applied sciences

MDPI

Article

# Practical Quantum Bit Commitment Protocol Based on Quantum Oblivious Transfer

**Yaqi Song [1,2,3] and Li Yang [1,2,3,*]**

1 State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China; songyaqi@iie.ac.cn
2 Data Assurance and Communication Security Research Center, Chinese Academy of Sciences, Beijing 100093, China
3 School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
* Correspondence: yangli@iie.ac.cn

Received: 14 September 2018; Accepted: 2 October 2018; Published: 19 October 2018


**Abstract:** Oblivious transfer (OT) and bit commitment (BC) are two-party cryptographic protocols which play crucial roles in the construction of various cryptographic protocols. We propose three practical quantum cryptographic protocols in this paper. We first construct a practical quantum random oblivious transfer (R-OT) protocol based on the fact that non-orthogonal states cannot be reliably distinguished. Then, we construct a fault-tolerant one-out-of-two oblivious transfer ($OT_1^2$) protocol based on the quantum R-OT protocol. Afterwards, we propose a quantum bit commitment (QBC) protocol which executes the fault-tolerant $OT_1^2$ several times. Mayers, Lo and Chau (MLC) no-go theorem proves that QBC protocol cannot be unconditionally secure. However, we find that computing the unitary transformation of no-go theorem attack needs so many resources that it is not realistically implementable. We give a definition of physical security for QBC protocols and prove that the practical QBC we proposed is physically secure and can be implemented in the real world.

**Keywords:** quantum cryptography; oblivious transfer; bit commitment; practical protocol; physical security

## 1. Introduction

Quantum oblivious transfer (QOT) and quantum bit commitment (QBC) protocols are basic in quantum cryptography. They are important building blocks of multi-party secure computations. The study of QOT was started by Crépeau and Kilian [1]. In 1992, a practical QOT protocol was proposed [2]. However, in these two protocols, if Bob measures the pulses after Alice disclosing the basis, he will get both messages and Alice's privacy will be destroyed. In the light of this drawback, Crépeau proposed a QOT protocol [3] based on a QBC scheme [4] to ensure that Bob cannot delay his measurement. Then, Yao proved that QOT constructed based on QBC [5] is secure. Shortly afterwards, Mayers, Lo and Chau separately presented no-go theorem and proved that there is no non-interactive QBC protocol with statistical security [6–9]. Subsequently, a great number of works that extend the framework of no-go theorem and further prove the impossibility of the standard QBC has been presented since Then, [10–16]. These results indicate that QOT protocols constructed based on QBC are not secure either. Then, quantum secure computations are also considered to be insecure [17–20].

Researchers Then, attempt to construct QBC protocols that can evade the no-go theorem. The most famous ones are relativistic QBC protocols, which were first proposed by Kent [21–24]. The protocol in Ref. [23] was implemented by different groups [25,26]. The time during commit phase and opening phase is limited by the distance between the trusted agents, which may be a restriction for building other multi-party cryptographic protocols. In addition, some QBC with computational security were

proposed. Unconditionally binding and computationally concealing QBC schemes were presented by Tanaka [27] and Chailloux [28], respectively, and in 2016, another computationally binding commitment scheme was proposed and it can be realized from hash functions like SHA-3 [29]. The security of these QBC protocols depends on the limited computing power of the adversary. Once the computing power is improved in the future, the security of these protocols are threatened. Several QBC protocols were proposed based on physical hypothesis, such as bounded-quantum-storage model [30,31], noisy-storage model [32–34] and technological limitations on non-demolition measurements [35], the security of these protocols is threatened by the development of techniques. Some QBC schemes with security requirements relaxed were put forward, such as cheat-sensitive QBC [36–39] and game theoretic secure QBC [40]. There are also some non-relativistic QBC schemes which are claimed to be unconditionally secure [41–46]. However, most of them only exist theoretically. For example, in Ref. [43] Bob stores the quantum registers unmeasured until *opening phase*, which can be hardly implemented in practice.

In this paper, we do not devote to evading the no-go theorem. We give the definition of physical security. As long as the physical security is satisfied, even the attacker who ownes all the resources of the earth cannot break the protocol. The physical security was first proposed in Ref. [47]. The time complexity of no-go theorem attack algorithm is $O(2^{3n})$, where $n$ is the security parameter of the QBC. In addition this algorithm needs at least $O(2^{2n})$ size of memory space to store the matrix of the unitary transformation. We define that if the entry number of the attack matrix is greater than the total number of protons on the earth (approximately $10^{50}$), QBC achieves physical-secure binding. It means when $n > 83$, no-go theorem attack can hardly be realized in practice. Compared with those QBC schemes based on physical hypothesis, the definition of physical security limits the attacker with all the resources of the earth. QBC protocols that achieve physical security are more secure than other protocols based on physical hypothesis. In this paper, we focus on how to construct practical quantum protocols with physical security.

In [48], Yang constructed QBC based on QOT. We modify the protocols so that it can be applied in practice and achieve physical security. The imperfect sources, quantum channel and detectors are all allowed in the modified protocols. Considering error-correcting code and tolerable error rate, we describe the protocols in detail and analyze the security and problems we may face in practice.

The practical QBC protocol proposed in this paper has advantages over many existing protocols. Compared with the relativistic QBC protocols, the time between *commit phase* and *opening phase* is not limited in our scheme. Compared with the computationally secure protocols and QBC based on physical hypothesis, the physical security of our scheme will not be threatened by the growing computing power and techniques. Compared with those theoretical protocols, our schemes allow the imperfect equipment and can be implemented in the real world. The QBC protocols in Refs. [47,48] are also theoretical. The security analysis of these theoretical protocols is based on the ideal world rather than the real world. Therefore, these theoretical protocols which are not fault-tolerant cannot achieve the security they declared and cannot be realized in the real world. Our practical quantum cryptographic protocols, which are allowing the imperfection of current optoelectronic apparatus, provide appropriate security parameters and security analysis in the practical conditions. In sum, the practical QBC protocol achieves physical security and can be possible realized. Since the selection of security parameters and security analysis are based on available optoelectronic apparatus, the implement and security of the protocols are more practical and reliable.

## 2. The Efficiency and Errors of Practical Apparatuses

In practical protocols, all apparatuses should be realizable and convenient. All the apparatuses in the protocols are divided into three types: emission apparatuses, channel and detection apparatuses. In a practical protocol, the following situations should be considered.

- Emission apparatuses. The practical and efficient single-photon sources have not yet been realized, while some researchers have been studying the spectra [49] and efficiency [50] of the single-photon

sources. In this paper, the single-photon sources are not adopted. Instead, we use weak coherent pulses with typical average photon number of $\mu_S$ in the following protocols, which can be easily prepared by standard semiconductor lasers and calibrated attenuators [51]. The error rate caused by the emission apparatuses is denoted as $\varepsilon_S$. A pulse is requested to contain only one kind of polarization, but more than one photon in a pulse are allowed.

- Channel loss and error. The existence of the channel loss leads to an imperfect transfer efficiency, and the noise in the channel leads to some channel error. Suppose the transfer efficiency of the channel is $\eta_C$, the error rate caused by the channel is $\varepsilon_C$. Refs. [52,53] provided the physical setups and detailed properties of some kinds of quantum channels.
- Detection apparatuses. In practice there is no detector with perfect detection efficiency. The quantum efficiency $\eta_D$ is the probability that the detector registers a count when one photon comes in, and the error rate caused by the detection apparatuses is $\varepsilon_D$, where the main error source is the dark count $d$. The single-photon detectors with high efficiency, like 80–93% have been realized in the laboratory [54,55].

Assume all the parameters described above are all known by both parities of the protocol, and the typical average photon number of the whole system is $\mu \equiv \mu_S \eta_C \eta_D$. Then, the overall error rate is $\varepsilon \equiv 1 - (1 - \varepsilon_S)(1 - \varepsilon_C)(1 - \varepsilon_D)$.

