Article

An Optical Implementation of Quantum Bit Commitment Using Infinite-Dimensional Systems

Guang Ping He

Special Issue

Recent Development and Application of Quantum Communication and Security Protocols, Volume II

Article

An Optical Implementation of Quantum Bit Commitment Using Infinite-Dimensional Systems

Guang Ping He

School of Physics, Sun Yat-sen University, Guangzhou 510275, China; hegp@mail.sysu.edu.cn

Abstract: Unconditionally secure quantum bit commitment (QBC) was widely believed to be impossible for more than two decades, but recently, based on an anomalous behavior found in quantum steering, we proposed a QBC protocol which can be unconditionally secure in principle. The protocol requires the use of infinite-dimensional systems, so it may seem less feasible in practice. Here, we propose a quantum optical method based on the Mach–Zehnder interferometer, which gives a very good approximation to such infinite-dimensional systems. Thus, it enables a proof-of-principle experimental implementation of our protocol, which can also serve as a practically secure QBC scheme. Other multi-party cryptographic protocols such as quantum coin tossing can be built upon it too. Our approach also reveals a relationship between infinity and non-locality, which may have an impact on the research of fundamental theories.

Keywords: secure multi-party computation; bit commitment; coin tossing; Mach–Zehnder interferometer; quantum steering

1. Introduction

Quantum cryptography has achieved great success in many fields such as key distribution [1], but there are still other cryptographic problems that remain unconquered. Bit commitment (BC) [2] is known to be an essential building block for coin tossing [1], oblivious transfer [3,4], and even more complicated multi-party secure computation protocols [5]. Unfortunately, since 1996, people started to realize that unconditionally secure quantum BC (QBC) is hard to achieve. The cheating strategy against the QBC protocol in ref. [2] was first proposed in ref. [6]. Shortly after, it was further asserted that all QBC protocols are not unconditionally secure in principle [7,8]. Later, refs. [9–14] reviewed the original no-go proof, with some examples of insecure protocols given in refs. [9,13]. Ref. [11] also extended the proof to cover ideal quantum coin tossing (QCT). More examples on how to break some promising BC protocols at that time were provided too [15,16]. Refs. [17–20] proved the impossibility of some types of BC with a slightly different security criterion. Refs. [21–25] gave quantitative studies on the security bounds of QBC, with ref. [22] focused on the protocol in ref. [1], while refs. [23,24] focused on another class of protocols. A very lengthy proof was first presented in the Heisenberg picture [26], then shortened and rephrased in the Schrödinger picture [27]. The validity of the no-go result was also studied in a world subject to superselection rules [28–30] or an epistemic local hidden variable theory [31]; for QBC associated with secret parameters [32,33] or secret probability distributions [34]; or when the participants are restricted to use Gaussian states and operations only [35]. Refs. [36,37] attempted to deduce the impossibility of QBC from the no-masking theorem. Ref. [38] studied the security of BC under the relativistic setting. Other efforts include refs. [39–44], which tried to proved the no-go theorem with alternative approaches. These results, known as the Mayers–Lo–Chau (MLC) no-go theorem, were widely accepted despitesome attempts towards secure QBC (e.g., the references in refs. [45–51]), and were considered as a serious drawback on the potential of quantum cryptography.

Nevertheless, the cheating strategy in all these no-go proofs is based on the Hughston–Jozsa–Wootters (HJW) theorem [52], a.k.a. the Uhlmann theorem [53,54]. Recently, it was found that, in infinite-dimensional systems, there exists a specific form of quantum states to which the HJW theorem does not apply [55]. Based on this finding, we proposed a QBC protocol and proved theoretically that it remains secure against the cheating strategy in the no-go proofs [56]. Therefore, implementing the protocol in practice will be of great significance, as it can re-open the venue to many useful multi-party secure computation protocols that were once closed by the MLC no-go theorem.

As pointed out in ref. [56], since the protocol requires infinite-dimensional systems, the implementation may be very hard if we want to use physical systems with an infinite number of energy levels, because it may imply an infinitely high energy. To circumvent the problem, here, we use the arrival time of photons as a trick, so that infinite-dimensional systems can be realized using simple optical devices. Consequently, the QBC protocol in ref. [56] can be implemented with a Mach–Zehnder (MZ) interferometer, which is within the capability of currently available technology.

2. Results

2.1. The Theoretical Description of the Protocol

Let us begin with a brief review on the definition of BC and the theoretical scheme in ref. [56]. BC is a two-party cryptography between Alice and Bob, which includes the following phases. In the commit phase, Alice decides the value of the bit b that she wants to commit and sends Bob a piece of evidence, e.g., some quantum states. Later, in the unveil phase, Alice announces the value of b, and Bob checks it with the evidence. The interval between the commit and unveil phases can be called the holding phase. An unconditionally secure BC protocol needs to be both binding (i.e., Alice cannot change the value of b after the commit phase) and concealing (Bob cannot know b before the unveil phase).

Since whether QBC can be unconditionally secure in principle is a very important theoretical problem, here, we only consider the ideal case without transmission errors, detection loss, dark counts, or other practical imperfections. In ref. [56], the following protocol was proposed:

Our theoretical QBC protocol:

The commit phase:

(i) Alice decides on the value of b ($b = 0$ or 1) that she wants to commit. Then, for $j = 1$ to s: She randomly picks an integer $i_j \in \{1, 2, \ldots, \infty\}$ and sends Bob a quantum register Ψ_j, which is an infinite-dimensional system prepared in the state $\psi_{i_j}^b = (|0\rangle + (-1)^b |i_j\rangle)/\sqrt{2}$.

That is, if $b = 0$ she randomly picks a state from the set:

$$\left\{ \psi_i^0 \equiv |\phi_{i+}\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |i\rangle), i = 1, \ldots, n-1 \right\}, \tag{1}$$

or, if $b = 1$, she randomly picks a state from the set:

$$\left\{ \psi_i^1 \equiv |\phi_{i-}\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |i\rangle), i = 1, \ldots, n-1 \right\}, \tag{2}$$

where $|0\rangle, |1\rangle, |2\rangle, \ldots, |i\rangle, \ldots$ are orthogonal to each other and $n \to \infty$.

Note that, in each round, i_j is independently chosen, while b remains the same for all j;

The holding phase:

(ii) Bob stores these s quantum registers unmeasuredly;

The unveil phase:

(iii) Alice announces the values of b and all i_j ($j = 1, \ldots, s$);

(iv) Bob tries to project each Ψ_j into the state $\psi_{i_j}^b = (|0\rangle + (-1)^b |i_j\rangle)/\sqrt{2}$. If the projections are successful for all registers, Bob accepts Alice's commitment. Else, if any of the projections fails, Bob concludes that Alice cheated.

The key reason that this protocol can be unconditionally secure is the specific forms of the states in Equations (1) and (2). In general, the cheating strategy in the no-go proofs [6–44] can be successful in most QBC protocols using other forms of quantum states for the following reason. Suppose that honest Alice is supposed to send Bob the state ψ'^0 (ψ'^1) if she wants to commit $b = 0$ ($b = 1$), where ψ'^0 (ψ'^1) is picked from a set of states described by the density matrix ρ_0^β (ρ_1^β). Since an unconditionally secure QBC protocol needs to be concealing against dishonest Bob, there should be the following:

$$\rho_0^\beta \simeq \rho_1^\beta \qquad (3)$$

so that Bob cannot discriminate the state himself. Then, the HJW theorem applies. That is, dishonest Alice can begin the QBC protocol by preparing the system $\alpha \otimes \beta$ in such a state that β alone has density matrix ρ_0^β. Then, she skips the measurement in the commit phase so that α and β remain entangled. In the unveil phase, since Equation (3) is satisfied, according to the HJW theorem, there exist two measurements M_0 and M_1 on α such that, if Alice applies M_0 (M_1) on α, then β will collapse to a state belonging to the set described by ρ_0^β (ρ_1^β). Therefore, Alice can unveil b as whatever value she likes in the unveil phase by choosing between the two measurements M_0 and M_1.

However, in our protocol, the two sets of states take the forms in Equations (1) and (2). Suppose that dishonest Alice prepares a bipartite system $\alpha \otimes \beta$ in the state:

$$|\Omega\rangle = \frac{1}{\sqrt{n-1}} \sum_{i=1}^{n-1} |\alpha_{i+}\rangle |\phi_{i+}\rangle \qquad (4)$$

so that she can cheat using the strategy in the no-go proofs. Here, $\{|\alpha_{i+}\rangle, i = 0, \ldots, n-1\}$ is an orthonormal basis of the n-dimensional system α. Let ρ_0^β and ρ_1^β be the density matrices corresponding to the sets $\{\psi_i^0 = |\phi_{i+}\rangle\}$ and $\{\psi_i^1 = |\phi_{i-}\rangle\}$, respectively. As shown in ref. [55], when $n \to \infty$, Equation (3) is satisfied, so that it seems to meet the requirement of the HJW theorem. Now, let us see what happens if Alice wants to cheat.

Surely, if she wants to unveil $b = 0$, all she needs is simply to use $\{|\alpha_{1+}\rangle, |\alpha_{2+}\rangle, \ldots, |\alpha_{(n-1)+}\rangle\}$ as the basis of the measurement M_0 and apply it on her system α, which will make Bob's system β collapse into one of the state in $\{|\phi_{i+}\rangle\}$ so that she can complete the protocol without being caught. Now, the question is, can she unveil $b = 1$ successfully? According to the HJW theorem, there should exist another measurement M_1 with the basis $\{|\alpha_{1-}\rangle, |\alpha_{2-}\rangle, \ldots, |\alpha_{(n-1)-}\rangle\}$, such that Equation (4) can be expressed as follows:

$$|\Omega\rangle \simeq \frac{1}{\sqrt{n-1}} \sum_{i=1}^{n-1} |\alpha_{i-}\rangle |\phi_{i-}\rangle \qquad (5)$$

so that Alice's measuring α, in this basis, will make β collapse into a state in $\{|\phi_{i-}\rangle\}$. To find the form of $\{|\alpha_{i-}\rangle\}$, following ref. [56], we expand each $|\phi_{i+}\rangle$ in Equation (4) using $\{|\phi_{i-}\rangle\}$, and the result is below:

$$\begin{aligned} |\Omega\rangle &= \frac{1}{\sqrt{n-1}} \sum_{i=1}^{n-1} \sqrt{1 - \frac{4}{n^2}} |\tilde{\alpha}_{i-}\rangle |\phi_{i-}\rangle \\ &+ \sqrt{\frac{2}{n}} |\tilde{\alpha}_{n-}\rangle |\phi_{n-}\rangle, \end{aligned} \qquad (6)$$

where

$$|\phi_{n-}\rangle \equiv \frac{1}{\sqrt{n}} \left(|0\rangle + \sum_{i=1}^{n-1} |i\rangle \right), \qquad (7)$$

$$|\tilde{\alpha}_{n-}\rangle \equiv \frac{1}{\sqrt{n-1}} \sum_{i=1}^{n-1} |\alpha_{i+}\rangle, \qquad (8)$$

and

$$|\tilde{\alpha}_{i-}\rangle \equiv \frac{1}{\sqrt{1 - \frac{4}{n^2}}} \left(\frac{2-n}{n}|\alpha_{i+}\rangle + \frac{2}{n} \sum_{i'=1, i' \neq i}^{n-1} |\alpha_{i'+}\rangle \right), \tag{9}$$

for $i = 1, \ldots, n - 1$.

For a given $i \in \{1, \ldots, n-1\}$, if Alice can project system α to $|\tilde{\alpha}_{i-}\rangle$, then Equation (6) shows that system β will collapse to the following:

$$
\begin{aligned}
|\tilde{\phi}_{i-}\rangle &\equiv c' \left[\frac{\sqrt{1 - \frac{4}{n^2}}}{\sqrt{n-1}} \left(|\phi_{i-}\rangle + \sum_{i'=1, i' \neq i}^{n-1} \langle \tilde{\alpha}_{i-}|\tilde{\alpha}_{i'-}\rangle |\phi_{i'-}\rangle \right) \right. \\
&\quad \left. + \sqrt{\frac{2}{n}} \langle \tilde{\alpha}_{i-}|\tilde{\alpha}_{n-}\rangle |\phi_{n-}\rangle \right] \\
&= c' \left[\sqrt{\frac{n^2-4}{n^2(n-1)}} \left(|\phi_{i-}\rangle - \frac{4\sum_{i'=1, i' \neq i}^{n-1} |\phi_{i'-}\rangle}{n^2-4} \right) \right. \\
&\quad \left. + \sqrt{\frac{2(n-2)}{n(n-1)(n+2)}} |\phi_{n-}\rangle \right], \tag{10}
\end{aligned}
$$

where

$$c' = \sqrt{\frac{n(n-1)(n+2)}{(n^2+2)}}. \tag{11}$$

Multiplying $\langle \phi_{i-}|$ by Equation (10), we have the following:

$$\langle \phi_{i-}|\tilde{\phi}_{i-}\rangle = \sqrt{1 - \frac{2n+2}{n^2+2}}. \tag{12}$$

In the limit $n \to \infty$, $|\tilde{\phi}_{i-}\rangle$ can be arbitrarily close to $|\phi_{i-}\rangle$. Thus, we know that $|\tilde{\alpha}_{i-}\rangle$ is the form of $\{|\alpha_{i-}\rangle\}$ that we are looking for.

Nevertheless, by taking the limit $n \to \infty$ in Equation (9), we find the following:

$$|\tilde{\alpha}_{i-}\rangle = -|\alpha_{i+}\rangle. \tag{13}$$

Consequently, if Alice wants to collapse β into a state in $\{|\phi_{i-}\rangle\}$ so that she can unveil $b = 1$ successfully, then the corresponding measurement M_1 is to measure α in the basis $\{-|\alpha_{1+}\rangle, -|\alpha_{2+}\rangle, \ldots, -|\alpha_{(n-1)+}\rangle\}$. Since the global negative sign before the state vectors has no physical meaning, the bases of the "two" measurements M_0 and M_1 are actually the same. Consequently, Alice no longer has the freedom to choose between two different measurements to alter the value of her committed bit b. Thus, the cheating strategy in the no-go proofs fails in our protocol. (Please see ref. [56] for the complete security proof.)

2.2. The Experimental Implementation

Ref. [56] was devoted to the problem of whether unconditionally secure QBC is allowed in principle. Thus, it only provided a theoretical description of the protocol without considering the implementation. To realize the protocol, the most important point is to find a feasible implementation of the infinite-dimensional systems. Here, we propose a trick to implement the infinite-dimensional system in each round of the protocol using a single photon only. The experimental apparatus is illustrated in Figure 1. In each of the s rounds of step (i) of the protocol, Alice sends a single photon either from the source S_0 (for sending ψ_i^0) or S_1 (for sending ψ_i^1), then splits it into two wave packets $|x\rangle$ and $|y\rangle$ by the 50:50 non-polarizing beam splitter BS_A. $|x\rangle$ is sent directly to Bob via path X while $|y\rangle$ is delayed by the storage ring SR_A (which introduces a delay time τ chosen by Alice secretly) before sending via path Y. At Bob's site, $|x\rangle$ is delayed by the storage rings SR_x and SR_B.

$|y\rangle$ is delayed by the storage ring SR_y, which is identical to SR_x, so that they introduce the same amount of delay time, then meets $|x\rangle$ at the 50:50 beam splitter BS_B and interferes. We can see that when the delay times caused by SR_A and SR_B are tuned to be equal, the complete apparatus forms a balanced MZ interferometer, so that ψ_i^0 (ψ_i^1) will make the detector D_0 (D_1) click with certainty in principle.
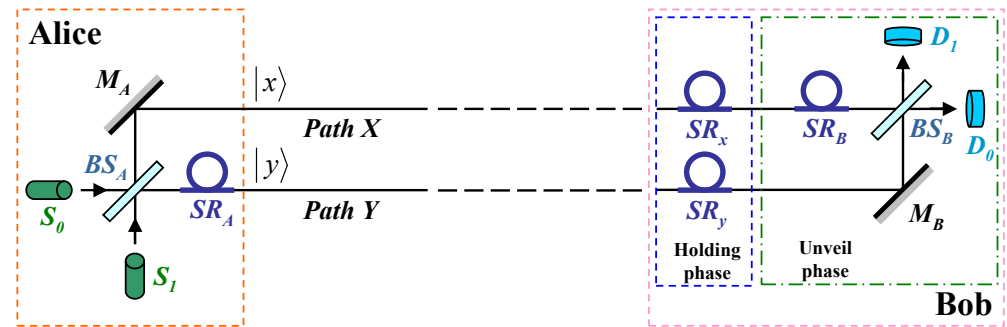

Figure 1. Diagram of the experimental apparatus of our QBC protocol. Alice sends photons from the single-photon source S_0 (S_1) when she wants to commit $b = 0$ ($b = 1$). Both BS_A and BS_B are 50:50 non-polarizing beam splitters, and M_A, M_B are mirrors. SR_A, SR_B, SR_x, and SR_y are storage rings. The photons are finally detected by the detectors D_0 and D_1.

Before running the protocol, Bob should set up another set of devices at his own site as a reference, which is completely identical to that of Alice's. By sending photons using this reference set and monitoring his detectors D_0 and D_1, he can estimate the error rate ε of the whole system, i.e., the probability that the photon ψ_i^0 (ψ_i^1) sent from the source S_0 (S_1) will mistakenly make the detector D_1 (D_0) click or simply get lost. For better performance, if the distance between Alice and Bob is very long, paths X and Y in Figure 1 should be implemented using optical fibers, instead of letting the photons travel through free space. Meanwhile, Bob should also have optical fibers of the same length in his reference set and place them in an environment (e.g., temperature, humidity, etc.) similar to that of the optical fibers placed between Alice and Bob in the actual set. The purpose is to ensure that the error rate ε that Bob learns from his reference set is very close to the one in the actual set. After obtaining ε all by himself, Bob runs the following experimental protocol with Alice.

