Unconditionally Secure Relativistic Quantum Qubit Commitment

Houquan Liu 1,2,3,* and Libo Yuan 1,2

1 Photonics Research Center, Guilin University of Electronic Technology, Guilin 541004, China; lbyuan@guet.edu.cn
2 Guangxi Key Laboratory of Optoelectronic Information Processing, Guilin University of Electronics Technology, Guilin 541004, China
3 Guangxi Key Laboratory of Automatic Detecting Technology and Instrument, Guilin University of Electronics Technology, Guilin 541004, China
* Correspondence: houquanliu@163.com

Abstract: Quantum qubit commitment is a stronger version of the quantum bit commitment. It is impossible to realize unconditionally secure quantum qubit commitment in nonrelativistic domain. In this paper, we propose an unconditionally secure relativistic quantum qubit commitment protocol for the first time, which will have some unique applications in the upcoming era of quantum network.

Keywords: quantum qubit commitment; quantum cryptography

1. Introduction

Quantum bit commitment [1,2] is a cryptographic mistrustful task between two adversarial parties, in which, the committer Alice decides the value of the bit $b$ ($b = 0$ or $1$) that she wants to commit to the receiver Bob, and sends him some quantum encrypted information about the bit for evidence, e.g., some quantum states, in the commit phase. Later, in the unveil phase, Alice announces the correct value of $b$ as well as some information for decrypting the evidence, then Bob decrypts the evidence and checks whether the decryption output value of $b$ is consistent with Alice’s announcement. If a quantum bit commitment protocol is secure against both Bob and Alice, and its security does not rely on any computational assumption, it is said to be unconditionally secure. Secure quantum bit commitment is an essential cryptographic primitive in quantum cryptography. It could be used as a building block for protocols implementing a wide range of other cryptographic tasks [3–5]. However, within the framework of nonrelativistic quantum mechanics, unconditionally secure quantum bit commitment is impossible since the perfect securities against Alice and Bob are incompatible, which is known as Mayers–Lo–Chau (MLC) no-go theorem [6,7]. Though there are some doubts on the generality of the theoretical model of quantum bit commitment used in the no-go proof and, new protocols attempting to evade the no-go theorem were proposed every now and then, the result of MLC no-go theorem is widely accepted nowadays, which was introduced in detail in ref. [8]. It is considered as a serious drawback in quantum cryptography, as it tells us when the rapid development of quantum computers makes the computational assumptions underlying present day classical bit commitment become distinctly vulnerable, the quantum cryptography cannot offer any compensating solution [9]. Fortunately, it was proved later that by imposing causal restrictions via relativistic quantum mechanics, unconditionally secure quantum bit commitment is possible [10–13].

Recently, quantum qubit commitment, a stronger version of the quantum bit commitment, was introduced in Ref. [14]. It was found that the quantum qubit commitment has some unique applications [15] beyond quantum bit commitment in the upcoming era of quantum network, including implementing a fair version of quantum state exchange [16] and preventing cheating in such a task that two quantum computers are demanded to...
generate certain quantum states independently and to be cross-checked afterward [17], in which one computer may try to delay to generate its state after the other party and cheat by learning from the other party’s state or even try to imperfectly clone the state to pretend to have high computational power. It was also pointed out [15] that secure quantum qubit commitment can break asynchronous quantum network assumption since it can effectively activate multiple quantum machines at the same time. These unique applications motivate the wide range of interest of developing unconditional security quantum qubit commitment protocols. However, it is found that, similar to quantum bit commitment, it is impossible to realize unconditionally secure quantum qubit commitment in nonrelativistic domain [14]. Naturally, as a consequence, researchers attempt to develop security quantum qubit commitment schemes via adding some additional experimental constraints or causal restrictions of relativistic quantum mechanics. In Ref. [15], a secure quantum qubit commitment scheme is proposed by using the approach of quantum one-time tables, in which a trusted third party is needed. To the best of our knowledge, however, it remains an open question whether unconditionally secure quantum qubit commitment protocol can be realized in relativistic domain. Therefore, it is both theoretically interesting and practically valuable to develop unconditional security relativistic quantum qubit commitment protocols, which must be in line with and will promote the development of the upcoming era of quantum network [18]. Stimulated by this, in this paper we focus on and, for the first time, propose an unconditionally secure relativistic quantum qubit commitment scheme.

Before giving our protocol, we first explain some details of the concepts of quantum qubit commitment and unconditional security that we used throughout this paper. In quantum qubit commitment, instead of a bit, Alice commits to a qubit from a certain set (that can potentially also contain nonorthogonal quantum states), and later unveils to Bob that she has indeed committed to that qubit [14]. The qubit set should be open, since if the qubits are prepared by a third party and are unknown to Alice, she cannot unveil the quantum state of the committed qubit in the unveil phase. The fundamental difference between quantum qubit commitment and quantum bit commitment is that a quantum qubit commitment protocol preserves the coherence of the committed quantum state, therefore, to commit to a specific qubit in the commit phase, Alice should present quantum states (obtained via appropriate unitary transformations of the committed qubit) rather than the quantum-encrypted classical information of the qubit to Bob for evidence (if she presents the quantum-encrypted classical information for evidence, it is essentially a quantum bit string commitment).

In Ref. [15], the authors defined that a quantum qubit commitment scheme is unconditionally secure if, without any assumption on computational power, its output is indistinguishable from the output of an instance of the ideal functionality unless the probability of the committer passing the unveil phase is lower than a certain threshold which can be made arbitrarily small by increasing the security parameters. Here we give a more straightforward mathematical description as: a quantum qubit commitment scheme is unconditionally secure if it guarantees \( \sum_k p_k < 1 + \delta(N) \) with \( \delta(N) \to 0 \) as \( N \to \infty \), where \( N \) is the security parameter and \( p_k \) is the probability of successfully unveiling the \( k \)th qubit of the qubit set in the unveil phase. It should be noted that \( \delta(N) \) is the probability of successfully unveiling the \( k_1 \)th qubit when Alice committed to the \( k \)th qubit \( (k_1 \neq k) \) in the commit phase, which can be made arbitrarily small by choosing the security parameters appropriately but cannot be zero. \( \sum_k p_k < 1 + \delta(N) \) will reduce to be \( p_1 + p_2 < 1 + \delta \) when there are only two qubits in the qubit set, which is the unconditionally secure condition of quantum bit commitment.

2. Quantum Qubit Commitment Scheme

In this section, we show our protocol. The relativistic geometry of our protocol is chosen to be same as that of Ref. [10], i.e., Alice and Bob agree on a fixed inertial reference frame with coordinates \( (x, y, z, t) \), within which the space-time point \( O \) is the origin and two points \( Q_0 = (-x, 0, 0, x) \) and \( Q_1 = (x, 0, 0, x) \) are lightlike separated from \( O \) (see Figure 1).
Alice and Bob each have agents, separated in their own secure laboratories, adjacent to each of the points \( O, Q_0, \) and \( Q_1 \).

![Diagram](image_url)

**Figure 1.** A nonideal implementation of the protocol. (Not to scale.) Alice and Bob control disjoint regions of space-time, representing their respective secure laboratories. Bob generates random Bell states at \( O' \) and shares them (dashed arrow) to Alice at point \( O \). At point \( O \), Alice then teleports the committed qubit to Bob and transmits the teleportation measurement outcomes via secure light-speed channels (solid arrows) to her agents at the points \( Q_i \), who relay them (dotted arrows) to Bob’s agents at the nearby points \( Q'_i \).