## 3. Practical Weak QOT and QBC

**Definition 1.** *Random Oblivious Transfer (R-OT) Channel.*
*Alice sends a random bit r to Bob via a channel, if*

1. *Bob obtains the bit value r with a probability p satisfying* $0 < b < p < a$, $a < \frac{1}{2}$, *where a and b are any two real numbers;*
2. *Alice does not know whether Bob has got the value of her bit.*

*Then, the channel is named as R-OT channel (an extended Rabin's OT channel).*

To construct a quantum string R-OT protocol, non-orthogonal states are used. There is no measuring apparatus that can distinguish non-orthogonal states with certainty. Only some probabilistic information can be obtained. Let Bob measure a sequence of photons in two quantum states $|\Psi_0\rangle$, $|\Psi_1\rangle$, where $\langle\Psi_0|\Psi_1\rangle = \cos\varphi$. Here we choose $\varphi = \frac{\pi}{6}$. The quantity of the information Bob obtains depends on the measurement he performs. The optimal measurement can differentiate the two non-orthogonal states with a probability of $1 - \cos\varphi$ [56–58], which is a kind of POVM measurement. Actually, the complicated measurement is not necessary. Even if we construct the protocol with the sub-optimal measurement, the security of the protocols can still be ensured, which will be analyzed in detail in Section 4. Through all of the measurements, we choose the most practical and easiest one. That is, Bob measures photons in two bases, $B_0 = \{|\Psi_0\rangle, |\Psi_0\rangle^\perp\}$ and $B_1 = \{|\Psi_1\rangle, |\Psi_1\rangle^\perp\}$ randomly. When the states is $|\Psi_0\rangle$, the measurement results may be $|\Psi_0\rangle$, $|\Psi_1\rangle$ or $|\Psi_1\rangle^\perp$. When the states is $|\Psi_1\rangle$, the measurement results may be $|\Psi_1\rangle$, $|\Psi_0\rangle$ or $|\Psi_0\rangle^\perp$. It can be seen that if Bob's measurement results in $|\Psi_x\rangle$, he cannot distinguish which state is sent by Alice. If his measurement results in $|\Psi_x\rangle^\perp$, which is orthogonal to $|\Psi_x\rangle$, the initial state cannot be $|\Psi_x\rangle$ and therefore is $|\Psi_{x\oplus1}\rangle$. In this sub-optimal measurement, although Bob cannot distinguish the non-orthogonal states with 100%, he unambiguously knows that the receiving state must be $|\Psi_{x\oplus1}\rangle$ when his measurement results in $|\Psi_x\rangle^\perp$. Ideally, the probability of getting a conclusive result is

$$p_{ideal} = \frac{1}{2} \times \frac{1}{2}(\langle\Psi_{x\oplus1}|\Psi_x\rangle^\perp \langle\Psi_x|\Psi_{x\oplus1}\rangle + \langle\Psi_x|\Psi_{x\oplus1}\rangle^\perp \langle\Psi_{x\oplus1}|\Psi_x\rangle) = \frac{1}{8}. \quad (1)$$

**Protocol 1.** *Practical weak quantum R-OT protocol.*

1. *Alice and Bob agree on three security parameters, N, α, and* $\varepsilon_{set}$. *The parameter N is the length of the qubit string sent by Alice. The parameter α is the expected fraction of Bob's successful detection. The parameter*

$\varepsilon_{set}$ *is the expected error rate.*
*The number of photons in a weak coherent pulse with typical average photon number of* $\mu_S$ *follows Poisson distribution* $p_n(\mu_S) = \frac{e^{-\mu_S}\mu_S^n}{n!}$. *It can be seen that the probability of no photon in a pulse is* $p_0(\mu_S) = e^{-\mu_S}$. *Then, the probability of detecting at least one photons in a pulse with typical average photon number* $\mu_S$ *through a channel with transfer efficiency* $\eta_C$ *by a detector with quantum efficiency* $\eta_D$ *is* $1 - e^{-\mu}$.
*They can set the fraction* $\alpha \simeq 1 - e^{-\mu}$ *which is the probability that Alice expects Bob to detect successfully and set error rate* $\varepsilon_{set} \simeq \varepsilon$ *or a little bit higher to allow other noise. The parameters satisfy the equation* $H(2\varepsilon_{set}) < \frac{1}{2} - (1 - e^{-\mu_S} - \mu_S e^{-\mu_S})/2\alpha$ *to resist photon number splitting attack [2].*

2. *Alice and Bob perform two tests.*
*Firstly, compare Alice's sending time* $t_i$ *with Bob's receiving time* $t_i'$ *for each pulse. Since the distance between Alice and Bob is fixed, by the test they can easily get the traveling time* $\theta$, *i.e.,* $\theta = t_i' - t_i$. *This test not only marks the address of each pulse, but also helps to distinguish the error caused by noises and dark counts.*
*Secondly, Alice sends a sequence of pulses through the quantum channel and tells Bob the bases of the pulses through a classical channel. Bob detects pulses in the other bases. If and only if Bob detects the pulses successfully with a probability greater than* $\alpha$ *and an error rate less than* $\varepsilon_{set}$, *he agrees to continue the protocol. Otherwise, they take counsel together to adjust the parameter* $\alpha$ *or* $\varepsilon_{set}$.
3. *Alice generates a random bit string* $(r_1, ..., r_N) \in \{0,1\}^N$, *and sends qubit string* $|\Psi_{r_1}\rangle, \ldots, |\Psi_{r_N}\rangle$ *to Bob. She also tells Bob the sending time* $t_i$ *of each pulse through the classical channel.*
4. *Bob records the receiving time* $t_i'$ *of each pulse and compares with the sending time. If and only if* $t_i' = t_i + \theta$, *he admits* $|\Psi_{r_i}\rangle$ *as a receiving pulse. He chooses* $B_0$ *or* $B_1$ *randomly to measure each receiving pulse. For these receiving pulses, when his measurement results in state* $|\Psi_x\rangle^{\perp}$, *he accepts the pulse as a conclusive pulse and takes the bit value of this pulse as* $x \oplus 1$.
5. *The parameters are agreed by Alice and Bob. After Step 1-4, if the number of the effective pulses detected by Bob is not approximately equal to* $\alpha N$, *Bob has the right to abort the protocol. This step is a verification for the malicious Alice.*

We regard Protocol 1 as a weak R-OT because it is similar to standard R-OT. But it is weaker in security when dishonest Alice sends different states, which will be explained in Section 4.2. Then, we construct a weak quantum $OT_1^2$ protocol based on R-OT protocol, the equivalence of R-OT and $OT_1^2$ has been proved in [59].

**Protocol 2.** *Practical weak quantum* $OT_1^2$ *protocol.*

1. *Alice and Bob execute Protocol 1 and an error correcting scheme. Denote Bob's probability of getting a conclusive bit as* $p_{con}(\mu)$. *After Protocol 1, if the number of Bob's conclusive bits is not approximately equal to* $Np_{con}(\mu)$, *he regards Alice as a malicious party and aborts the protocol. If Bob agrees to continue, they decide on a security parameter k according to an error correcting scheme and the probability* $p_{con}(\mu)$. *The values of k are analyzed in Section 4 and listed in Table 1.*
2. *The error correcting scheme is applied to* $\alpha N$ *bits words with expected error rate* $\varepsilon_{set}$, *which is non-uniqueness. The following is only an example of this kind of scheme, which is based on* $(63, 57, 3)$ *Hamming code.*
*There are k bits in sets I and J after the process of error correction, respectively. Let* $l_{obt}$ *denotes the number of the bits in I or J before error correction. Alice divides two sequences of* $l_{obt}$ *bits into 63-bit blocks and performs the wire link permutation W on it. When* $l_{obt} = 63\left\lceil \frac{l_{obt}}{63} \right\rceil - \Delta$, $\Delta$ *bits of the block in front should be added to the last block. Then, calculate the syndromes* $s_{A_i}$ *and discard the check bits of each block. Repeat above operations four times and send these syndromes to Bob. Bob divides his* $l_{obt}$ *bits into 63-bit blocks and performs the wire link permutation W on it. When* $l_{obt} = 63\left\lceil \frac{l_{obt}}{63} \right\rceil - \Delta$, $\Delta$ *bits of the block in front should be added to the last block. For each round, he calculates the syndromes* $s_{B_i}$ *and* $s_i = s_{A_i} \oplus s_{B_i}$. *Correct the error in each block and discard all check bits. After error correction, assume the error rate reduces to* $\varepsilon_1'$.

3. *Bob discards all check bits and selects from the remaining bits to obtain two sets $I$ and $J$, where $I = \{i_1, \ldots, i_k\}$ and $J = \{j_1, \ldots, j_k\}$ with $I \cap J = \emptyset$. The $k$ bits $r_{i_1}, \ldots, r_{i_k}$ are chosen from the conclusive bits. In case the conclusive bits in Bob's hand are a little less than k, he adds some random bits.*
4. *Bob chooses a random bit $m$. If $m = 0$, he sends $\{X, Y\} = \{I, J\}$ to Alice. Otherwise, he sends $\{X, Y\} = \{J, I\}$.*
5. *After receiving $(X, Y)$, Alice encrypts her messages $b_0$ and $b_1$ with $r_i$,*

$$\begin{cases} c_0 = b_0 \oplus_{i \in X} r_i, \\ c_1 = b_1 \oplus_{i \in Y} r_i. \end{cases}$$

*Then, Alice sends $c_0$, $c_1$ to Bob.*
6. *Bob calculates $\oplus_{i \in I} r_i$ and decrypts $c_m$ to obtain $b_m$.*

According to the error correcting scheme, the relation between the parameters $k$ and $l_{obt}$ is

$$k = 57 \left\lceil \frac{l_{obt}}{63} \right\rceil - \Delta = l_{obt} - 6 \left\lceil \frac{l_{obt}}{63} \right\rceil. \tag{2}$$

Suppose the error rate of each bit in Protocol 1 is $\varepsilon_1 = 0.3\%$, which is a general value in practice. After error correction, the error rate can be reduced to $\varepsilon_1' = 0.0757\%$ [60]. As long as there is one bit error in key used in the decryption algorithm, Bob cannot obtain $b_m$ in Protocol 2. The error rate of Protocol 2 is $\varepsilon_2$. The relation of $\varepsilon_2$ and $\varepsilon_1'$ is

$$\varepsilon_2 = 1 - (1 - \varepsilon_1')^k. \tag{3}$$

When $\varepsilon_1' = 0.0757\%$, the values of $\varepsilon_2$ changing with the parameter $k$ are shown in Figure 1.

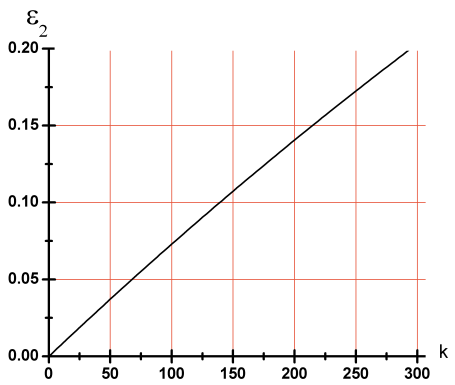


**Figure 1.** The error rate of Protocol 2 changing with the size of sets.

Protocol 2 is different from standard QOT since Alice may not transfer a correct message to Bob. If we set the upper bound of the error rate as 20%, the parameter $k$ should be less than 295 according to Equation (3).

Then, we can construct a quantum bit commitment protocol by executing the quantum $OT_1^2$ protocol $l$ times as follows.

**Protocol 3.** *Practical quantum bit commitment protocol.*
*Commit phase:*

1. *Alice randomly divides her commit value as $b = b_0^{(i)} \oplus b_1^{(i)}$, $i = 1, \ldots, l$.*
2. *Bob generates local random numbers $\{m_i = 0, 1 | i = 1, \ldots, l\}$.*
3. *Alice executes Protocol 2 with Bob $l$ times, and Bob can obtain the values $\{b_{m_i}^{(i)} | i = 1, \ldots, l\}$.*

*Opening phase:*

1. *Alice opens* $\{b_0^{(i)}, b_1^{(i)}; r_{i_1}^{(i)}, \ldots, r_{i_k}^{(i)}; r_{j_1}^{(i)}, \ldots, r_{j_k}^{(i)} | i = 1, \ldots l\}$.
2. *Bob verifies whether* $\{b_0^{(i)}, b_1^{(i)}; r_{i_1}^{(i)}, \ldots, r_{i_k}^{(i)}; r_{j_1}^{(i)}, \ldots, r_{j_k}^{(i)} | i = 1, \ldots l\}$ *are consistent with his* $\{b_{m_i}^{(i)}; r_{i_1}^{(i)}, ..., r_{i_k}^{(i)} | i = 1, \ldots l\}$ *and those conclusive bits in J. If the consistency holds more than 80% of l rounds, he admits Alice's commitment value as b. Otherwise, he regards Alice as a malicious party and aborts the protocol.*

In practice, the physical system and the coded bit string in $OT$ protocols unavoidably have some errors. In Section 3, assume $\varepsilon_1 = 0.3\%$, $k \leq 295$, the error rate of $OT_1^2$ can be less than 20%. But it does not impact the construction of a BC protocol.

## 4. The Security of QOT

A standard $OT_1^2$ scheme satisfies the following requirements.

- **Correctness** If both parities are honest and follow the protocols, Bob obtains one of the message $b_m$ sent by Alice correctly.
- **Privacy for Alice** If Alice is honest, Bob cannot obtain both of the messages sent by Alice.
- **Privacy for Bob** If Bob is honest, Alice cannot distinguish which message Bob obtains.

The aim of our QOT is to construct a practical QBC. Therefore, the correctness of the QOT protocols is not necessary. To detect a cheating Alice, suppose the probability that an honest Bob cannot get a correct message is less than 20%. Execute Protocol 2 $l$ times to construct QBC scheme. If and only if there are less than $0.2l$ rounds where Alice does not disclose the consistent results, Bob admits Alice's commitment.

For the security of $OT_1^2$ protocol, He [61] has proved that the $OT_1^2$ protocol implemented upon all-or-nothing OT is not covered by the cheating strategy in Ref. [17]. Therefore, the following security analysis of $OT_1^2$ does not contain the attack of entangled states.

### *4.1. Privacy for Alice*

The operations executed by Bob in Protocol 2 include measuring the states sent by Alice, selecting the elements in Set $I$ and $J$ Then, sending $X, Y$ to Alice, decrypting the ciphertext $c_0$ or $c_1$. It can be seen that only in the measurement, he can cheat and take a more superior measurement to obtain more conclusive results, which may lead him to get both $b_0$ and $b_1$. We analyze the probabilities of getting a conclusive bit for the honest Bob and the malicious Bob in order to determine the security parameters in the practical protocols.

#### 4.1.1. Analysis on the Probability of Getting a Conclusive Bit for Honest Bob

Let $|n_0\rangle$ and $|n_{\frac{\pi}{6}}\rangle$ denote n-photon states of polarization 0 and $\frac{\pi}{6}$, respectively. For an honest Bob, if he chooses the measurement basis $B_1$ to detect $|1_0\rangle$, the probability of the state collapsing to $|1_{\frac{2\pi}{3}}\rangle$ is $\frac{1}{4}$. For $|n_0\rangle$, the probability of at least one of the photons collapse to the state with polarization of $\frac{2\pi}{3}$ is $1 - \left(\frac{3}{4}\right)^n$. Therefore, the probability of getting a conclusive resulting in a pulse which contains $n$ photons is

$$p(n) = \frac{1}{2} \times \left[1 - \left(\frac{3}{4}\right)^n\right]. \tag{4}$$

The probability of getting a conclusive bit in a pulse with the typical average photon number $\mu$ is

$$\begin{aligned} p_{con}(\mu) &= \sum_{n=1}[p_n(\mu) \times p(n)] \\ &= \sum_{n=1}\left\{\frac{1}{2}\left[1-\left(\frac{3}{4}\right)^n\right]\frac{e^{-\mu}\mu^n}{n!}\right\} \\ &= \frac{1}{2}\left[\sum_{n=1}\frac{e^{-\mu}\mu^n}{n!} - e^{-\frac{\mu}{4}}\sum_{n=1}\frac{e^{-\frac{3\mu}{4}}\left(\frac{3\mu}{4}\right)^n}{n!}\right] \\ &= \frac{1}{2}\left(1-e^{-\frac{\mu}{4}}\right). \end{aligned} \tag{5}$$

It can be seen that an honest Bob is supposed to obtain $Np_{con}(\mu)$ conclusive bits. The probability of getting a conclusive bit in one pulse with different $\mu$ can be seen in Figure 2. The larger $\mu_S$ of emission apparatus and more efficient detector they use, the higher efficiency the protocol has.

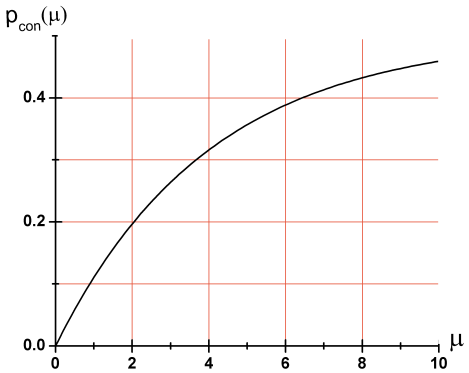


**Figure 2.** The probability that an honest Bob gets conclusive bit changing with $\mu$.

4.1.2. Analysis on the Probability of Getting a Conclusive Bit for Malicious Bob

Assume that the malicious Bob has the ability of separating $n$ photons by photon number splitting attack. For a single photon, the successful probability of optimal measurement to distinguish the two non-orthogonal states is $1 - cos\varphi$, which has been proved in Refs. [56–58]. For $n$ photons, a malicious Bob's probability of distinguishing the non-orthogonal sates is

$$p'(n) = 1 - cos^n\varphi. \tag{6}$$

Then, a malicious Bob using photon number splitting attack and optimal measurement for single-photon can get a conclusive bit with the probability of

$$p'_{con}(\mu) = \sum_{n=1} p_n(\mu) \times p'(n) = 1 - e^{-\mu(1-\frac{\sqrt{3}}{2})}. \tag{7}$$

Here we consider that the malicious Bob has an ideal detector, the quantum efficient $\eta'_D$ of which is 100%. Thus, $\mu' = \mu_S\eta_C = \frac{\mu}{\eta_D}$. Assume that the protocols are executed over atmospheric channel, the quantum efficiency $\eta_D$ of an honest Bob's detector is 80% and this kind of detector has already been realized in the laboratory [54,55]. The cheating Bob's probability of getting a conclusive bit is

$$p''_{con}(\mu) = 1 - e^{-\frac{5\mu}{4}(1-\frac{\sqrt{3}}{2})}, \tag{8}$$

which can be seen in Figure 3. A malicious Bob can get about $[1 - e^{-\frac{5\mu}{4}(1-\frac{\sqrt{3}}{2})}]N$ conclusive bits.

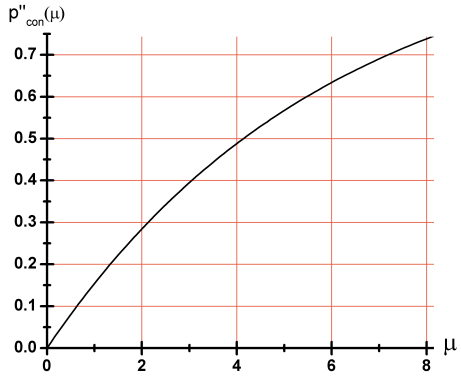


**Figure 3.** The probability that a malicious Bob gets a conclusive bit changing with $\mu$.

4.1.3. Contrastive Analysis and Determination of the Parameters in Practical Protocols

If a malicious Bob wants to obtain both $b_0$ and $b_1$ in Protocol 2, he must get at least $2k$ conclusive bits in Protocol 1. The difference between an honest Bob's probability of obtaining a conclusive bit and half of a malicious Bob's probability of obtaining a conclusive bit is $p_{diff}(\mu) = p_{con}(\mu) - \frac{1}{2}p''_{con}(\mu)$, which can be seen in Figure 4.

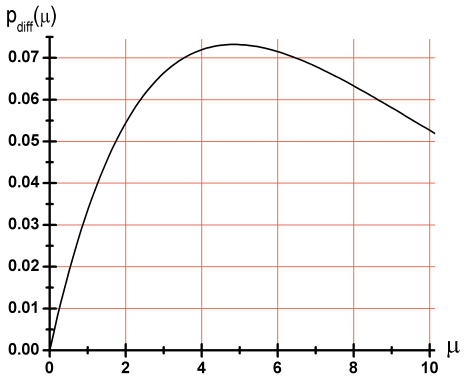


**Figure 4.** The difference between an honest Bob's probability of obtaining a conclusive bit and half of a malicious Bob's probability of obtaining a conclusive bit changing with $\mu$.

When $\mu = 4.85$, the difference $p_{diff}(\mu)$ takes a maximum value 0.0732. The probability of obtaining $i$ conclusive bits is $p_{obt}$, which is referred to the binomial distribution and shown in Figure 5.

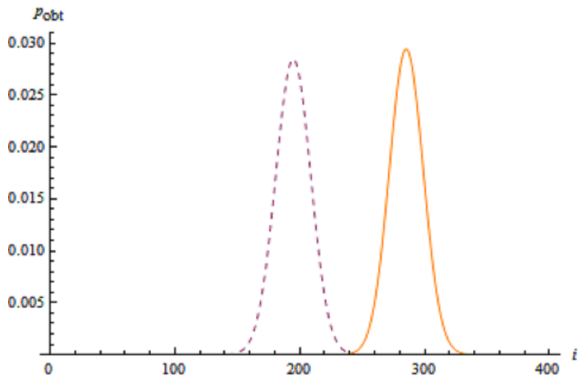


**Figure 5.** The solid line denotes the probability of an honest Bob obtains $i$ conclusive bits when $N = 800$, $\mu = 5$. It can be seen that an honest Bob can obtain more than 259 conclusive bits with a great probability. The dashed line denotes the probability of a malicious Bob obtains $i + 259$ conclusive bits.

Suppose the probability of the case where the number of conclusive bits obtained by an honest Bob is no more than $l_{obt}$ is $p_1$, and the probability of the case where the number of conclusive bits obtained by a malicious Bob is no less than $2l_{obt}$ is $p_2$. Then,

$$p_1 = \sum_{i=0}^{l_{obt}} C_N^i [p_{con}(\mu)]^i [1 - p_{con}(\mu)]^{N-i} \tag{9}$$

$$p_2 = \sum_{i=2l_{obt}}^{N} C_N^i [p'_{con}(\mu)]^i [1 - p'_{con}(\mu)]^{N-i} \tag{10}$$

To ensure that the honest Bob obtains one correct message in Protocol 2 and the malicious Bob cannot obtain both $b_0$ and $b_1$, $p_1$ and $p_2$ should be small enough.

The probability that an honest Bob cannot execute Protocol 2 successfully is $p$,

$$p = 1 - (1 - \varepsilon_2)(1 - p_1). \tag{11}$$

To detect a cheating Alice, $p$ should be less than 20%. Given an error rate $\varepsilon_2$, $p_1$ has an upper bound $p_{1t}$ to ensure $p \leq 20\%$. To ensure the concealing of the BC protocol, $p_2$ is set up with a magnitude of $10^{-6}$.

When $\mu$ is too low, the difference between the probability of obtaining a conclusive bit by an honest and a malicious Bob is not large enough to select the proper parameters. When $\mu$ is too large, the proper $k$ is large, which will lead to a large $\varepsilon_2$. Then, there is no proper parameters either. It can be seen from Table 1 that when $2 \leq \mu \leq 6$, we can always find the proper parameters to execute the protocols successfully.

**Table 1.** When $p = 20\%$, $N = 800$, $p_2$ is controlled to be a magnitude of $10^{-6}$, the values of parameters with different $\mu$.

| $\mu$ | $p_{con}(\mu)$ | $p'_{con}(\mu)$ | $l_{obt}$ | $k$ | $\varepsilon_2$ | $p_{1t}$ | $p_1$ | $p_2$ |
|---|---|---|---|---|---|---|---|---|
| 2 | 0.197 | 0.285 | 143 | 131 | 0.0944 | 0.117 | 0.107 | $3.25 \times 10^{-6}$ |
| 3 | 0.264 | 0.395 | 190 | 172 | 0.122 | 0.0887 | 0.0484 | $1.85 \times 10^{-6}$ |
| 4 | 0.316 | 0.488 | 228 | 210 | 0.147 | 0.0621 | 0.0312 | $1.53 \times 10^{-6}$ |
| 5 | 0.357 | 0.567 | 260 | 236 | 0.164 | 0.0435 | 0.0324 | $7.45 \times 10^{-7}$ |
| 6 | 0.388 | 0.634 | 283 | 259 | 0.178 | 0.0267 | 0.0236 | $4.73 \times 10^{-6}$ |

### *4.2. Privacy for Bob*

The attack for Alice is to send different states which can bias the measurements that will be conclusive for Bob. Then, she may have a larger probability to guess Bob's choice $m$. In our protocol, if and only if Bob's measurement results in state $|\Psi_0\rangle^{\perp}$ and $|\Psi_1\rangle^{\perp}$, he admits it a conclusive bit. We analyze the case where Alice sends all the states dishonestly and the case where Alice sends only one state dishonestly in R-OT protocol.

#### 4.2.1. The Attack that Alice Sends Only One State Dishonestly in R-OT Protocol

In Step (3) of Protocol 1, an honest Alice is supposed to send the state $|\Psi_0\rangle$ or $|\Psi_1\rangle$ only. However, a malicious Alice may replace one of the pulse ($|\Psi_{r_c}\rangle$) with $|\Psi_0\rangle^{\perp}$ instead. This attack makes Bob more likely to accept this pulse as a conclusive results and Alice has a higher probability to distinguish which set is Set $I$. Then, we analyze whether this attack is effective both in R-OT and $OT_1^2$ protocols.

In Protocol 1, when Alice replaces one of the pulses ($|\Psi_{r_c}\rangle$) with $|\Psi_0\rangle^{\perp}$, the number of the photons in the pulse follows Poisson distribution. Let $|n_{\frac{\pi}{2}}\rangle$ denotes an n-photon state with the polarization $\frac{\pi}{2}$. For an honest Bob, he chooses the measurement basis $B_1$ with the probability of 1/2. When he measures $|1_{\frac{\pi}{2}}\rangle$ with $B_1$, the probability that the state collapse to $|1_{\frac{2\pi}{3}}\rangle$ is $\langle\frac{\pi}{2}|\frac{2\pi}{3}\rangle\langle\frac{2\pi}{3}|\frac{\pi}{2}\rangle = 3/4$. When

he measures $|n_{\frac{\pi}{2}}\rangle$ with $B_1$, the probability that at least one of the photons of $|n_{\frac{\pi}{2}}\rangle$ collapse to the state with polarization of $\frac{2\pi}{3}$ is $1-(\frac{1}{4})^n$. According to Equation (5), the probability of choosing the basis $B_1$ and getting a conclusive bit in a pulse is

$$p_{B_1 con}(\mu) = \sum_{n=1} \left\{ \frac{1}{2} \left[ 1 - \left( \frac{1}{4} \right)^n \right] \frac{e^{-\mu}\mu^n}{n!} \right\} = \frac{1}{2} \left( 1 - e^{-\frac{3\mu}{4}} \right). \tag{12}$$

When Bob chooses the measurement basis $B_0$ to detect the fake pulse, if there is only one photon in the pulse, the probability that he accepts it as conclusive pulse is 100%. The probability of choosing the basis $B_0$ and getting a conclusive bit in a pulse is

$$p_{B_0 con}(\mu) = \frac{1}{2}(1 - e^{-\mu}). \tag{13}$$

Therefore, when Alice replaces one of the pulses with $|\Psi_0\rangle^{\perp}$, the average probability of Bob getting a conclusive result is

$$p_{(i)} = p_{B_0 con}(\mu) + p_{B_1 con}(\mu) = 1 - \frac{1}{2}e^{-\mu} - \frac{1}{2}e^{-\frac{3\mu}{4}}. \tag{14}$$

Consequently, Bob accepts the fake pulse as a conclusive result with a larger probability of $p_{(i)}$ than the situation where Alice is honest. In the following, we will analyze that although the cheating Alice has a larger probability to know Bob's choice $m$, she still has no idea what is got by Bob. In standard $OT_1^2$, if Alice has a probability larger than the legal threshold of knowing Bob's choice, she breaks Bob's privacy. In this paper, Protocol 2 is the block of constructing QBC. The security that requests Alice cannot know what is obtained by Bob is enough. It can be seen that the security is weaker than the standard $OT_1^2$. Therefore, we call it weak quantum $OT_1^2$, and Alice attacking the weak $OT_1^2$ successfully means that she knows the content of the message obtained by Bob.

Protocol 2 is a fault-tolerant quantum $OT_1^2$ scheme with $p \leq 20\%$. When Bob does not get the correct message with a probability of $p$, whether Alice attacks successfully cannot be defined. Then, consider Alice's attack in the condition that Bob gets the correct message. When Alice replaces one of the pulses ($|\Psi_{r_c}\rangle$) with $|\Psi_0\rangle^{\perp}$ instead, the index of the fake pulse may be in Set $I$, $J$, or neither in $I$ nor $J$. If Alice does not see the index $c$ in Set $X$ or $Y$, she randomly guesses which message Bob obtains. Suppose the probability that she guesses the correct $m$ is $\frac{1}{2}p[c \notin I \wedge c \notin J]$. If Alice finds the index $c$ in Set X or Y, she believes the set which contains $c$ is Set $I$. In other words, when the index of the fake pulse in Set $I$, Alice knows Bob's choice with a large probability; when the index of the fake pulse in Set $J$, she has no choice to break the protocol. Then, Alice needs the following conditions to know the content of the message obtained by Bob.

(i) Bob accepts the fake pulse as a conclusive result.
(ii) Bob picks the index of the fake pulse into Set $I$.
(iii) Bob's measuring result of $|\Psi_0\rangle^{\perp}$ is consistent with Alice's conjecture of $r_c$.

Item (iii) ensures that Bob can obtain a correct message. Suppose the probability of the above three conditions being satisfied is $p(3con)$. The probability that Alice knows the content of the message obtained by Bob is

$$p(OT) = p(3con) + \frac{1}{2}p(c \notin I \wedge c \notin J). \tag{15}$$

The probability of Item (i) being satisfied is $p_{(i)}$. In the practical protocol, an honest Bob is supposed to obtain $Np_{con}(\mu)$ conclusive bits, where $p_{con}(\mu) = (1 - e^{-\frac{\mu}{4}})/2$ according to Equation (5).

He picks $k$ bits from the conclusive results to form Set $I$. Assume the number of conclusive result is still $Np_{con}(\mu)$. The probability that Bob accepts the fake pulse as the conclusive pulse and picks it in Set $I$ is

$$p(c \in I) = p_{(i)} \cdot \frac{C^{k-1}_{Np_{con}(\mu)-1}}{C^{k}_{Np_{con}(\mu)}} = \frac{k(2-e^{-\mu}-e^{-\frac{3\mu}{4}})}{N(1-e^{-\frac{\mu}{4}})}. \tag{16}$$

Suppose the probability that Bob measures in basis $B_0$ and gets a conclusive bit $r_c = 1$ is $p_{B_0con}(\mu)$, the probability that Bob measures in basis $B_1$ and gets a conclusive bit $r_c = 0$ is $p_{B_1con}(\mu)$. It can be seen that $p_{B_0con}(\mu) > p_{B_1con}(\mu)$. Alice knows that Bob is more likely to obtain $r_c = 1$. In the case that $c \in I$, the conditional probability that Bob accepts $r_c = 1$ is

$$\begin{aligned} p(r_c = 1|c \in I) &= \frac{p(r_c = 1|c \in I)}{p(r_c = 1|c \in I) + p(r_c = 0|c \in I)} \\ &= \frac{p_{B_0con}(\mu)}{p_{B_0con}(\mu) + p_{B_1con}(\mu)} \\ &= \frac{1-e^{-\mu}}{2-e^{-\mu}-e^{-\frac{3\mu}{4}}}. \end{aligned} \tag{17}$$

The second "=" holds because Bob randomly picks the elements of Set $I$ from his conclusive results in well-distributed. Therefore, the probability of the above three conditions being satisfied is

$$p(3con) = p(r_c = 1 \wedge c \in I) = p(r_c = 1|c \in I)p(c \in I) = \frac{k}{N} \cdot \frac{1-e^{-\mu}}{1-e^{-\frac{\mu}{4}}}. \tag{18}$$

Then, we analyze the condition that the index $c$ is neither in Set $I$ nor $J$. When Bob does not receive the fake pulse, the index $c$ is certainly not in the sets, the probability of which is $p_0(\mu) = e^{-\mu}$. When Bob receives the fake pulse, the probability that the index $c$ is not in the two sets depends on his choice of the elements in the sets. Suppose the probability that the index $c$ is not in the two sets when Bob receives the fake pulse is

$$p_1[c \notin I \wedge c \notin J] = p_{(i)}p[c \notin I \wedge c \notin J|Con] + (1-p_0(\mu)-p_{(i)})p[c \notin I \wedge c \notin J|Inc], \tag{19}$$

where $p[c \notin I \wedge c \notin J|Con]$ denotes the probability of the condition where Bob accepts the fake pulse as a conclusive result but does not choose it in Set $I$ nor $J$; $p[c \notin I \wedge c \notin J|Inc]$ denotes the probability of the condition where Bob accepts the fake pulse as an inconclusive result but does not choose it in Set $J$. Assume that Bob chooses $x$ bits of the conclusive results into Set $J$ while $k-x$ bits of the inconclusive results into Set $J$, where $0 \le x \le p_{con}(\mu)N - k$. Then, the number of conclusive results neither in Set $I$ nor $J$ is $p_{con}(\mu)N - k - x$, the number of inconclusive results not in Set $J$ is $[1-p_0(\mu)-p_{con}(\mu)]N - (k-x)$. Therefore, the probability $p_1[c \notin I \wedge c \notin J]$ is

$$\begin{aligned} &p_1[c \notin I \wedge c \notin J] \\ =&p_{(i)}\frac{p_{con}(\mu)N-k-x}{p_{con}(\mu)N} + [1-p_0(\mu)-p_{(i)}]\frac{[1-p_0(\mu)-p_{con}(\mu)]N-(k-x)}{[1-p_0(\mu)-p_{con}(\mu)]N} \\ =&1-e^{-\mu} - \frac{2+2e^{-\frac{\mu}{4}}-8e^{-\mu}+2e^{-\frac{7\mu}{4}}+2e^{-2\mu}}{(1-e^{-\frac{\mu}{4}})(1-2e^{-\mu}+e^{-\frac{\mu}{4}})}\frac{k}{N} - \frac{2(1-e^{-\mu})(1+e^{-\frac{\mu}{4}}-e^{-\frac{3\mu}{4}}-e^{-\mu})}{(1-e^{-\frac{\mu}{4}})(1-2e^{-\mu}+e^{-\frac{\mu}{4}})}\frac{x}{N}. \end{aligned} \tag{20}$$

Then, the probability that Alice attacks Protocol 2 successfully is

$$\begin{aligned} p(OT) &= p(3con) + \frac{1}{2}p_0(\mu) + \frac{1}{2}p_1[c \notin I \wedge c \notin J] \\ &= \frac{1}{2} + \frac{e^{-\mu} - e^{-\frac{5\mu}{4}} - e^{-\frac{7\mu}{4}} + e^{-2\mu}}{(1-e^{-\frac{\mu}{4}})(1-2e^{-\mu}+e^{-\frac{\mu}{4}})}\frac{k}{N} - \frac{(1-e^{-\mu})(1+e^{-\frac{\mu}{4}} - e^{-\frac{3\mu}{4}} - e^{-\mu})}{(1-e^{-\frac{\mu}{4}})(1-2e^{-\mu}+e^{-\frac{\mu}{4}})}\frac{x}{N}. \end{aligned} \tag{21}$$

When $x = \lfloor p_{con}(\mu)N - k \rfloor$, the minimum of $p(OT)$ is

$$\begin{aligned} p(OT)_{min} =& \frac{1}{2} - \frac{\left\lfloor \frac{1}{2}(1-e^{-\frac{\mu}{4}})N \right\rfloor (1-e^{-\mu})(1+e^{-\frac{\mu}{4}} - e^{-\frac{3\mu}{4}} - e^{-\mu})}{(1-e^{-\frac{\mu}{4}})(1-2e^{-\mu}+e^{-\frac{\mu}{4}})N} \\ &+ \frac{(1-e^{-\frac{3\mu}{4}})(1+e^{-\frac{\mu}{4}} - 2e^{-\frac{5\mu}{4}})}{(1-e^{-\frac{\mu}{4}})(1-2e^{-\mu}+e^{-\frac{\mu}{4}})}\frac{k}{N}. \end{aligned} \tag{22}$$

When $x = 0$, the maximum of $p(OT)$ is

$$p(OT)_{max} = \frac{1}{2} + \frac{(e^{-\mu} - e^{-\frac{5\mu}{4}} - e^{-\frac{7\mu}{4}} + e^{-2\mu})}{(1-e^{-\frac{\mu}{4}})(1-2e^{-\mu}+e^{-\frac{\mu}{4}})}\frac{k}{N}. \tag{23}$$

The minimum and the maximum probabilities that Alice attacks Protocol 2 successfully with different $\mu$ are listed in Table 2. Actually, Bob putting more index of conclusive results in Set $I$ and $J$ is beneficial for him to get more information about $b_0$ and $b_1$. Bob should prefer to select $x = \lfloor p_{con}(\mu)N - k \rfloor$. Even if Alice guesses which message Bob obtains without any trick, she has a probability of $1/2$ to get the right answer. It can be seen from Table 2 that when Bob chooses $x = \lfloor p_{con}(\mu)N - k \rfloor$, the probability that Alice breaks the $OT_1^2$ protocol is $p(OT)_{min} < 1/2$, which causes that Alice replaces one of the states with $|\Psi_0\rangle^{\perp}$ is not an effective attack. In addition, we will show in Section 5.2 that even Bob chooses $x = 0$, Alice cannot break the binding of our QBC protocol.

**Table 2.** The probabilities of Alice breaking Bob's privacy in our $OT_1^2$ protocol. $p(OT)_{min}$ and $p(OT)_{max}$ denote the maximum probabilities that Alice breaks Protocol 2 with different $\mu$ when $N = 800$.

| $\mu$ | $k$ | $p(OT)_{min}$ | $p(OT)_{max}$ |
|---|---|---|---|
| 2 | 131 | 0.4462 | 0.5129 |
| 3 | 172 | 0.4227 | 0.5070 |
| 4 | 210 | 0.4238 | 0.5034 |
| 5 | 236 | 0.4174 | 0.5015 |
| 6 | 259 | 0.4194 | 0.5007 |

#### 4.2.2. The Attack that Alice Sends All States Dishonestly in R-OT Protocol

The attack that Alice sends all states dishonestly may be detected by Bob through the different ratio of conclusive results. She should generate different proportions of different states. For example, Alice sends states in Breidbart basis to increase the proportion of Bob's conclusive (inconclusive) bits. Consider the ideal case, for $|\Psi_0\rangle = |0\rangle$ and $|\Psi_1\rangle = |\pi/6\rangle$, the states in Breidbart basis are $|\frac{\pi}{12}\rangle$ and $|\frac{7\pi}{12}\rangle$. If Alice sends the state $|\frac{\pi}{12}\rangle$ and Bob randomly chooses the measurement basis $B_0$ or $B_1$, the probability that Bob obtains a conclusive bit is

$$p_c = \frac{1}{2}\left\langle \frac{\pi}{12} \middle| \frac{\pi}{2} \right\rangle \left\langle \frac{\pi}{2} \middle| \frac{\pi}{12} \right\rangle + \frac{1}{2}\left\langle \frac{7}{12} \middle| \frac{2\pi}{3} \right\rangle \left\langle \frac{2\pi}{3} \middle| \frac{\pi}{12} \right\rangle = \frac{1}{2} - \frac{\sqrt{3}}{4}. \tag{24}$$

If Alice sends the state $|\frac{7\pi}{12}\rangle$ and Bob randomly chooses the measurement basis $B_0$ or $B_1$, the probability that Bob obtains a conclusive bit is

$$p'_c = \frac{1}{2}\left\langle \frac{7\pi}{12} \middle| \frac{\pi}{2} \right\rangle \left\langle \frac{\pi}{2} \middle| \frac{7\pi}{12} \right\rangle + \frac{1}{2}\left\langle \frac{7\pi}{12} \middle| \frac{2\pi}{3} \right\rangle \left\langle \frac{2\pi}{3} \middle| \frac{7\pi}{12} \right\rangle = \frac{1}{2} + \frac{\sqrt{3}}{4}. \tag{25}$$

It is clear that when Alice sends $|\frac{\pi}{12}\rangle$, she knows that Bob is likely to get an inconclusive bit. When Alice sends $|\frac{7\pi}{12}\rangle$, she knows that Bob is likely to get a conclusive bit. In order to ensure the ratio of the conclusive result is 1/8 according to Equation (1), Alice should set the proportion of $|\frac{\pi}{12}\rangle$ as $\frac{1}{2} + \frac{\sqrt{3}}{4}$ and the proportion of $|\frac{7\pi}{12}\rangle$ as $\frac{1}{2} - \frac{\sqrt{3}}{4}$. According to Equation (25), the ratio of state $|\frac{7\pi}{12}\rangle$ accepted as conclusive results and inconclusive results is $\frac{\frac{1}{2}+\frac{\sqrt{3}}{4}}{\frac{1}{2}-\frac{\sqrt{3}}{4}}$ in $OT_1^2$ protocol, which is around 13.9. When Alice receives the index set $X$ and $Y$, she regards the set contains more index of $|\frac{7\pi}{12}\rangle$ as the set $I$. By this attack, she can know the value of $m$ chosen by Bob with a large probability.

However, $\left\langle \frac{7\pi}{12} \middle| \frac{\pi}{2} \right\rangle \left\langle \frac{\pi}{2} \middle| \frac{7\pi}{12} \right\rangle = \left\langle \frac{7\pi}{12} \middle| \frac{2\pi}{3} \right\rangle \left\langle \frac{2\pi}{3} \middle| \frac{7\pi}{12} \right\rangle$ means that Alice has no idea about Bob's the measurement results by this attack. Bob cannot obtain the correct bit in $OT_1^2$ protocol, while Alice cannot disclose the correct $r_i$ in the opening phase of QBC protocol.

## 5. The Security of QBC

BC protocol is binding if Alice cannot change the value of $b$ after she commits and it is concealing if Bob cannot obtain $b$ before the opening phase. Protocol 3 is both physically binding and concealing in practice. We first show the concealing property.

### *5.1. Concealing of QBC*

We first analyze the ideal protocol without error and loss to prove that QBC in ideal conditions is information-theoretically concealing. Then, further consider the practical conditions.

**Theorem 1.** *Protocol 3 in ideal conditions without imperfect facilities and errors is information-theoretically concealing.*

**Proof.** According to the description of Protocol 3, it is easy to see that the relation of $r_i$, ciphertext $c_0$, $c_1$ and the commit value $b$ is

$$\bigoplus_{i=1}^{2k} r_i = c_0 \oplus c_1 \oplus b. \tag{26}$$

Suppose $\rho_{b'}^{(2k)}$ is the density operator of the whole state received by Bob when Alice commits $b$, where $b' = c_0 \oplus c_1 \oplus b$. Then

$$\rho_{b'}^{(2k)} = \frac{1}{2^{2k-1}} \sum_{\oplus_{i=1}^{2k} r_i = b'} |\Psi_{r_i}\rangle\langle\Psi_{r_i}|. \tag{27}$$

As $\langle\Psi_0|\Psi_1\rangle = \cos\varphi$, define

$$|\Psi_0\rangle = \begin{bmatrix} \cos\frac{\varphi}{2} \\ \sin\frac{\varphi}{2} \end{bmatrix}, \qquad |\Psi_1\rangle = \begin{bmatrix} \cos\frac{\varphi}{2} \\ -\sin\frac{\varphi}{2} \end{bmatrix}$$

According to the process of analysis in [62], the density operators $\rho_0^{(2k)}$ and $\rho_1^{(2k)}$ satisfy

$$\rho_0^{(2k)} - \rho_1^{(2k)} = 2 \times \begin{bmatrix} 0 & \sin\frac{\varphi}{2}\cos\frac{\varphi}{2} \\ \sin\frac{\varphi}{2}\cos\frac{\varphi}{2} & 0 \end{bmatrix}^{\otimes 2k}. \tag{28}$$

Then, trace distance is

$$D(\rho_0^{(2k)}, \rho_1^{(2k)}) = \frac{1}{2} Tr \left| \rho_0^{(2k)} - \rho_1^{(2k)} \right| = (\sin \varphi)^{2k}. \tag{29}$$

For any positive polynomial $p(\cdot)$ and every sufficiently large $n$,

$$D(\rho_0^{(2k)}, \rho_1^{(2k)}) < \frac{1}{p(n)} \tag{30}$$

holds. The theorem is proved. □

In practical QBC protocol, the commit value is $b = b_0^{(i)} \oplus b_1^{(i)}$, where $i = 1, 2, ..., l$. The $OT_1^2$ protocol is executed $l$ times. When Bob breaks Alice's privacy just once in $OT_1^2$ protocol, he knows the commit value. Some security parameters of $OT_1^2$ protocol are given is Table 1 and the probability that Bob breaks Alice's privacy $p_2$ is controlled to be a magnitude of $10^{-6}$. Suppose the times of executing $OT_1^2$ protocol in bit commitment protocol is $l = 40$, a malicious Bob can obtain what Alice has committed before opening phase with a probability of

$$p_{br} = 1 - (1 - 10^{-6})^{40} \approx 4.0 \times 10^{-5}. \tag{31}$$

In practical protocol, the probability of breaking the concealing of bit commitment around $4.0 \times 10^{-5}$ is allowed.

### *5.2. Binding of QBC*

All of Alice's attacks can be divided into two categories, i.e., without entangled states, and with entangled states.

#### 5.2.1. Attacks without Entangle States

When Alice attacks QBC protocol without entangle states, she has two different strategy. One is to attack QBC protocol directly. The other is to attack privacy for Bob of $OT_1^2$ first and knows Bob's choice $m$. Then, she changes the message $b_{m\oplus 1}^{(i)}$ in the opening phase.

The former attack for Alice is to change the values of $b_0^{(i)}$ or $b_1^{(i)}$ just in the opening phase of QBC protocol. But some of these values are known by Bob. Alice has no idea about which bits Bob obtains. Because our $OT_1^2$ is a fault-tolerant scheme, the probability that Bob can obtain a correct $b_0$ or $b_1$ successfully is $1 - p = 0.8$, which is the probability that there is no error for the key used in the decryption algorithm of $OT_1^2$ protocol and the conclusive results are enough to construct Set $I$. Bob has a probability of $p = 20\%$ of getting neither of the messages, a probability of 40% of getting the message $b_0$, and a probability of 40% of getting the message $b_1$. Therefore, if Alice randomly changes the message $b_0^{(i)}$ or $b_1^{(i)}$, her probability of being detected is 40%. Alice's commitment in Protocol 3 contains $l$ same value of $b$. A strategy for the cheating Alice is to commit "0" with the number of $\frac{l}{2}$ and commit "1" with the number of $\frac{l}{2}$ in *commit phase*, and change half of them in *opening phase*. Therefore, for $l = 40$, Alice's success probability of attacking is

$$p'_{br} = (1 - 0.4)^{20} \approx 3.6 \times 10^{-5}. \tag{32}$$

In practical protocol, the probability of breaking the binding of the bit commitment is allowed to be around $3.6 \times 10^{-5}$.

The QBC protocol is a compositional protocol, which calls the $OT_1^2$ protocol several times. In Section 4.2, we analyze the privacy for Bob of $OT_1^2$ protocol. Alice could attack by replacing one of the states with $|\Psi_0\rangle^{\perp}$. Suppose the cheating Alice commits "0" with the number of $\frac{l}{2}$ and commit "1" with the number of $\frac{l}{2}$ in *commit phase*. When Alice attacks $l/2$ rounds without detection,

she can break the binding of QBC. Bob has a probability of $p = 20\%$ getting neither of the messages. When Bob gets none of the correct messages, Alice can change one of the messages without being detected. When Bob gets one of the messages, the probability that Alice attacks without detection is not greater than $p(OT) = p(3con) + \frac{1}{2}p_0(\mu) + \frac{1}{2}p_1\,[c \notin I \wedge c \notin J]$. The reason is that when the index $c$ is neither in Set $I$ nor $J$, it is possible that the fake state $|\Psi_0\rangle^{\perp}$ is accepted as a conclusive bit and Alice discloses an inconsistent result in *opening phase* of QBC. The probability that Alice attacks one round without being detected is

$$\begin{aligned} & p(1round) \\ \leq & p + (1-p)p(OT) \\ = & \frac{1}{2} + \frac{e^{-\mu} - e^{-\frac{5\mu}{4}} - e^{-\frac{7\mu}{4}} + e^{-2\mu}}{(1-e^{-\frac{\mu}{4}})(1-2e^{-\mu}+e^{-\frac{\mu}{4}})}\frac{k}{N} - \frac{(1-e^{-\mu})(1+e^{-\frac{\mu}{4}}-e^{-\frac{3\mu}{4}}-e^{-\mu})}{(1-e^{-\frac{\mu}{4}})(1-2e^{-\mu}+e^{-\frac{\mu}{4}})}\frac{x}{N}. \end{aligned} \tag{33}$$

When Alice attacks $OT_1^2$ protocol and changes $b_0$ or $b_1$ in *opening phase* of QBC, the probability that the attack is not detected by Bob is

$$p(BC) = [p(1round)]^{l/2}. \tag{34}$$

When Bob selects none of conclusive results into Set $J$, the maximum probability of attacking is

$$p(BC)_{max} = [p(1round)_{max}]^{l/2} = [p + (1-p)p(OT)_{max}]^{l/2}, \tag{35}$$

which are listed in Table 3. Alice has the maximum probability of attacking the binding of QBC protocol with magnitudes of $10^{-5}$, which is allowed in practice.

**Table 3.** The maximum probabilities of Alice breaking the binding of QBC protocol by replacing one state of $|\Psi_0\rangle^{\perp}$ with different $\mu$ when $N = 800$.

| $\mu$ | $k$ | $p(1round)_{max}$ | $p(BC)_{max}$ |
|---|---|---|---|
| 2 | 131 | 0.6103 | $5.1 \times 10^{-5}$ |
| 3 | 172 | 0.6056 | $4.4 \times 10^{-5}$ |
| 4 | 210 | 0.6027 | $4.0 \times 10^{-5}$ |
| 5 | 236 | 0.6012 | $3.8 \times 10^{-5}$ |
| 6 | 259 | 0.6005 | $3.7 \times 10^{-5}$ |

5.2.2. Attack with Entangle States

The entanglement generation and control [63–66] are the preconditions of the attack with entangle states. Then, we analyze this kind of attacks. In Protocol 1, the states are generated by Alice and sent to Bob. After sending the states, if Alice does not perform the EPR type attack, she can do nothing with the outgoing states. If she prepares entangled states and sends a part of them to Bob, she tries to find the local unitary transformation to change the value of commitment, which is actually the no-go theorem attack.

When Alice commits "0" or "1", she prepares

$$|0\rangle = \sum_{i=1}^{2k} \alpha_i |e_i\rangle_A \otimes |\Psi_{r_i}\rangle_B, \quad |1\rangle = \sum_{j=1}^{2k} \beta_i |e'_j\rangle_A \otimes |\Psi_{r_j}\rangle_B, \tag{36}$$

respectively, where

$$\bigoplus_{i=1}^{2k} r_i = c_0 \oplus c_1, \quad \bigoplus_{j=1}^{2k} r_j = c_0 \oplus c_1 \oplus 1, \tag{37}$$

If Alice wants to change the value of commitment from "0" to "1", she needs to get state $|\nu\rangle$ with the same reduced density operator as $|0\rangle$, which satisfies $|\langle 1|\nu\rangle| = F(\rho_0^{2k}, \rho_1^{2k}) = 1 - \delta$. Then, she must find out the unitary transformation acting on A alone to transform $|0\rangle$ into $|\nu\rangle$. The calculation of unitary transformation is presented in Appendix A. As $|\nu\rangle$ and $|1\rangle$ are so similar, Bob can hardly detect the cheating Alice.

However, according to Appendix A, the no-go theorem attack algorithm's time complexity is $O(2^{3n})$, besides, this algorithm needs at least $O(2^{2n})$ size of memory space to store the matrix. The entry number of matrix $U_A$ is $2^{2k} \times 2^{2k}$, according to Table 1 this number is greater than the number of protons on the earth. It means that Alice is unable to get the matrix in practice, and the storage time of quantum states is limited. The bit commitment could be executed over a period of time to prevent Alice from applying transformation with the other part of entanglement states. Therefore, in practice Alice can hardly attack the binding of the bit commitment protocol with this method. Therefore, our protocol achieves the physical security defined in Section 1.

## 6. Discussions

In this paper, we analyze the situation where the protocols are executed on an atmospheric window with a high efficiency detector of 80%. If a malicious Bob has a greater ability to obtain information near Alice's site and has a super channel, the transfer efficiency could be 100%. To defend the attack, the product of the efficiency of transfer and an honest Bob's detector $\eta_C\eta_D$ should be increased to 80%.

If we execute the protocols in optical fiber, the bit commitment protocol can be realized between two parties with a long distance. For a malicious Bob who uses photon number splitting attack and has a detector with an efficiency less than $\eta_D/80\%$, the analysis and security of the protocol also hold. It means that our protocols can probably be applied over a long distance in the future.

We considered another construction of quantum bit commitment protocol. In quantum R-OT protocol, Bob prepares a random qubit string $|\Phi_1\rangle, ..., |\Phi_n\rangle$ and sends it to Alice, where $|\Phi_i\rangle \in \{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$. Alice generates random bit string $(r_1, ..., r_N) \in \{0,1\}^N$. When $r_i = 0$, she keeps the ith qubit unchanged and sends it back to Bob; when $r_i = 1$, she rotates the state along y axis with $\frac{\pi}{6}$, and sends the qubit back to Bob, that is

$$\begin{cases} r_i = 0, \ |\Phi_i\rangle \longrightarrow |\Phi_i\rangle, \\ r_i = 1, \ |\Phi_i\rangle \longrightarrow |\Phi_i + \frac{\pi}{6}\rangle. \end{cases}$$

Bob chooses $B_0$ or $B_1$ randomly to measure the pulses coming from Alice, where $|\Psi_0\rangle = |\Phi_i\rangle$ and $|\Psi_1\rangle = |\Phi_i + \frac{\pi}{6}\rangle$. From these receiving pulses, if and only if his measurement results in state $|\Psi_x\rangle^{\perp}$, he accepts a pulse as a conclusive pulse and takes the bit value of this pulse as $x \oplus 1$.

When attacking the quantum bit commitment protocols by no-go theorem, Alice usually prepares states as $|0\rangle = \Sigma_i \alpha_i |e_i\rangle_A \otimes |\phi_i\rangle_B$ and $|1\rangle = \Sigma_j \beta_j |e'_j\rangle_A \otimes |\phi'_j\rangle_B$. Then, she keeps the first register herself and sends the second register to Bob. Only by Alice's local unitary transformation, she can cheat by changing the value of the commit bit $b$ in *opening phase*. In the protocol above, the quantum states are prepared by Bob and Alice has no original states. However, when she rotates the coming states, she can make the operation as a controlled unitary transformation. The control bit in the transformation is entangled with the other register. Similarly, Alice can cheat by local unitary transformation on the other register. The construction above actually is not beyond the no-go theorem and increase the complexity of the practical system. Therefore, we construct a more practical and easier protocol in Section 3.

## 7. Conclusions

Based on two non-orthogonal states, we construct a practical quantum R-OT protocol. Afterwards we construct a one-out-of-two oblivious transfer protocol based on the quantum R-OT protocol. Finally,

we present a bit commitment protocol based on the one-out-of-two protocol. The security of concealing is kept by the measurement hypothesis and superposition principle of state in quantum mechanics. The binding of the bit commitment protocol is physically secure. By using weak coherent pulses and allowing some errors, our protocols can be applied in practice. With the advent of the higher efficiency detectors in optical fiber, our protocol can be realized with a long distance.

**Author Contributions:** L.Y. designed the research and the architecture of the protocols. Y.S. wrote the manuscript and gave security analysis. Authors have read and approved the final manuscript.

**Funding:** This research was funded by National Natural Science Foundation of China under Grant No. 61672517 and National Cryptography Development Fund under Grant No. MMJJ20170108.

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

## Appendix A. Alice's Attack for Binding of QBC

1. The Schmidt decomposition of $|0\rangle$, $|1\rangle$ and the polar decomposition of $\sqrt{\rho_1^B}\sqrt{\rho_0^B}$

For the entangled states prepared by Alice, there is an orthogonal basis set of $2k$ dimensions for subsystems $A$ and $B$. Therefore, $|0\rangle$ can be written as

$$|0\rangle = \sum_{i,j} \theta_{ij} |i\rangle_A \otimes |j\rangle_B, \tag{A1}$$

where $i, j \in \{0, 1, ..., 2^{2k} - 1\}$, and

$$\theta_{ij} = \sum_l \alpha_{lA} \langle i|e_l\rangle_{AB} \langle j|\Psi_{r_l}\rangle_B. \tag{A2}$$

The entries $\theta_{ij}$ compose $2^{2k} \times 2^{2k}$ matrix $\Theta$. $\Theta$ can be decomposed by the singular value decomposition as $\Theta = UDV$, where $D$ is a diagonal matrix with positive elements, and $U$ and $V$ are unitary matrices.

$$|0\rangle = \sum_{i,j,l} u_{il} d_{ll} v_{lj} |i\rangle_A \otimes |j\rangle_B. \tag{A3}$$

Define $|x_l\rangle_A = \sum_i u_{il}|i\rangle_A$, $|y_l\rangle_B = \sum_j v_{lj}|j\rangle_B$, and $\lambda_l = d_{ll}$, the state $|0\rangle$ becomes

$$|0\rangle = \sum_l \lambda_l |x_l\rangle_A \otimes |y_l\rangle_B, \tag{A4}$$

where $\{|x_l\rangle_A\}$, $\{|y_l\rangle_B\}$ form two orthogonal basis sets. Similarly,

$$|1\rangle = \sum_l \lambda'_l |x'_l\rangle_A \otimes |y'_l\rangle_B. \tag{A5}$$

For $\rho_1^B$ and $\rho_0^B$, the related polar decomposition is

$$\sqrt{\rho_1^B}\sqrt{\rho_0^B} = \left|\sqrt{\rho_1^B}\sqrt{\rho_0^B}\right| T. \tag{A6}$$

There is an orthogonal basis set with which $\rho_0^B$ and $\rho_1^B$ are in block-diagonal form [62] and blocks have a general expression, so that we can give the entries of matrix $T$ based on this orthogonal basis.

2. Solving $U_A$. Based on the proof of Uhlmann's theorem given by Jozsa [67], we have

$$|\nu\rangle = \left(I \otimes \sqrt{\rho_0^B} T^\dagger\right) \sum_i |x'_i\rangle_A \otimes |y'_i\rangle_B. \tag{A7}$$

It can be seen that there is a local unitary transformation $U_A$ for Alice to transform $|0\rangle$ into $|\nu\rangle$. According to Equation (A4), $\rho_0^B = \sum_i |\lambda_i|^2 |y_i\rangle_{BB}\langle y_i|$, it gives

$$\begin{aligned} |\nu\rangle &= \left(I \otimes \sqrt{\rho_0^B} T^\dagger\right) \sum_i |x_i'\rangle_A \otimes |y_i'\rangle_B \\ &= \sum_{i,j} |x_i'\rangle_A \otimes \lambda_j |y_j\rangle_{BB}\langle y_j| T^\dagger |y_i'\rangle_B \\ &= \sum_j \lambda_j \left(\sum_i {}_B\langle y_j| T^\dagger |y_i'\rangle_B |x_i'\rangle_A\right) \otimes |y_j\rangle_B. \end{aligned} \tag{A8}$$

It can be seen that

$$U_A |x_j\rangle = \sum_i {}_B\langle y_j| T^\dagger |y_i'\rangle_B |x_i'\rangle_A. \tag{A9}$$

Then, Alice can get all elements of $U_A$ from this equation.

## References


1. Crépeau, C.; Kilian, J. Achieving oblivious transfer using weakened security assumptions. In Proceedings of the IEEE 29th Symposium on Foundations of Computer Science (FOCS'88), White Plains, NY, USA, 24–26 October 1988; pp. 42–52.
2. Bennett, C.; Brassard, G.; Crépeau, C.; Skubiszewska, M.H. Practical quantum oblivious transfer. In Proceedings of the Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'91), Santa Barbara, CA, USA, 11–15 August 1991; pp. 351–366.
3. Crépeau, C. Quantum oblivious transfer. *J. Mod. Opt.* **1994**, *41*, 2445–2454.
4. Brassard, G.; Crépeau, C.; Jozsa, R.; Langlois, D. A quantum bit commitment scheme provably unbreakable by both parties. In Proceedings of the IEEE 34th Symposium on Foundations of Computer Science (FOCS'93), Palo Alto, CA, USA, 3–5 November 1993; pp. 362–371.
5. Yao, A.C.C. Security of quantum protocols against coherent measurements. In Proceedings of the 27th Annual ACM Symposium on Theory of computing, Las Vegas, Nevada, USA, 29 May–1 June 1995; pp. 67–75.
6. Mayers, D. The trouble with quantum bit commitment. *arXiv* **1996**, arXiv:9603015.
7. Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **1997**, *78*, 3414–3417.
8. Lo, H.K.; Chau, H.F. Is quantum bit commitment really possible? *Phys. Rev. Lett.* **1997**, *78*, 3410–3413.
9. Brassard, G.; Crépeau, C.; Mayers, D.; Salvail, L. A brief review on the impossibility of quantum bit commitment. *arXiv* **1997**, arXiv:9712023.
10. Bub, J. The quantum bit commitment theorem. *Found. Phys.* **2001**, *31*, 735–756.
11. Cheung, C.Y. Insecurity of quantum bit commitment with secret parameters. *arXiv* **2000**, arXiv:0601206.
12. 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.
13. Magnin, L.; Magniez, F.; Leverrier, A.; Cerf, N.J. Strong no-go theorem for Gaussian quantum bit commitment. *Phys. Rev. A* **2010**, *81*, 010302.
14. Chailloux, A.; Kerenidis, I. Optimal bounds for quantum bit commitment. In Proceedings of the IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS 2011), Palm Springs, CA, USA, 22–25 October 2011; pp. 354–362.
15. Li, Q.; Li, C.; Long, D.; Chan, W.H.; Wu, C. On the impossibility of non-static quantum bit commitment between two parties. *Quantum Inf. Process.* **2012**, *11*, 519–527.
16. Chiribella, G.; D'Ariano, G.M..; Perinotti, P.; Schlingemann, D.; Werner, R. A short impossibility proof of quantum bit commitment. *Phys. