum state: $(p, q) \triangleq \frac{1}{\sqrt{2}}(|0\rangle_p |0\rangle_q + |1\rangle_p |1\rangle_q) = \frac{1}{\sqrt{2}}(|+\rangle_p |+\rangle_q + |-\rangle_p |-\rangle_q)$. Once the measurement result of qubit q belongs to $|0\rangle$ (or $|-\rangle$), then the measurement result of qubit p must belong to $|0\rangle$ (or $|-\rangle$), and vice versa. Two qubits are in this interconnected state no matter how far apart they are, and this is the EPR effect of quantum mechanics as explained in the Section 2.1.

4 Security Analysis and Discussion

4.1 Hiding

If Alice behaves as described in this protocol, her bit is not disclosed to Bob whatever he does. In the QBC protocols, there are two quantum states for evidence: one for $x = 0$ and another for $x = 1$. In order to hide x, the density operator of the evidence state should be almost the same. The reason for this fact is that quantum ensembles (systems with various possibilities) are characterized by a density matrix. When two systems are characterized by the same density matrix, no measurement whatsoever can tell them apart.

Let's first analyze the density matrices. As previously mentioned in Section 2.4, with respect to $r_4 = r_2 + r_3 + C_{1n}, r_5 = r_1 + r_2 + C_{2n}$, in terms of a single bit (full adder), it can be written as the following form $S = A \oplus B \oplus C_{in}, C_{out} = A \cdot B + C_{in} \cdot (A \oplus B)$, i.e., $r_{1i} \oplus r_{4i} \oplus C_{2i} = r_{3i} \oplus r_{5i} \oplus C_{1i}$, where $C_{2i} = f(r_{1(i+1)}, r_{4(i+1)}, r_{2(i+1)}), C_{1i} = f(r_{3(i+1)}, r_{5(i+1)}, r_{2(i+1)})$. Therefore, quantum pairs $[a_i, c_i]$ and $[a_{i+1}, c_{i+1}]$ are not independent of each other in the choice of $x = 0$.

However, when the choice $x = 1$ is made, since r_1 and r_3 follows the randomization principle, each qubit of (a, c) can be regarded as a system consisting of $|0\rangle, |+\rangle, |1\rangle, |-\rangle$ mixed with an equal probability of $1/4$, which has a density matrix $\rho_{mix} = \frac{1}{2}(|0\rangle\langle 0| + |1\rangle\langle 1|)$. Let ρ_x^B be the density matrix corresponding to the mixture (a, c) sent by Alice when classical bit x is committed. Since each qubit of sequence (a, c) is independent of each other in the choice of $x = 1$, we

get

$$\sum_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}} \frac{1}{N} |\psi\rangle_{ac} \langle\psi|_{ac} = \rho_0^B \neq \rho_1^B = \bigotimes_{i=1}^{2n} \rho_{min},$$

where:

N is the normalization constant;

$|\psi\rangle_{ac} = |r_1, r_4\rangle_a \otimes |r_3, r_5\rangle_c$;

$|r_1, r_4\rangle_a = |r_{11}, r_{41}\rangle \otimes |r_{12}, r_{42}\rangle \otimes ... \otimes |r_{1n}, r_{4n}\rangle$;

$|r_3, r_5\rangle_c = |r_{31}, r_{51}\rangle \otimes |r_{32}, r_{52}\rangle \otimes ... \otimes |r_{3n}, r_{5n}\rangle$;

$\sum$ is sum up for all $r_1, r_4, r_3, r_5, C_{1n}, C_{2n}$ that satisfy the equation $r_1 + r_4 + C_{2n} = r_3 + r_5 + C_{1n}$.

Here, although $\rho_0^B \neq \rho_1^B$, the protocol remains in hiding because Bob does not hold multiple copies of system (a, c). The specific analysis is given below: In the commit phase, Bob receives the evidence of commitment from Alice in the form of $[a_1, a_2, ..., a_n, c_1, c_2, ..., c_n]$, containing sequence a and sequence c. It has been shown that the quantum sequence (a, c) is a non-entangled state (each qubit belongs to the set $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$) when the choice $x = 0$, and that the quantum sequence is a subsystem of the entangled system (each qubit belongs to the set $\{p, q\}$) when the choice $x = 1$. Assuming that Bob can determine whether the evidence state is a subsystem of the entangled system, it means that Bob can tell Alice's choice. However, as explained in Corollary 2, this is not possible for Bob.

Given that the above difference in the two commitments fails to be distinguished, we will focus on the choice $x = 0$. In this choice, the quantum sequence (a, c) is not an arbitrary non-entangled state. The proposed protocol requires that the polarization bases r_1 and r_3 and the encoded binary strings r_4 and r_5 need to meet $r_1 + r_4 + C_{2n} = r_3 + r_5 + C_{1n}$ (adding C_{1n} and C_{2n} to complement the carry digit for the lowest bit). In general, the key to Bob's cheating successfully lies in determining whether sequence a correlates with sequence c. If a correlation exists, it indicates that Alice has chosen $x = 0$; otherwise, it is classified as having chosen $x = 1$. Furthermore, we will specifically analyze whether Bob has a strategy to determine whether the two sequences are associated.

Considering Bob's possible cheating behaviour, he holds valid information about the commitment x in the commit phase as (a, c), beyond which there is no other valid information. As we have learned the commitment $x = 0$, it needs to satisfy $r_1 + r_4 + C_{2n} = r_3 + r_5 + C_{1n}$, where $C_{2i} = r_{1(i+1)} r_{4(i+1)} + r_{1(i+1)} \overline{r_{2(i+1)}} + \overline{r_{2(i+1)}} r_{4(i+1)}$. Based on the no-cloning theorem, Bob, who holds only (r'_1, r'_3, r'_4, r'_5), cannot identify any C_{2i} of the bit string C_2. Similarly, he cannot identify any C_{1i} for the reason that $C_{1i} = f(r_{3(i+1)}, r_{5(i+1)}, r_{2(i+1)})$. Therefore, Bob has no strategy to analyze whether quantum pairs $[b_i, c_i]$ and $[b_{i+1}, c_{i+1}]$ are associated. Let ρ'_x be the density matrix corresponding to the mixture $[b_i, c_i]$ sent by Alice when classical bit x is committed. The following discussion will focus on whether ρ'_0 equals ρ'_1. With respect to the input parameter $C_2 \triangleq C_{21} C_{22} ... C_{2n}$, it is trivial to get the following theorem according to the truth table of full adder.

Theorem 4. *A one-bit full-adder adds three one-bit numbers, written as* $A + B + C_{in}$*, where* A *and* B *are the operands, and* C_{in} *is a bit carried in from the previous less-significant stage. Given that the probability of all three one-bit numbers being 0 or 1 is* $1/2$*, it follows that the probability of the output carry* C_{out} *being 0 or 1 is also* $1/2$*.*

For $i = n$, the probability of r_{1n}, r_{4n} and C_{2n} being 0 or 1 is $1/2$, it follows that the probability of the output carry $C_{2(n-1)}$ being 0 or 1 is also $1/2$ based on Theorem 4. In this case, for $i = n - 1$, it follows that the probability of the output carry $C_{2(n-2)}$ being 0 or 1 is also $1/2$. And so on, each bit of C_2 can be either 0 or 1 with exactly the same probability of $1/2$. In summary, there is the formula $r_2 = r_1 \oplus r_4 \oplus C_2$ that holds, where C_2 is a totally random number for Bob. Similarly, there is the formula $r_2 = r_3 \oplus r_5 \oplus C_1$ that holds, where C_1 is a totally random number for Bob. In summary, the scheme picks the key $C_2 \triangleq C_{21}C_{22}...C_{2n}$, we get the mutual information of $r_{1i} \oplus r_{4i}$ and r_{2i}, i.e., $I_0\left(r_{1i} \oplus r_{4i}; r_{2i}\right) = 0$. Additionally, $I_0\left(r_{3i} \oplus r_{5i}; r_{2i}\right) = 0, I_0\left(r_{4i}; r_{5i}\right) = 0$.

In conclusion, there is $\rho_0' = \rho_1'$. As mentioned above, when two systems are characterized by the same density matrix, no measurement whatsoever can tell them apart, and the protocol meets hiding.

4.2 Binding

If Bob behaves as described in this protocol, then no matter what Alice does, she cannot tamper with the commitment in the opening phase. In the proposed scheme, the preparation of the sequence c forces Alice to make a choice. Specifically, whenever Alice is trying to prepare a sequence c capable of passing the *Non-Entanglement Check*, then the sequence a sent with it must not be a mixed state. The protocol requires that at each round, if $r_{1i}' = r_{1i}$, r_{4i}' must be a result that Alice can ascertain. In entanglement, one constituent cannot be fully described without considering the other. If a_i is part of an entangled system, in which case the description of qubit a_i is a mixed state, hence it can only commit to entanglement at this point.

1) On the one hand, if Alice commits to $x = 0$ **honestly in the first phase, then no matter what Alice does, she cannot tamper with the commitment to** $x = 1$ **in the opening phase.**

To begin with, since in the first phase, Alice only prepared sequence (a, c) and no sequence (b, d), yet pretending to commit $x = 1$ requires sending sequence (b, d) to Bob. In the choice of $x = 1$, Bob's main purpose is to verify the EPR effect of the Bell state, i.e., verify that each qubit of the pair $[a_i, b_i]$ (or $[c_i, d_i]$) belongs to the same state. Therefore, she will copy sequence a based on the identified data (r_1, r_4) and the copied sequence a is called the sequence b. Similarly copying the sequence c as the sequence d. It is easy to see that the situation would be worse if Alice had submitted not sequence b and sequence d in the second phase, but a completely new sequence b' or a new sequence d'. This is because the match between the sequence (b', d') and the sequence (a, c) is not as good as the match between the sequence (b, d).

In this case of cheating, Bob will inevitably measure the computational polarization of a Hadamard polarization qubit or vice versa. These measurements (r'_{4i} and r''_{4i}) are incompatible if $r'_{1i} \neq r_{1i}$. Moreover, Alice hopes that these incompatible measurements will be lucky enough to completely match to pass the *Entanglement Check*. This she cannot do reliably because these incompatible measurements are the result of probabilistic behaviour based on quantum superposition principle. Therefore, this cheating venture required Alice to be not only lucky but brave, as in the majority of cases, the gamble would have failed and been detected as cheating. Assuming that the probability of Alice and Bob choosing the same polarization bases r_{1i} and r'_{1i} is 1/2, then for each b_i, the probability of her getting a lucky victory is

$$Pr(r''_{4i} = r'_{4i}) = Pr(r'_{1i} = r_{1i}) \times Pr(r''_{4i} = r'_{4i} | r'_{1i} = r_{1i})$$

$$+Pr(r'_{1i} \neq r_{1i}) \times Pr(r''_{4i} = r'_{4i} | r'_{1i} \neq r_{1i}) = \frac{1}{2} + \frac{1}{2} \times \frac{1}{2} = \frac{3}{4}.$$

Similarly, for each d_i, the probability of her getting a lucky win is

$$Pr(r''_{5i} = r'_{5i}) = Pr(r'_{3i} = r_{3i}) \times Pr(r''_{5i} = r'_{5i} | r'_{3i} = r_{3i})$$

$$+Pr(r'_{3i} = r_{3i}) \times Pr(r''_{5i} = r'_{5i} | r'_{3i} = r_{3i}) = \frac{3}{4}.$$

To sum up, for all b_i and d_i with $i \in \{1, 2, ..., n\}$, the probability that she will get a lucky win is

$$Pr(\text{Successfully cheating entanglement from non-entanglement}) = (\frac{3}{4})^{2n}.$$

2) On the other hand, if Alice commits to $x = 1$ honestly in the first phase, then no matter what Alice does, she cannot tamper with the commitment to $x = 0$ in the opening phase.

To begin with, Alice has prepared only sequence (a, b, c, d) when the value $x = 1$ is chosen by her, but now needs to send the proof $(r_1, r_2, r_3, C_{1n}, C_{2n})$ to convince Bob that $x = 0$ was her initial choice. In the choice of $x = 0$, Bob's main purpose is to verify whether sequence (a, c) satisfies $r_1 + r_4 + C_{2n} = r_3 + r_5 + C_{1n}$. As mentioned above, the *Non-Entanglement Check* consists of two steps. In order to pass the first step of the check, Alice only needs to $\overset{n}{\underset{i=1}{DO}}$ pick a bit r_{1i} and measures b_i with computational basis if $r_{1i} = 0$ and Hadamard basis otherwise. Record $r''_{4i} = 0$ if $\{|0\rangle, |+\rangle\}$ as result and $r''_{4i} = 1$ if $\{|1\rangle, |-\rangle\}$ as result. Once she has honestly announced outcomes (r_1, r''_4), then the first step of the check always passes. Therefore the same conclusion can be drawn: once she has honestly announced outcomes (r_3, r''_5), then the second step of the check always passes.

Further to the above conclusions, it is necessary to describe the Einstein-Podolsky-Rosen effect [7,1] to show why Alice can always pass the sequence check. The EPR effect involves the fact that two qubits are always found to have the same polarization, regardless of the basis used to observe them, provided that both are on the same basis. In this case, it was not until the opening phase that

Alice made measurements of the sequence b and sequence d to get the probability result r''_4, r''_5. In the opening phase, Bob focuses only on qubits measured on the same basis, when the polarisations of these qubit pairs happen to always be the same.

As showed above, we know that Alice will always be able to match Bob's quadruple (r'_1, r'_3, r'_4, r'_5) as long as she announces (r_1, r_3, r''_4, r''_5) honestly. However, tampering with the choice $x = 0$, these data also required $r_1 + r_4 + C_{2n} = r_3 + r_5 + C_{1n}$, which is always not fulfilled. The variables on the left-hand side of the equation are parameters concerning sequence a, and the variables on the right-hand side of the equation are parameters concerning sequence c. In this case of cheating, Alice has a goal to guess which qubit ($r_{1i} \neq r'_{1i}$ or $r_{3i} \neq r'_{3i}$) Bob does not verify because the qubit's number at these positions can be stated by Alice at will without being questioned. This can't be achieved, therefore she must consider all the qubits. In order to fulfill the formula above, Alice would have to provide the proof $(r_1, r_2, ret_3, C_{1n}, C_{2n}) \rightarrow (r_1, ret_3, r''_4, r''_5)$ or $(r_1, r_2, r_3, C_{1n}, C_{2n}) \rightarrow (r_1, r_3, r''_4, ret_5)$ that fulfill the requirement instead of r_3 or r''_5, and each different bit substitution would be rejected probability. In the above strategy, for example, it ensures that the first requirement is met, as honestly announced (r_1, r''_4). For example, the calculated quadruple (e.g. $(r_1, ret_3, r''_4, r''_5)$) will meet the requirement of 2.1):

2.1) For all i, $r'_{4i} = r''_{4i}$ if $r'_{1i} = r_{1i}$;

2.2) For all i, $r'_{5i} = r''_{5i}$ if $r'_{3i} = ret_{3i}$.

Considering to announce $ret_5 = r_1 + r''_4 - r_3 + C_{2n} - C_{1n}$, Alice would provide the proof $(r_1, r_2, r_3, C_{1n}, C_{2n})$ to pass the verification. The major source of uncertainty r''_4 is the method used to calculate ret_5. Therefore, the values of the binary strings r''_5 and ret_5 are independent of each other, and theoretically $Pr(r''_{5i} = ret_{5i}) = Pr(r''_{5i} \neq ret_{5i}) = \frac{1}{2}$. A major problem with the experimental method is that the qubit c_i can only pass the check if $r''_{5i} = ret_{5i}$. Each difference in bits ($r''_{5i} \neq ret_{5i}$) has a probability of 1/2 not being detected, and the gamble will fail and be detected as cheating, i.e.,

$$Pr(\text{Successful cheat if announce } ret_5)$$

$$= (Pr(r''_{5i} = ret_{5i}) + Pr(r''_{5i} \neq ret_{5i}) \times Pr(r_{3i} = r'_{3i}))^n = (\frac{3}{4})^n.$$

Furthermore, considering to announce $ret_3 = r_1 + r''_4 - r''_5 + C_{2n} - C_{1n}$, Alice would provide the proof $(r_1, r_2, ret_3, C_{1n}, C_{2n})$. The major source of uncertainty r''_4 and r''_5 is the method used to calculate ret_3. Theoretically $Pr(r_{3i} = ret_{3i}) = Pr(r_{3i} \neq ret_{3i}) = \frac{1}{2}$. Based on the quantum uncertainty principle [16,8], and the fact that Bob only cares about measurements on the same polarization basis, there is a higher probability of getting a lucky win. More specifically, purely in terms of a qubit, it has a probability of 1/2 to pass the check because it is not cared for by Bob, and on the other hand, it has a probability of 1/2 to collapse to the desired state. Therefore, for each bit of difference ($r_{3i} \neq ret_{3i}$), she has a higher probability of 3/4 not being detected. A comparison of the two results reveals that the probability of a lucky win by announcing $(r_1, r_2, ret_3, C_{1n}, C_{2n})$

is higher, i.e.,

$$Pr(\text{Successful cheat if announce } ret_3)$$

$$= (Pr(r_{3i} = ret_{3i}) + Pr(r_{3i} \neq ret_{3i}) \times \frac{3}{4})^n = (\frac{7}{8})^n.$$

The probability can be made arbitrarily small by increasing the security parameters n in the protocol.

3) Alice's cheating based on the MLC attack strategy.

In fact, in addition to preparing the initial state honestly as in the above method, based on the powerful MLC attack strategy [13,14,15], Alice can also prepare the appropriate entanglement state by herself to implement the delayed measurement attack, as follows.

In the commit phase:

Alice prepares the following quantum states:

$$|\psi\rangle_{abcde} = \frac{1}{N} \sum_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}} |r_1, r_4\rangle_a |r_1, r_4\rangle_b |r_3, r_5\rangle_c |r_3, r_5\rangle_d |\varepsilon_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}\rangle_e,$$

where:

N is the normalization constant;

$\sum$ is sum up for all $r_1, r_4, r_3, r_5, C_{1n}, C_{2n}$ that satisfy the equation $r_1 + r_4 + C_{2n} = r_3 + r_5 + C_{1n}$;

$|r_1, r_4\rangle = |r_{11}, r_{41}\rangle \otimes |r_{12}, r_{42}\rangle \otimes ... \otimes |r_{1n}, r_{4n}\rangle$;

$|r_3, r_5\rangle = |r_{31}, r_{51}\rangle \otimes |r_{32}, r_{52}\rangle \otimes ... \otimes |r_{3n}, r_{5n}\rangle$, where $|r_{ij}, r_{kl}\rangle$ denotes the qubit that encodes r_{kl} with r_{ij} as the basis. That is, denote $|0\rangle, |+\rangle, |1\rangle, |-\rangle$ as $|0,0\rangle, |1,0\rangle, |0,1\rangle, |1,1\rangle$;

$\{|\varepsilon_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}\rangle_e\}$ ($r_1, r_4, r_3, r_5, C_{1n}, C_{2n}$ taking all possible values) is a set of orthogonal bases for system e.

Then, Alice sends systems (a, c) to Bob and keeps systems (b, d, e) for herself.

In the opening phase:

If Alice intends to claim that $x = 0$, it is clear that she only needs to measure the system e on the basis of $\{|\varepsilon_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}\rangle_e\}$ to know what kind of $r_1, r_4, r_3, r_5, C_{1n}, C_{2n}$ to publish based on the measurement results to successfully pass Bob's check.

If Alice intends to claim $x = 1$, as long as the proposed protocol meets the hiding condition, i.e., it is impossible to distinguish whether Alice commits $x = 0$ or $x = 1$ from the reduced density matrix of systems (a, c) alone, then, based on the HJW theorem [12], there exists a set of orthogonal bases $\{|\varepsilon'_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}\rangle_e\}$ with respect to system e such that $|\psi\rangle_{abcde}$ can be rewritten as:

$$|\psi\rangle_{abcde} = \frac{1}{N} \sum_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}} U_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}} \left(|\Phi^+\rangle_{ab} |\Phi^+\rangle_{cd}\right) |\varepsilon'_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}\rangle_e,$$

where:

$U_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}$ is the unitary transformation acting only on the system (b,d);

$$\left|\Phi^{+}\right\rangle_{ab}=\frac{|00\rangle_{a_1b_1}+|11\rangle_{a_1b_1}}{\sqrt{2}}\otimes\frac{|00\rangle_{a_2b_2}+|11\rangle_{a_2b_2}}{\sqrt{2}}\otimes...\otimes\frac{|00\rangle_{a_nb_n}+|11\rangle_{a_nb_n}}{\sqrt{2}};$$

$$\left|\Phi^{+}\right\rangle_{cd}=\frac{|00\rangle_{c_1d_1}+|11\rangle_{c_1d_1}}{\sqrt{2}}\otimes\frac{|00\rangle_{c_2d_2}+|11\rangle_{c_2d_2}}{\sqrt{2}}\otimes...\otimes\frac{|00\rangle_{c_nd_n}+|11\rangle_{c_nd_n}}{\sqrt{2}}.$$

Therefore, Alice measures the system e with the basis of $\{\left|\varepsilon'_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}\right\rangle_e\}$, so that the results of the measurement can be used to determine what unitary transformation $U^{+}_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}$ should be applied to the systems (b,d), i.e., the systems (a,b,c,d) can be transformed into the form $\left|\Phi^{+}\right\rangle_{ab}\left|\Phi^{+}\right\rangle_{cd}$. This successfully passes Bob's check.

The Problem of Preparing the Initial State

In order to prepare the initial state $|\psi\rangle_{abcde}$, first, we make system $\{|\varepsilon_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}\rangle_e\}$ by Deutsch-Jozsa algorithm. Then, the system e is further used as control-qubits to complete the preparation of the initial state $|\psi\rangle_{abcde}$.

The superposition state $|\varphi\rangle$ is achieved by the Deutsch-Jozsa algorithm taking all $r_1,r_4,r_3,r_5,C_{1n},C_{2n}$ that satisfy $r_1+r_4+C_{2n}=r_3+r_5+C_{1n}$:

$$|\varphi\rangle=\frac{1}{\sqrt{2^k}}\sum_{x\in\{0,1\}^k}|x\rangle\,|f\,(x)\rangle,$$

where:

$k=4n+2$, $x=r_1||r_4||r_3||r_5||C_{1n}||C_{2n}$;

$f(x)=y_1\vee y_2\vee...\vee y_n$, with $\vee$ is a logical disjunction operation. Assume $g(x)=r_1+r_4+C_{2n}-r_3-r_5-C_{1n}\triangleq y_1y_2...y_n$, with $y_1y_2...y_n$ is the binary expression of the output of the function $g(x)$.

When the measurement of $|f(x)\rangle$ is $|0\rangle$, the superposition state $\{|\varepsilon_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}\rangle_e\}$ of all solutions satisfying $r_1+r_4+C_{2n}=r_3+r_5+C_{1n}$ is obtained from $\{|x\rangle\}$.

However, the probability of getting $|0\rangle$ by measuring $|f(x)\rangle$ is $1/2^n$. It is clear that as n increases, the probability of successfully obtaining the system $\{|\varepsilon_{r_{1i},r_{4i},r_{3i},r_{5i},C_{1n},C_{2n}}\rangle_e\}$ (and hence the initial state $|\psi\rangle_{abcde}$) by Deutsch-Jozsa algorithm decreases exponentially with n, i.e., the probability of Alice's cheating success decreases exponentially with n.

This illustrates that the MLC attack strategy is not applicable to the proposed protocol. Note that MLC attacks on previous QBC protocols, such as BCJL [5], do not suffer from similar difficulties in preparing the initial state since solutions that satisfy the condition account for a non-negligible proportion of the total in the BCJL protocol.

Finally, we should mention that the new protocol is perfect with respect to noiseless quantum channels. Indeed, in quantum cryptography, the noise is of

central importance in revealing the activity of the adversary. In the presence of noise (noise in quantum communication channels, and of course errors generated by operations), the protocol has to be able to assess whether the error is generated by noise or by the attacker's cheating behavior. It is clear that provided the error rate of the quantum channels and operations is lower than a certain threshold, we can reduce the probability of success of Alice's cheating to an arbitrarily small value by increasing n in the proposed protocol. From Bob's point of view, the density matrices of the quantum pairs sent to him for commitment $x = 0$ and $x = 1$ are arbitrarily close to each other. On the other hand, if the error rate of the quantum channels and operations exceeds a certain threshold, then neither party can tell whether the error is caused by the channels and operations or by the other party's attempt to cheat. As with the BB84 protocol, a secure protocol cannot be executed under a poor noisy quantum channel.

5 Conclusion

In summary, we proposed a secure non-interactive bit commitment protocol where the *binding* of the protocol relies on the nonlocality effect of Bell states and the principle of quantum superposition states, and the *hiding* of the protocol relies on the no-communication theorem of the quantum entangled states and the quantum no-cloning theorem. Because QBC is a primitive of quantum cryptography, the proposed QBC protocol can be applied to construct more sophisticated secure quantum cryptography protocols, such as coin tossing, oblivious transfer, and two-party quantum computations, which are the foundation of quantum cryptographic protocols.

Acknowledgements

This work is supported by the National Natural Science Foundation of China (61872245), Shenzhen Science and Technology Program (JCYJ20180305123639326).

References

1. A. Aspect, P. Grangier, and G. Roger. Experimental realization of einstein-podolsky-rosen-bohm gedankenexperiment: a new violation of bell's inequalities. *Physical review letters*, 49(2):91, 1982.
2. 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.
3. C. H. Bennett, G. Brassard, and S. Breidbart. Quantum cryptography ii: How to re-use a one-time pad safely even if p = np. *Natural Computing*, 13(4):453–458, 2014.
4. M. Blum. Coin flipping by telephone. In *Proceedings of IEEE Compcon*, pages 133–137, 1982.

5. G. Brassard, C. Crépeau, R. Jozsa, and D. Langlois. A quantum bit commitment scheme provably unbreakable by both parties. In *Proceedings of 1993 IEEE 34th Annual Foundations of Computer Science*, pages 362–371, 1993.
6. 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.
7. A. Einstein, B. Podolsky, and N. Rosen. Can quantum-mechanical description of physical reality be considered complete? *Physical Review*, 47(10):777–780, 1935.
8. A. Furuta. One thing is certain: Heisenberg's uncertainty principle is not dead. *Scientific American*, 2012.
9. 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.
10. S. Goldwasser, S. Micali, and R. L. Rivest. A digital signature scheme secure against adaptive chosen-message attacks. *SIAM Journal on computing*, 17(2):281–308, 1988.
11. H. Halvorson. Generalization of the hughston-jozsa-wootters theorem to hyperfinite von neumann algebras. *Journal of Mathematical Physics*, 2003.
12. L. Hughston, R. Jozsa, and W. Wootters. A complete classification of quantum ensembles having a given density matrix. *Physics Letters A*, 183(1):14–18, 1993.
13. H. K. Lo and H. F. Chau. Is quantum bit commitment really possible? *Physical Review Letters*, 78:3410–3413, 1997.
14. 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.
15. D. Mayers. Unconditionally secure quantum bit commitment is impossible. *Physical Review Letters*, 78:3414–3417, 1997.
16. M. Ozawa. Universally valid reformulation of the heisenberg uncertainty principle on noise and disturbance in measurement. *Physical Review A*, 67(4):042105, 2003.
17. A. Peres and D. R. Terno. Quantum information and relativity theory. *Reviews of Modern Physics*, 76(1):93–123, 2004.
18. E. Schrödinger. Die gegenwärtige situation in der quantenmechanik. *Naturwissenschaften*, 23(49):823–828, 1935.
19. X. Sun, F. He, and Q. Wang. Impossibility of quantum bit commitment, a categorical perspective. *Axioms*, 9(1):28, 2020.
20. S. Wiesner. Conjugate coding. *ACM Sigact News*, 15(1):78–88, 1983.