Before the commitment, Alice and Bob agree on a security parameter \( N \), and a public fixed qubit set \( \{ |\psi_i\rangle \}_{i=1}^d \), where \( \{ |0\rangle_X, |1\rangle_X \} \) is an orthonormal basis in \( H_X \) space, \( a_k \) and \( \beta_k \) are complex weight factors, and \( d \) is the number of the qubits in the set. In our protocol, the qubit set is constrained by two restrictive conditions: (1) any two of the four qubits \( a|0\rangle_X + \beta|1\rangle_X \) and \( \beta|0\rangle_X + a|1\rangle_X \) cannot be selected as elements of the qubit set at the same time for arbitrary \( a \) and \( \beta \) parameters; (2) any two elements, \( |\psi_0\rangle_X = a_0|0\rangle_X + \beta_0|1\rangle_X \) and \( |\psi_1\rangle_X = a_1|0\rangle_X + \beta_1|1\rangle_X \), of the qubit set should satisfy \( x<\psi_1|\psi_0> < \psi_0|\psi_1> \ x < < 1 - \epsilon \), where \( \epsilon \) is the probability of the channel errors. Any set satisfying the above two restrictive conditions can be used as a qubit set of our protocol. The second restrictive condition is related to the non-ideal case that there exist channel errors. In the following, we first present our protocol in an idealized form and ignore the second restrictive condition. In the ideal case, we assume perfect state preparations, transmissions, and measurements. We also make idealizations about the relativistic geometry and signaling speed as Ref. [10], supposing that Alice can signal at precisely light speed, all information processing is instantaneous, and the distances from both parties’ labs to the relevant points \( O, Q_0, \) and \( Q_1 \) are infinitesimal and can be considered to be negligible.

**Commit:** In the commit phase, Bob prepares securely a set of qubits \( \{ |\Psi_i\rangle \}_{i=1}^N \) independently randomly chosen from Bell states and keeps them private.

\[
|\phi_1\rangle_{AB} = \frac{1}{\sqrt{2}}(-|0\rangle_A|0\rangle_B + |1\rangle_A|1\rangle_B), \quad |\phi_2\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|0\rangle_B - |1\rangle_A|1\rangle_B), \\
|\phi_3\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B), \quad |\phi_4\rangle_{AB} = \frac{1}{\sqrt{2}}(|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B),
\]

At point \( O \), Bob sends qubits \( B (|\_\rangle_B) \) to himself. To commit to a qubit \( a|0\rangle_X + \beta|1\rangle_X \) in \( H_X \) space, Alice carries out teleportation via measuring qubits \( X (|\_\rangle_X) \) and \( A \) collectively in the Bell basis resulting qubits \( B \) on Bob’s side collapse to \( a|0\rangle_B + \beta|1\rangle_B \) and \( \beta|0\rangle_B + a|1\rangle_B \) with equal probability, and sends over secure channels to her agents at \( Q_0 \) and \( Q_1 \) the outcomes of the collective measurement of qubits \( X \) and \( A \). In this stage, the collapsed states of qubits \( B \) act as the evidence of the commitment and preserve the coherence of the committed qubit; and the outcomes of the
Although such cheating does not increase Alice’s probability of successfully revealing any probabilities \( \alpha \) qubit and the outcomes of the collective measurement to adjacent Bob’s agents to unveil such as \( m \) the input qubit are equivalent. In the second scenario, we ask if it is possible for Alice to pretend that \( \alpha \) collapse to matter which of the four qubits Alice inputs, the output is that qubits B on Bob’s side correct qubit, it cannot be prohibited. However, from the perspective of the output, no such as qubit \( \alpha \) input qubit \( \alpha \) {\( |\alpha\rangle \) collective measurement of qubits X and A. For example, she can pretend that the input three remaining ones of the four qubits just by properly interchanging her results of the input qubit (committed qubit) from \( \alpha \) O first case is that Alice follows the honest strategy at point about Alice’s choice until she chooses to unveil the qubit.

A distant location can send information to Bob simply by measuring the qubits on her side, guaranteed by the theorem of impossibility of superluminal signaling. Since if Bob can Bob cannot get any information about the committed qubit by only measuring the qubits in Alice’s side does not change the reduced density matrix of the qubits in Bob’s side, so strategy that Bob prepares any kind of quantum state), any local measurement performed obviously secure against Bob. It is because no matter what strategy Bob takes (including the strategy that Bob prepares any kind of quantum state), any local measurement performed in Alice’s side does not change the reduced density matrix of the qubits in Bob’s side, so Bob cannot get any information about the committed qubit by only measuring the qubits in his side before the unveiling. From another perspective, the security against Bob is guaranteed by the theorem of impossibility of superluminal signaling. Since if Bob can learn something about the committed qubit before the unveiling, it means that an Alice in a distant location can send information to Bob simply by measuring the qubits on her side, which is essentially superluminal signaling. Hence, in our protocol, Bob can learn nothing about Alice’s choice until she chooses to unveil the qubit.

The security of this protocol against Alice should be discussed in different cases. The first case is that Alice follows the honest strategy at point O. In this case, she cannot change the collapsed states of qubits B again after O, but she is free to pretend that one original input qubit (committed qubit) from \( a|0\rangle_X + \beta|1\rangle_X \) and \( \beta|0\rangle_X \pm a|1\rangle_X \) is any one of the three remaining ones of the four qubits just by properly interchanging her results of the collective measurement of qubits X and A. For example, she can pretend that the input qubit \( a|0\rangle_X + \beta|1\rangle_X \) is \( a|0\rangle_X - \beta|1\rangle_X \) by interchanging her measurement results \(|\phi_1\rangle_{XA}\) with \(|\phi_2\rangle_{XA}\) and \(|\phi_3\rangle_{XA}\) with \(|\phi_4\rangle_{XA}\). However, because of the prior agreement that any two of the four qubits \( a|0\rangle_X \pm \beta|1\rangle_X \) and \( \beta|0\rangle_X \pm a|1\rangle_X \) cannot be selected as the elements of the qubit set \( \{|\psi_k\rangle_X\}_{k=1}^{d} \) at the same time, Alice’s cheating has no positive significance if qubit \( a|0\rangle_X + \beta|1\rangle_X \) is one of the element of the qubit set. The reverse case is that Alice’s input qubit \( a|0\rangle_X + \beta|1\rangle_X \) is not the element of the qubit set while she unveils the right one, such as qubit \( a|0\rangle_X - \beta|1\rangle_X \). From the perspective of the input, this is of course cheating. Although such cheating does not increase Alice’s probability of successfully revealing any correct qubit, it cannot be prohibited. However, from the perspective of the output, no matter which of the four qubits Alice inputs, the output is that qubits B on Bob’s side collapse to \( a|0\rangle_B \pm \beta|1\rangle_B \) and \( \beta|0\rangle_B \pm a|1\rangle_B \) with equal probability, implying the four inputs are equivalent. In the second scenario, we ask if it is possible for Alice to pretend that the input qubit \( a|0\rangle_X + \beta|1\rangle_X \) is another qubit with parameters different from a and \( \beta \), such as \( m|0\rangle_X + a|1\rangle_X \). If she tries to do this, she needs to pretend that the string of qubit \( |\phi_0\rangle_B = a|0\rangle_B + \beta|1\rangle_B \) within the collapsed qubits B is the string of \( |\phi_1\rangle_B = m|0\rangle_B + n|1\rangle_B \). The results of Ref. [19] show that once the density matrix of the qubit string is fixed, the probabilities \( p_i \) of Bob accepting a revelation of the string of \( |\phi_i\rangle_B \) satisfy \( p_0 + p_1 < 1 + \delta \).
where \( \delta \) can be made arbitrarily small by choosing the security parameters appropriately, therefore Alice has no successful strategy for such cheating.

Second, in the case that Alice does not follow the honest strategy at point \( O \), we can suppose that some operations are carried out at this point, but they leave her significantly uncommitted and retain as much freedom as possible in her choice of which qubit to unveil. We then further suppose that in the causal future of \( O \), all the strategies that the agent on the line segment \( (O, Q_0) \) can follow form a set \( \{ S_{qj} \} \), and the probabilities of successfully unveiling the qubit \( |\psi_k\rangle_X \) when the agent on the line segment \( (O, Q_0) \) performs the strategy \( S_{qj} \), while the other agent on the line segment \( (O, Q_1) \) performs \( S_{1j} \) is \( T_{qjk}(S_{qj}, S_{1j}, |\psi_k\rangle_X) \). Similar to the discussion in the case that Alice follows the honest strategy at point \( O \), by the results of Ref. [19] again, when the two agents follow \( S_{qj} \) and \( S_{1j} \) strategies, once the qubits B collapse to the states corresponding to the committed qubit \( |\psi_k\rangle_X \), there should exist no cheating strategy for Alice to successfully unveil any other qubit unless the probability of passing the unveil phase is lower than a certain threshold \( \delta \) which can be made arbitrarily small by increasing the security parameters, therefore the sum of the probabilities of successfully unveiling all the qubits of the public fixed qubit set except \( |\psi_k\rangle_X \) when the two agents follow \( S_{qj} \) and \( S_{1j} \) strategies must be less than \( 1 - T_{qjk} \), resulting in \( \sum T_{qjk} < 1 + \delta \). Moreover, by Minkowski causality, any operations carried out on the half-open line segment \( (O, Q_0) \) cannot affect the operations carried out on the half-open line segment \( (O, Q_1) \), and vice versa. The agent at \( Q_1 \) can only guess the strategy \( \hat{S}_{qj} \) that the agent at \( Q_0 \) follows with probability \( t_{qj} \) which must be agreed by the two agents at or before \( O \) or decided by the agent at \( Q_1 \) alone, hence satisfies \( \sum t_{qj} = 1 \). Therefore, the probability of successfully unveiling the qubit \( |\psi_k\rangle_X \) in the unveil phase is \( p_k = \sum_{qj} t_{qj} r_{qj} T_{qjk} \), where \( r_{qj} \) is the probability of the agent at \( Q_1 \) following \( S_{1j} \) when the agent at \( Q_0 \) follows \( S_{qj} \), which must satisfy \( \sum r_{qj} = 1 \). Combining the three conditions \( \sum T_{qjk} < 1 + \delta \), \( \sum t_{qj} = 1 \), and \( \sum r_{qj} = 1 \), we have \( \sum p_k = \sum_{qj} t_{qj} r_{qj} T_{qjk} < 1 + \delta \). This is consistent with our above mathematical definition of unconditionally secure of a quantum qubit commitment.

4. Discussion of Qubit Certification

Classical certification [20,21] is a well-known constraint that a quantum cryptographic protocol guarantees to all the other parties that one party is restricted so that, to avoid being detected as cheating, his quantum inputs must take the form of pure states of the basis elements of a public fixed basis \( \{|i\rangle \}_{i=1}^d \) of the appropriate \( d \)-dimensional input space. Here, as the qubit set \( \{|\psi_k\rangle_X\}_{k=1}^d \) in the quantum qubit commitment is not always a set of orthonormal bases in \( H_X \) space, we define qubit certification, a new constraint similar to classical certification, that a protocol guarantees to all the other parties that one party is restricted so that his quantum inputs must be a specific qubit of the public fixed set, which can be described as, in a quantum qubit commitment, that any unveiled qubit commitments necessarily have a definite committed qubit choosing from the public set. Like all technologically unconstrained quantum bit commitment protocols, [9,12] do not force Alice to commit to a specific bit, the protocol here does not force to commit to a specific qubit, as it does not prevent Alice from preparing states in \( H_X \) entangled with other system \( H_C \) with the form \( \sum_{k} \sqrt{p_k} |k\rangle_C |\psi_k\rangle_X \), where \( \{|k\rangle_C\}_{k=1}^d \) is a set of orthonormal bases. In the commitment, Alice can choose to keep the states in quantum entanglement, and input \( |\rangle_X \) as the committed qubit and store the entangled state \( |\rangle_C \) and then measure it in the computational basis until unveiling. In this case there is a definite committed qubit without being detected cheating, but from Alice’s perspective the unveiled qubit remains unknown with subjective probabilities obeying \( \sum p_k = 1 \). It does not rule out the case that Alice’s measurement result of qubit \( C \) is \( |k\rangle_C \) \( (k \neq k) \) but she successfully unveils qubit \( |\psi_k\rangle_X \), or even the case that she prepares states entangling the subset \( \{|\psi_k\rangle_X\}_{k=1}^{d_1} \) of \( \{|\psi_k\rangle_X\}_{k=1}^d \) \( (d_1 < d) \) with \( \{|k\rangle_C\}_{k=1}^{d_1} \), i.e., \( \sum_{k=1}^{d_1} \sqrt{p_k} |k\rangle_C |\psi_k\rangle_X \) satisfying \( \sum p_k = 1 \), but successfully unveils a qubit \( |\psi_k\rangle_X \notin \{|\psi_k\rangle_X\}_{k=1}^{d_1} \) with a probability \( \delta \), which can be made
arbirtarily small by choosing the security parameters appropriately as there is no any measurement result that could act as an evidence to support Alice to obtain a successful probability of unveiling this qubit higher than the successful probability of just guessing by chance. Hence, we say a quantum qubit commitment protocol with a security parameter $N$ is unconditionally secure when it guarantees $\sum_k p_k < 1 + \delta(N)$ with $\delta(N) \to 0$ as $N \to \infty$. It is the complete mathematical definition of unconditionally secure of a quantum qubit commitment that we presented above.

5. The Non-Ideal Case in Practical Application

The protocol proposed above is idealized with some ideal assumptions. In this section, we discuss the non-ideal case in practical application. Realistically, it is not possible for Alice and Bob to have secure access to precisely the same space–time point to exchange a qubit; Alice cannot signal at precisely light speed; and information cannot be processed instantaneously. In a realistic implementation, all the corrections about the idealized assumptions of these aspects will introduce time delays at various stages of the protocol. The effects of these time delays can be discussed same as the other relativistic protocols [9,12]. If the corrections are small, the protocol remains secure and the only significant effect is that Alice can only persuade Bob that her commitment is binding from some point in the near causal future of $O$, rather than from $O$ itself [9,12].

Realistically, too, perfect state preparations, transmissions, and measurements are impossible with unavoidable channel losses and errors. A low possibility of losses does not affect the security since the security parameter $N$ of the protocol implies essentially committing $N$ copies of the qubit, hence Bob can always be able to receive enough evidence qubits to finally check Alice’s unveiling. To deal with the channel errors, we consider that the two qubits $|\psi_0\rangle_X = a_0|0\rangle_X + b_0|1\rangle_X$ and $|\psi_1\rangle_X = a_1|0\rangle_X + b_1|1\rangle_X$ are two arbitrary elements of the public qubit set $\{|\psi_l\rangle_X \}_{l=1}^d$. If Alice attempts to cheat to pretend that the committed qubit $|\psi_0\rangle_X$ is $|\psi_1\rangle_X$ in a concrete implementation, she needs to persuade Bob that the strings of $|\psi_0\rangle_B = a_0|0\rangle_B \pm b_0|1\rangle_B$ and $b_0|0\rangle_B \pm a_0|1\rangle_B$ within the collapsed qubits B are the strings of $|\psi_1\rangle_B = a_1|0\rangle_B \pm b_1|1\rangle_B$ and $b_1|0\rangle_B \pm a_1|1\rangle_B$, respectively. Let $p_I^1_B = <\psi_1|\psi_0>_B <\psi_0|\psi_1>_B$ be the probability of Bob accepting a revelation of $|\psi_1\rangle_B$ for the $i$th $|\psi_0\rangle_B$. We have $p_I^1 = |a_0^*a_1 + b_0^*b_1|^2$, and the probability that Alice is detected cheating in unveiling $|\psi_1\rangle_B$ is $1 - p_I^1$. If the probability of the channel errors $\epsilon$ is bigger than $1 - p_I^1$, Alice can always claim that the error was due to channel errors, even if she did cheat. Therefore, Bob can be guaranteed that Alice’s commitment is binding only when $1 - p_I^1 >> \epsilon$. Since it can be found that $p_I^1 = \chi <\psi_1|\psi_0>_X \chi <\psi_0|\psi_1>_X$ in our protocol, it finally becomes $\chi <\psi_1|\psi_0>_X \chi <\psi_0|\psi_1>_X << 1 - \epsilon$, which gives, to counter the channel errors, a definite constraint in determining the qubit set. When this constraint condition is satisfied, the channel errors make no essential difference as long as they are small and Bob needs only to check that Alice’s revelation is statistically consistent with the output corresponding to the unveiled qubit and statistically inconsistent with the other. In practical application, we think that $1 - \chi <\psi_1|\psi_0>_X \chi <\psi_0|\psi_1>_X \geq 2\epsilon$ is good enough to implement our protocol. To illustrate this constraint more visually, we suppose that $|\psi_0\rangle_X = |0\rangle_X$ and $|\psi_1\rangle_X = \cos\theta|0\rangle_X + \sin\theta|1\rangle_X$ are two qubits in the qubit set and $\epsilon = 3\%$ in a practical application, hence we have $\chi <\psi_1|\psi_0>_X \chi <\psi_0|\psi_1>_X = \cos\theta$. In this case, the constraint $1 - \chi <\psi_1|\psi_0>_X \chi <\psi_0|\psi_1>_X \geq 2\epsilon$ requires $\cos^2\theta \leq 94\%$, i.e., the angle $\theta$ is not smaller than $\arccos(\sqrt{0.94}) = 14.1788^\circ$.

6. Conclusions and Discussion

Quantum qubit commitment is a rather new concept, which was first proposed in 2018 [14]. It was pointed out in 2021 [15] that the quantum qubit commitment has some unique and important applications beyond quantum bit commitment in the upcoming era of quantum network. Therefore, it is both theoretically interesting and practically valuable to develop unconditional secure quantum qubit commitment protocols. In this paper, we
proposed an unconditionally secure relativistic quantum qubit commitment protocol for the first time. Comparing to the existed quantum bit commitment, our protocol does not destroy the coherence of the committed qubit (the collapsed states of qubits B preserve the coherence of the committed qubit). This is the fundamental difference between quantum qubit commitment and quantum bit commitment.

Since quantum qubit commitment is a stronger version of the quantum bit commitment, our quantum qubit commitment protocol of course can be used to fulfill quantum bit commitment. However, to preserve the coherence of the committed qubit, when our protocol is used to execute a quantum bit commitment, it needs more quantum resources (quantum entanglement in our protocol) than the dedicated quantum bit commitment protocols [9,10,12]. This is the limitation of our protocol.

In the last two decades, relativistic quantum cryptography has become an important branch of quantum physics. Numerous researchers have carried out a great deal of research in this field, including revealing information causality as a physical principle in quantum physics [22] as well as developing relativistic quantum protocols with wide range of important applications, such as quantum tokens [23] and quantum tagging [24]. As our proposed protocol is the first unconditionally secure relativistic quantum qubit commitment scheme, we think that it comes timely in the rapid development of relativistic quantum cryptography and will help stimulate further interest in the theory and practical implementation of this field.

Author Contributions: Conceptualization, H.L. and L.Y.; funding acquisition, H.L. and L.Y.; investigation, H.L.; writing—original draft, H.L.; writing—review and editing, H.L. and L.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by the National Key Research and Development Program of China (Grant No. 2019YFB2203903), the National Natural Science Foundations of China (Grant No. 62065006), the Natural Science Foundation of Guangxi (Grants No. 2019GXNSFAA245024 and No. 2020GXNSFBA159059), the Science and Technology Project of Guangxi (Grant No. AD19245064), Guangxi Key Laboratory Project of Optoelectronic Information Processing (Grant No. GD20103), and Guangxi Key Laboratory Project of Automatic Detection Technology and Instrument (Grant No. YQ20103).

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References
1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9–12 December 1984; IEEE: New York, NY, USA, 1984; pp. 175–179.
2. Brassard, G.; Crépeau, C.; Jozsa, R.; Langlois, D. A quantum bit commitment scheme provably unbreakable by both parties. In Proceedings of the IEEE 34th Annual Foundations of Computer Science, Palo Alto, CA, USA, 3–5 November 1993; pp. 362–371.
3. Bennett, C.H.; Brassard, G.; Crépeau, C.; Skubiszewska, M.-H. Practical Quantum Oblivious Transfer. In CRYPTO ’91: Proceedings of the 11th Annual International Cryptology Conference on Advances in Cryptology; Springer: Berlin/Heidelberg, Germany, 1992; pp. 351–366.
4. Kent, A. Location-oblivious data transfer with flying entangled qudits. Phys. Rev. A 2011, 84, 012328. [CrossRef]
5. Molina-Terriza, G.; Vaziri, A.; Ursin, R.; Zeilinger, A. Experimental Quantum Coin Tossing. Phys. Rev. Lett. 2005, 94, 040501. [CrossRef] [PubMed]
6. Lo, H.-K.; Chau, H.F. Is Quantum Bit Commitment Really Possible? Phys. Rev. Lett. 1997, 78, 3410–3413. [CrossRef]
7. Mayers, D. Unconditionally Secure Quantum Bit Commitment is Impossible. Phys. Rev. Lett. 1997, 78, 3414–3417. [CrossRef]
8. He, G.P. Quantum key distribution based on orthogonal states allows secure quantum bit commitment. J. Phys. A Math. Theor. 2011, 44, 445305. [CrossRef]
9. Kent, A. Unconditionally Secure Bit Commitment. Phys. Rev. Lett. 1999, 83, 1447–1450. [CrossRef]
10. Kent, A. Unconditionally Secure Bit Commitment by Transmitting Measurement Outcomes. Phys. Rev. Lett. 2012, 109, 130501. [CrossRef] [PubMed]
11. Liu, Y.; Cao, Y.; Curty, M.; Liao, S.-K.; Wang, J.; Cui, K.; Li, Y.-H.; Lin, Z.-H.; Sun, Q.-C.; Li, D.-D.; et al. Experimental Unconditionally Secure Bit Commitment. *Phys. Rev. Lett.* 2014, 112, 010504. [CrossRef] [PubMed]
12. Kent, A. Unconditionally secure bit commitment with flying qudits. *New J. Phys.* 2011, 13, 113015. [CrossRef]
13. Lunghi, T.; Kaniewski, J.; Bussieres, F.; Houllmann, R.; Tomamichel, M.; Kent, A.; Gisin, N.; Wehner, S.; Zbinden, H. Experimental bit commitment based on quantum communication and special relativity. *Phys. Rev. Lett.* 2013, 111, 180504. [CrossRef] [PubMed]
14. Modi, K.; Pati, A.K.; Sen, A.; Sen, U. Masking Quantum Information is Impossible. *Phys. Rev. Lett.* 2018, 120, 230501. [CrossRef] [PubMed]
15. Lie, S.H.; Kwon, H.; Kim, M.S.; Jeong, H. Quantum one-time tables for unconditionally secure qubit-commitment. *Quantum* 2021, 5, 405. [CrossRef]
16. Lee, Y.; Takagi, R.; Yamasaki, H.; Adesso, G.; Lee, S. State Exchange with Quantum Side Information. *Phys. Rev. Lett.* 2019, 122, 010502. [CrossRef]
17. Elben, A.; Vermersch, B.; van Bijnen, R.; Kokail, C.; Brydges, T.; Maier, C.; Joshi, M.K.; Blatt, R.; Roos, C.F.; Zoller, P. Cross-Platform Verification of Intermediate Scale Quantum Devices. *Phys. Rev. Lett.* 2020, 124, 010504. [CrossRef]
18. Kimble, H.J. The quantum internet. *Nature* 2008, 453, 1023–1030. [CrossRef]
19. Kent, A. Quantum Bit String Commitment. *Phys. Rev. Lett.* 2003, 90, 237901. [CrossRef]
20. Kent, A. Impossibility of unconditionally secure commitment of a certified classical bit. *Phys. Rev. A* 2000, 61, 042301. [CrossRef]
21. Kent, A. Why classical certification is impossible in a quantum world. *Quantum Inf. Process.* 2011, 11, 493–499. [CrossRef]
22. Pawłowski, M.; Paterek, T.; Kaszlikowski, D.; Scarani, V.; Winter, A.; Żukowski, M. Information causality as a physical principle. *Nature* 2009, 461, 1101. [CrossRef]
23. Kent, A.; Pitalúa-García, D. Flexible quantum tokens in spacetime. *Phys. Rev. A* 2020, 101, 022309. [CrossRef]
24. Kent, A. Quantum tagging for tags containing secret classical data. *Phys. Rev. A* 2011, 84, 022335. [CrossRef]