Our experimental QBC protocol:

The commit phase:

(i) *Alice and Bob agree on a maximum delay time $\tau_{\max}$ and the sending times t_j ($j = 1, \ldots, s$) with $t_1 < t_2 < \cdots < t_s$ and $\tau_{\max} < t_j - t_{j-1}$ ($j = 2, \ldots, s$). Then, Alice decides on the value of b ($b = 0$ or 1) that she wants to commit, and for $j = 1$ to s:*

Alice randomly picks $\tau_j \in [0, \tau_{\max}]$ and sets the delay time of her storing ring SR_A as τ_j. Then, she sends Bob a photon Ψ_j from the source S_b at time t_j;

Note that, in each round, τ_j is independently chosen, while b remains the same for all j;

The holding phase:

(ii) *Bob stores the wave packets of each photon in SR_x and SR_y unmeasuredly;*

The unveil phase:

(iii) *Alice announces the values of b and all τ_j ($j = 1, \ldots, s$);*

(iv) *For $j = 1$ to s: Bob sets the delay time of his storing ring SR_B as τ_j. Then, he releases the wave packets of photon Ψ_j from SR_x and SR_y and directs them into his part of the MZ interferometer (as presented in the green dash-dot box at the right-hand side of Figure 1);*

If there are, in total, about $(1 - \varepsilon)s$ photons (see Appendix A for the tolerable range of statistical deviations) detected by D_b instead of $D_{\bar{b}}$, then Bob accepts Alice's commitment. Otherwise, Bob concludes that Alice cheated.

2.3. The Relationship between the Two Protocols

Now, we show that, in principle, the above experimental protocol is a faithful implementation of the theoretical one. In the experimental protocol, following the occupation number representation widely used in quantum optics [57], at time t if there is a wave packet of a photon on path X and no wave packet on path Y, the state can be denoted by $|1\rangle_X|0\rangle_Y$. Conversely, if there is a wave packet on path Y and no wave packet on path X, the state can be denoted by $|0\rangle_X|1\rangle_Y$. To make the time t more explicit, let us write them as $|t\rangle_X|0\rangle_Y$ and $|0\rangle_X|t\rangle_Y$, respectively. That is, we use the symbol t in $|\ldots\rangle$ to denote the time that the wave packet of a single photon presents in the path, instead of the number of photons, and $|0\rangle$ to denote that no wave packet is presented in the path at any time. Obviously, the state $|t\rangle_P$ is orthogonal to $|t'\rangle_P$ ($P = X, Y$) for any $t \neq t'$ and they are all orthogonal to $|0\rangle_P$. For simplicity, suppose that, except for SR_A, SR_B, SR_x, and SR_y, the time for the photon to travel through all other devices in Figure 1 is negligible. Under this formalism, when Alice sends the photon Ψ_j ($j = 1, \ldots, s$) from the source S_b at time t_j, the initial state of Ψ_j after passing BS_A is as shown:

$$|\Psi_j\rangle_{ini} = \frac{1}{\sqrt{2}}(|t_j\rangle_X|0\rangle_Y + (-1)^b|0\rangle_X|t_j\rangle_Y). \tag{14}$$

After passing SR_A, which introduces the delay time τ_j to path Y, the state of Ψ_j that left Alice's site is as below:

$$|\psi_j\rangle_A = \frac{1}{\sqrt{2}}(|t_j\rangle_X|0\rangle_Y + (-1)^b|0\rangle_X|t_j + \tau_j\rangle_Y). \tag{15}$$

In the unveil phase, when Bob learns Alice's delay time τ_j and sets SR_B accordingly, the final state of the photon Ψ_j arriving at BS_B after passing SR_x, SR_y and SR_B is as follows:

$$
\begin{aligned}
|\psi_j\rangle_{fin} &= \frac{1}{\sqrt{2}}(|t_j + \tau_{hold} + \tau_j\rangle_X|0\rangle_Y \\
&\quad + (-1)^b|0\rangle_X|t_j + \tau_j + \tau_{hold}\rangle_Y) \\
&= \frac{1}{\sqrt{2}}(|t'_j\rangle_X|0\rangle_Y + (-1)^b|0\rangle_X|t'_j\rangle_Y),
\end{aligned} \tag{16}
$$

where τ_{hold} is the length of the time that Ψ_j was stored in SR_x and SR_y, and

$$t'_j \equiv t_j + \tau_{hold} + \tau_j. \tag{17}$$

Meanwhile, when combined with BS_B, the detectors D_0 and D_1 serve as the projective operators:

$$P_0 \equiv |\psi\rangle_0\langle\psi|_0 \tag{18}$$

and

$$P_1 \equiv |\psi\rangle_1\langle\psi|_1, \tag{19}$$

respectively, where

$$|\psi\rangle_0 \equiv \frac{1}{\sqrt{2}}(|t_B\rangle_X|0\rangle_Y + |0\rangle_X|t_B\rangle_Y) \tag{20}$$

and

$$|\psi\rangle_1 \equiv \frac{1}{\sqrt{2}}(|t_B\rangle_X|0\rangle_Y - |0\rangle_X|t_B\rangle_Y), \tag{21}$$

with t_B denoting the time that Bob applies the measurement. Therefore, if Bob takes $t_B = t'_j$, then, in the ideal case where the error rate ε is negligible, the detector D_b should click with certainty where b is Alice's committed bit. Otherwise, he knows that Alice cheated.

To see that the above presentation of the states is equivalent to that in our theoretical QBC protocol, let us view the time range $[0, \tau_{max}]$ (within which Alice picks her delay time

τ_j) as a series of time slots $T_1, T_2, \ldots, T_i, \ldots, T_{n-1}$. Here, $0 \leq T_i \leq \tau_{\max}$ ($i = 1, \ldots, n - 1$), and $T_i \neq T_{i'}$ for any $i \neq i'$. When time can be treated as a continuous variable, there is an infinite number of choices for T_i, i.e., $n \to \infty$. Now, for each Ψ_j ($j = 1, \ldots, s$), let us define:

$$|0\rangle \equiv |t_j\rangle_X |0\rangle_Y \tag{22}$$

and

$$|i\rangle \equiv |0\rangle_X |t_j + T_i\rangle_Y. \tag{23}$$

It is easy to verify that $\langle i' | i \rangle = \delta_{i'i}$. That is, a single photon Ψ_j can be treated as an n-dimensional system, with $\{|i\rangle, i = 0, \ldots, n - 1\}$ being an orthonormal basis.

With these newly defined $|0\rangle$ and $|i\rangle$, we can see that, in the experimental protocol, when Alice chooses the delay time as $\tau_j = T_i$ ($i \in \{1, \ldots, n - 1\}$), Equation (15) can be rewritten as follows:

$$|\psi_j\rangle_A = \frac{1}{\sqrt{2}}(|0\rangle + (-1)^b |i\rangle). \tag{24}$$

This is exactly the state that Alice sends in step (i) of the theoretical protocol for committing the bit b, as shown by Equations (1) and (2). Thus, it is proven that our proposed experimental protocol is equivalent to the theoretical one in principle, so that the security proof in ref. [56] also applies. Consequently, the experimental protocol is secure as long as time can be treated as a continuous variable so that the condition $n \to \infty$ can be reached.

2.4. Feasibility

The experimental apparatus shown in Figure 1 is much the same as those of the quantum key distribution (QKD) and quantum private query protocols in refs. [57–59]. The only difference is that our protocol requires two more storage rings SR_x and SR_y. The QKD protocol in ref. [57] was already realized experimentally in ref. [60]. By comparing our apparatus with Figure 1 of ref. [60], we can see that the technology in ref. [60] is sufficient for implementing our protocol too. Detailed description of the actual experimental devices can be found in Section III of ref. [60].

An important part of the implementation is to find storage rings SR_x and SR_y with a sufficiently long delay time because they determine the holding time (the time interval between the commit phase and the unveil phase) of the protocol. Using 150 km of optical fiber (which was proven to be able to guarantee sufficiently high key rate for QKD in practice) to make the storage ring can generate about 500 μs delay time. While such a holding time seems short, it is already sufficient for practical applications such as quantum coin tossing, as shown in Appendix B.

2.5. Practical Difficulties

The security of the practical implementation of the protocol, however, is limited by two difficulties. (1) The length of the classical communications between Alice and Bob has to remain finite, so that Alice cannot announce the delay times τ_j ($j = 1, \ldots, s$) with an unlimited number of digits. (2) The delay time of the storage rings SR_A and SR_B cannot be adjusted to an unlimited precision either, so that Alice and Bob cannot set τ_j precisely to any desired value. Consequently, the number of choices for the time slots T_i in Equation (23) (from which τ_j can be picked) cannot really go to infinite. Instead, when the above two difficulties limit the precision of time control to $\Delta\tau$, the number of time slots within the range $[0, \tau_{\max}]$ is as below:

$$n = \tau_{\max}/\Delta\tau + 1. \tag{25}$$

Therefore, the quantum optical method in Section 2.2 actually implements finite n-dimensional systems, instead of infinite-dimensional ones. That is, though the two protocols are equivalent in principle, in practice, the experimental scheme is not a faithful implementation of our theoretical protocol in Section 2.1. Thus, it cannot be as secure as the latter.

Nevertheless, making use of this limitation for cheating is technically challenging too. Suppose that Alice and Bob know the value of $\Delta\tau$ and therefore know the actual finite n. According to Section 5 of ref. [56], if Alice wants to cheat, she needs to have the technology to prepare entangled states in the form of Equation (4) in the commit phase, which is the quantum superposition of n different states. Moreover, later in the unveil phase, when she measures system α to complete her cheating, she needs to discriminate her measurement result between $|\alpha_{i+}\rangle$ and $|\tilde{\alpha}_{i-}\rangle$, where the latter is defined by Equation (9). Multiplying $\langle\alpha_{i+}|$ by it and we yield the following:

$$|\langle\alpha_{i+}|\tilde{\alpha}_{i-}\rangle|^2 = 1 - \frac{4}{n+2} \qquad (26)$$

(i.e., Equation (3.10) of ref. [56]). In our experimental protocol, suppose that the storage rings can achieve a precision of $\Delta\tau = 300$ ps; then, for $\tau_{max} = 500$ μs, there is $n \simeq 1.67 \times 10^6$. We can see that $|\langle\alpha_{i+}|\tilde{\alpha}_{i-}\rangle|^2$ is so close to 1 that even a tiny amount of noise and error in Alice's experimental devices (which is inevitable in practice) could make the discrimination between $|\alpha_{i+}\rangle$ and $|\tilde{\alpha}_{i-}\rangle$ impossible. On the other hand, if Bob is dishonest and wants to learn the committed bit b before the unveil phase, according to Section 7 of ref. [56], he needs to be capable of discriminating the two density matrices $\rho_0^\beta = \rho_+^{\otimes s}$ and $\rho_1^\beta = \rho_-^{\otimes s}$ where the trace distance between ρ_+ and ρ_- is below:

$$D(\rho_+, \rho_-) = \frac{1}{\sqrt{n-1}} \qquad (27)$$

(i.e., Equation (3.1) of ref. [56]). Again, in the practical setting, such a tiny difference between the states could be completely drowned by the noise and error in the experimental devices. Therefore, even with the limited n value achievable today, the experimental protocol in Section 2.2 can at least be used as a practically secure (instead of unconditionally secure) QBC scheme, or serve as a proof-of-principle implementation of the theoretical protocol in Section 2.1.

3. Discussion

In summary, we showed that, as long as time can be treated as a continuous variable, then each infinite-dimensional system in the unconditionally secure QBC protocol proposed in ref. [56] can be realized using a single photon. Thus, we obtained an experimental implementation of this QBC protocol which is feasible under currently available technology. Other "post-cold-war era" multi-party cryptographic protocols are, therefore, made possible too, e.g., quantum coin tossing, as elaborated in Appendix B.

The dimension of the systems cannot really be infinite in practice though, making the current experimental implementation a practically secure QBC only. Nevertheless, it still has an advantage over many other practically secure QBC protocols (e.g., refs. [61–63]). While these protocols could be more feasible than ours in practice, their security is based on certain practical limitations. For example, currently available quantum memory cannot store the quantum states for a long period of time, so that, as long as the holding phase of the protocol is longer than this period of time, we can be sure that Alice can no longer cheat by storing the states and delaying the measurement until the unveil phase. However, as technology advances, the storage time of quantum memory will increase, making it harder and harder to keep the corresponding protocol secure. On the contrary, the security of our experimental protocol is based on the unconditionally secure theoretical protocol in ref. [56]. Practical limitation is the reason that weakens its security so that it can be practically secure only, not the reason that makes it secure. Therefore, with the advance in the technology on the precision of the delay time adjustment, we can expect the security of this experimental protocol to be constantly improved towards that of the theoretical protocol in ref. [56]. Meanwhile, it is also worth studying whether some new technologies can be adopted to

implement the infinite-dimensional systems to make our protocol even more feasible, e.g., the continuous phase noise resulting from gain switching laser operation [64].

Our result may also contribute to the development of fundamental theories. There is a brilliant idea called the CBH theorem [65], which intends to deduce quantum theory by using three information–theoretic constraints as fundamental axioms: (I) the impossibility of superluminal information transfer, (II) the impossibility of perfect broadcasting of an unknown state, and (III) the impossibility of unconditionally secure BC. The reason for including the last constraint is that Alice's cheating strategy against BC requires the use of entangled states, as can be seen from Section 2.1 of the current work. That is, the impossibility of unconditionally secure BC entails the existence of non-locality, which is one of the essential feature of quantum theory. However, in the three QBC protocols we previously proposed in refs. [45–47], which manage to evade the MLC no-go theorem, non-locality is necessary even for honest participants. This observation implies that, if the constraint (III) is wrong, i.e., unconditionally secure QBC exists, then non-locality is also entailed. For this reason, we tend to believe that the (in)validity of constraint (III) has nothing to do with the existence of non-locality. The latter has to exist in our physical world. To complete the deduction of quantum theory from information–theoretic axioms, we should look for another constraint to replace constraint (III). Nevertheless, the finding of the unconditionally secure QBC protocol in ref. [56] may blur the above picture at first glance. This is because the protocol makes use of infinite-dimensional systems instead of entangled states, so that it seems to indicate that, in addition to non-locality, infinity should also be taken into account as the quantum resources that need to be entailed if we want to build quantum theory completely on top of information–theoretic axioms. Notably, the result in the current work provides a clue to clean this mist. As can be seen from Figure 1, in our implementation of the infinite-dimensional systems, each photon state is divided spatially into two wave packets that travel along different paths, so that non-locality is introduced. Therefore, the current implementation scheme bridges infinity with non-locality, so that non-locality could still be considered as the only quantum resource that guarantees unconditionally secure QBC.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

BC	Bit Commitment
QBC	Quantum Bit Commitment
MLC	Mayers–Lo–Chau
HJW	Hughston–Jozsa–Wootters
MZ	Mach–Zehnder
QKD	Quantum Key Distribution
QCT	Quantum Coin Tossing

Appendix A. Confidence Interval of the Error Rate

In the last step of our experimental QBC protocol, Bob is supposed to find $(1 - \varepsilon)s$ photons detected by D_b instead of $D_{\bar{b}}$ when Alice is honest. However, since ε is only the statistical average of the error rate of the experimental apparatus, Bob cannot expect to find exactly $(1 - \varepsilon)s$ photons detected correctly. A certain range of statistical deviations has to be allowed. Now, let us estimate the size of this range.

According to Theorem 3.3 of ref. [2] (which is based on Bernshtein's law of large numbers), when each of the s photons stands the probability $p = (1 - \varepsilon)$ to make the

correct detector D_b click, for arbitrarily small positive value $\delta \leq p(1-p)$, the probability for the case $|s'/s - p| \geq \delta$ to occur satisfies this equation:

$$\Pr(\left|\frac{s'}{s} - p\right| \geq \delta) \leq 2e^{-s\delta^2}. \tag{A1}$$

Here, s' denotes the actual number of photons being detected correctly in a complete run of the protocol. This inequality means that s' should be within the range $[(1-\varepsilon)s - \delta s, (1-\varepsilon)s + \delta s]$, albeit with a probability $2e^{-s\delta^2}$ at the most. For example, when $s = 10{,}000$, $\varepsilon = 10\%$, and $\delta = 5\%$, we have $2e^{-s\delta^2} \simeq 2.8 \times 10^{-11}$, which is extremely small. As a result, the number of photons that are actually detected by Bob's D_b should be within the range $[8500, 9500]$, otherwise he can confidently conclude that Alice is dishonest.

Appendix B. Quantum Coin Tossing as an Application

Although the holding time of our QBC protocol may look short even with state-of-the-art optical delay devices, it is sufficient for some practical applications. Here, as an example, we will show how quantum coin tossing (QCT, a.k.a. quantum coin flipping) [1] can be realized.

The goal of QCT is to provide a method for two separate parties, Alice and Bob, to generate a random bit value $c = 0$ or 1 remotely, while they do not trust each other. If the parties have opposite desired values, e.g., Alice wants $c = 0$ while Bob wants $c = 1$, then it is called weak QCT. Conversely, if their desired values are random, then it is called strong QCT. Here, we focus on strong QCT. Such a protocol is considered secure if neither party can bias the outcome, so that $c = 0$ and $c = 1$ will occur with the equal probabilities $1/2$, just as if they are tossing an ideal fair coin. Possible application scenarios of QCT may include the case where divorced and separated couples want to decide how to divide their property over the telephone. Other more complicated applications such as online gambling can be constructed through it too.

Strong QCT with an arbitrarily small bias was also considered a hard task if unconditionally secure QBC is impossible [11], but, when QBC becomes available, QCT can easily be built upon it as follows.

Strong QCT protocol:

(I) *Alice and Bob complete the commit phase of our QBC protocol, where Alice picks the value of her committed bit b randomly;*

(II) *During the holding phase, Bob picks a random bit x and announces it to Alice through the classical channel;*

(III) *Alice and Bob complete the unveil phase of our QBC protocol. That is, Alice unveils her committed bit b, and Bob checks whether she is honest or not;*

(IV) *Both Alice and Bob accept $y \equiv b \oplus x$ as the coin tossing result.*

It is trivial to show that, if the QBC protocol is secure (i.e., Alice cannot change b after the commit phase and Bob cannot know b before the unveil phase), then, the value of the final tossing result y is completely random. Neither Alice nor Bob can bias it to any specific value.

In this example, the commit and unveil phases of the QBC protocol are separated merely by step (II), where only one classical bit x is transferred. Bob can decide the value of x beforehand but keep it secret from Alice during step (I). Then, step (II) can be performed automatically under the control of classical computers, which can be performed very quickly. Therefore, the holding time in our QBC protocol is already long enough for such operations, so that it can result in a useful QCT protocol in practice.

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; p. 175.
2.   Brassard, G.; Crépeau, C.; Jozsa, R.; Langlois, D. A quantum bit commitment scheme provably unbreakable by both parties. In Proceedings of the 34th Annual IEEE Symposium on Foundations of Computer Science, Palo Alto, CA, USA, 3–5 November 1993; IEEE: Los Alamitos, CA, USA, 1993; p. 362.
3.   Rabin, M.O. *How to Exchange Secrets by Oblivious Transfer*; Technical Report TR-81; Aiken Computation Laboratory, Harvard University: Cambridge, MA, USA, 1981. Available online: http://eprint.iacr.org/2005/187.pdf (accessed on 18 March 2010).
4.   Even, S.; Goldreich, O.; Lempel, A. A randomized protocol for signing contracts (Extended abstract). In *Advances in Cryptology, Proceedings of the Crypto '82, Santa Barbara, CA, USA, 23–25 August 1982*; Chaum, D., Rivest, R.L., Sherman, A.T., Eds.; Plenum: New York, NY, USA, 1982; p. 205.
5.   Kilian, J. Founding cryptography on oblivious transfer. In Proceedings of the 1988 ACM Annual Symposium on Theory of Computing, Chicago, IL, USA, 2–4 May 1988; ACM: New York, NY, USA, 1988; p. 20.
6.   Mayers, D. The trouble with quantum bit commitment. *arXiv* **1996**, arXiv:quant-ph/9603015v3.
7.   Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **1997**, *78*, 3414. [CrossRef]
8.   Lo, H.-K.; Chau, H.F. Is quantum bit commitment really possible? *Phys. Rev. Lett.* **1997**, *78*, 3410. [CrossRef]
9.   Crépeau, C. What is going on with quantum bit commitment? In Proceedings of the Pragocrypt '96: 1st International Conference on the Theory and Applications of Cryptology, Prague, Czech Republic, 3–7 November 1996.
10. Chau, H.F.; Lo, H.-K. Making an empty promise with a quantum computer. *Fortsch. Phys.* **1998**, *46*, 507. [CrossRef]
11. Lo, H.-K.; Chau, H.F. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Physica D* **1998**, *120*, 177. [CrossRef]
12. Brassard, G.; Crépeau, C.; Mayers, D.; Salvail, L. The security of quantum bit commitment schemes. In Proceedings of the Randomized Algorithms, Satellite Workshop of 23rd International Symposium on Mathematical Foundations of Computer Science, Brno, Czech Republic, 24–28 August 1998.
13. Bub, J. The quantum bit commitment theorem. *Found. Phys.* **2001**, *31*, 735. [CrossRef]
14. Broadbent, A.; Schaffner, C. Quantum cryptography beyond quantum key distribution. *Designs Codes Cryptogr.* **2016**, *78*, 351. [CrossRef]
15. Brassard, G.; Crépeau, C.; Mayers, D.; Salvail, L. A brief review on the impossibility of quantum bit commitment. *arXiv* **1997**, arXiv:quant-ph/9712023v1.
16. Brassard, G.; Crépeau, C.; Mayers, D.; Salvail, L. Defeating classical bit commitments with a quantum computer. *arXiv* **1998**, arXiv:quant-ph/9806031v1.
17. Damgård, I.; Kilian, J.; Salvail, L. On the (im)possibility of basing oblivious transfer and bit commitment on weakened security assumptions. In *Advances in Cryptology, Proceedings of the EUROCRYPT '99, Prague, Czech Republic, 2–6 May 1999*; LNCS; Springer: Berlin/Heidelberg, Germany, 1999; Volume 1592, pp. 56–73.
18. Kent, A. Impossibility of unconditionally secure commitment of a certified classical bit. *Phys. Rev. A* **2000**, *61*, 042301. [CrossRef]
19. Canetti, R.; Fischlin, M. Universally composable commitments. *Lect. Notes Comput. Sci.* **2001**, *2139*, 19.
20. Kent, A. Why classical certification is impossible in a quantum world. *Quantum Inf. Process.* **2012**, *11*, 493. [CrossRef]
21. Spekkens, R.W.; Rudolph, T. Degrees of concealment and bindingness in quantum bit commitment protocols. *Phys. Rev. A* **2001**, *65*, 012310. [CrossRef]
22. Spekkens, R.W.; Rudolph, T. Optimization of coherent attacks in generalizations of the BB84 quantum bit commitment protocol. *Quant. Inf. Comput.* **2002**, *2*, 66. [CrossRef]
23. D'Ariano, G.M. The quantum bit commitment: A finite open system approach for a complete classification of protocols. *arXiv* **2002**, arXiv:quant-ph/0209149v1.
24. D'Ariano, G.M. The quantum bit commitment: A complete classification of protocols. *arXiv* **2002**, arXiv:quant-ph/0209150v1.
25. Chailloux, A.; Kerenidis, I. Optimal bounds for quantum bit commitment. In Proceedings of the 52nd IEEE Symposium on Foundations of Computer Science, Palm Springs, CA, USA, 22–25 October 2011; p. 354.
26. D'Ariano, G.M.; Kretschmann, D.; Schlingemann, D.; Werner, R.F. Reexamination of quantum bit commitment: The possible and the impossible. *Phys. Rev. A* **2007**, *76*, 032328. [CrossRef]
27. Chiribella, G.; D'Ariano, G.M.; Perinotti, P.; Schlingemann, D.M.; Werner, R.F. A short impossibility proof of quantum bit commitment. *Phys. Lett. A* **2013**, *377*, 1076. [CrossRef]
28. Mayers, D. Superselection rules in quantum cryptography. *arXiv* **2002**, arXiv:quant-ph/0212159v2.
29. Kitaev, A.; Mayers, D.; Preskill, J. Superselection rules and quantum protocols. *Phys. Rev. A* **2004**, *69*, 052326. [CrossRef]
30. Halvorson, H. Remote preparation of arbitrary ensembles and quantum bit commitment. *J. Math. Phys.* **2004**, *45*, 4920. [CrossRef]
31. Disilvestro, L.; Markham, D. Quantum protocols within Spekkens' toy model. *Phys. Rev. A* **2017**, *95*, 052324. [CrossRef]
32. Cheung, C.-Y. Secret parameters in quantum bit commitment. *arXiv* **2005**, arXiv:quant-ph/0508180v2.
33. Cheung, C.-Y. Insecurity of quantum bit commitment with secret parameters. *Int. J. Mod. Phys. B* **2007**, *21*, 4271. [CrossRef]
34. Cheung, C.-Y. On the question of secret probability distributions in quantum bit commitment. *Chin. J. Phys.* **2019**, *58*, 320. [CrossRef]

35. Magnin, L.; Magniez, F.; Leverrier, A.; Cerf, N.J. Strong no-go theorem for Gaussian quantum bit commitment. *Phys. Rev. A* **2010**, *81*, 010302. [CrossRef]

36. Modi, K.; Pati, A.K.; De, A.S.; Sen, U. Masking quantum information is impossible. *Phys. Rev. Lett.* **2018**, *120*, 230501. [CrossRef]

37. Bhowmick, S.; Srivastav, A.; Pati, A.K. No-masking theorem for observables and no-bit commitment. *arXiv* **2022**, arXiv:2209.12261v1.

38. Vilasini, V.; Portmann, C.; del Rio, L. Composable security in relativistic quantum cryptography. *New J. Phys.* **2019**, *21*, 043057. [CrossRef]

39. Chiribella, G.; D'Ariano, G.M.; Perinotti, P. Probabilistic theories with purification. *Phys. Rev. A* **2010**, *81*, 062348. [CrossRef]

40. Li, Q.; Li, C.-Q.; Long, D.-Y.; Chan, W.H.; Wu, C.-H. On the impossibility of non-static quantum bit commitment between two parties. *Quantum Inf. Process.* **2012**, *11*, 519. [CrossRef]

41. Gutoski, G.; Rosmanis, A.; Sikora, J. Fidelity of quantum strategies with applications to cryptography. *Quantum* **2018**, *2*, 89. [CrossRef]

42. Sikora, J.; Selby, J. A simple proof of the impossibility of bit-commitment in generalised probabilistic theories using cone programming. *Phys. Rev. A* **2018**, *97*, 042302. [CrossRef]

43. Nagy, M.; Nagy, N. An information-theoretic perspective on the quantum bit commitment impossibility theorem. *Entropy* **2018**, *20*, 193. [CrossRef]

44. Sun, X.; He, F.; Wang, Q. Impossibility of quantum bit commitment, a categorical perspective. *Axioms* **2020**, *9*, 28. [CrossRef]

45. He, G.P. Secure quantum bit commitment against empty promises. *Phys. Rev. A* **2006**, *74*, 022332. [CrossRef]

46. He, G.P. Quantum key distribution based on orthogonal states allows secure quantum bit commitment. *J. Phys. A Math. Theor.* **2011**, *44*, 445305. [CrossRef]

47. He, G.P. Simplified quantum bit commitment using single photon nonlocality. *Quantum Inf. Process.* **2014**, *13*, 2195. [CrossRef]

48. He, G.P. Chapter 4: Density matrices in quantum bit commitment. In *Understanding Density Matrices*; Danielsen, N.V., Ed.; Nova Science Publishers: New York, NY, USA, 2019; pp. 139–164.

49. Yuen, H.P. An unconditionally secure quantum bit commitment protocol. *arXiv* **2012**, arXiv:1212.0938v1.

50. Srikanth, R. Quantum bit commitment and the reality of the quantum state. *Found. Phys.* **2018**, *48*, 92. [CrossRef]

51. Cheung, C.-Y. Unconditionally secure quantum bit commitment using modified double-slit and unstable particles. *arXiv* **2023**, arXiv:2305.12902v1.

52. Hughston, L.P.; Jozsa, R.; Wootters, W.K. A complete classification of quantum ensembles having a given density matrix. *Phys. Lett. A* **1993**, *183*, 14. [CrossRef]

53. Uhlmann, A. The "transition probability" in the state space of a *-algebra. *Rep. Math. Phys.* **1976**, *9*, 273. [CrossRef]

54. Kirkpatrick, K.A. The Schrödinger-HJW Theorem. *Found. Phys. Lett.* **2006**, *19*, 95. [CrossRef]

55. He, G.P. Chaos in quantum steering in high-dimensional systems. *Phys. Rev. A* **2018**, *97*, 042340. [CrossRef]

56. He, G.P. Unconditionally secure quantum bit commitment based on the uncertainty principle. *Proc. R. Soc. A* **2019** , *475*, 20180543.

57. Goldenberg, L.; Vaidman, L. Quantum cryptography based on orthogonal states. *Phys. Rev. Lett.* **1995**, *75*, 1239. [CrossRef]

58. Koashi, M.; Imoto, N. Quantum cryptography based on split transmission of one-bit information in two steps. *Phys. Rev. Lett.* **1997**, *79*, 2383. [CrossRef]

59. Xu, S.-W.; Sun, Y.; Lin, S. Quantum private query based on single-photon interference. *Quantum Inf. Process.* **2016**, *15*, 3301. [CrossRef]

60. Avella, A.; Brida, G.; Degiovanni, I.P.; Genovese, M.; Gramegna, M.; Traina, P. Experimental quantum-cryptography scheme based on orthogonal states. *Phys. Rev. A* **2010**, *82*, 062309. [CrossRef]

61. Danan, A.; Vaidman, L. Practical quantum bit commitment protocol. *Quantum Inf. Process.* **2012**, *11*, 769. [CrossRef]

62. Ng, N.H.Y.; Joshi, S.K.; Chia, C.M.; Kurtsiefer, C.; Wehner, S. Experimental implementation of bit commitment in the noisy-storage model. *Nat. Commun.* **2012**, *3*, 1326. [CrossRef]

63. Nikolopoulos, G.M. Optical scheme for cryptographic commitments with physical unclonable keys. *Opt. Express.* **2019**, *27*, 29367. [CrossRef]

64. Shakhovoy, R.; Puplauskis, M.; Sharoglazova, V.; Duplinskiy, A.; Sych, D.; Maksimova, E.; Hydyrova, S.; Tumachek, A.; Mironov, Y.; Kovalyuk, V.; et al. Phase randomness in a semiconductor laser: Issue of quantum random-number generation. *Phys. Rev. A* **2023**, *107*, 012616. [CrossRef]

65. Clifton, R.; Bub, J.; Halvorson, H. Characterizing quantum theory in terms of information-theoretic constraints. *Found. Phys.* **2003**, *33*, 1561. [CrossRef]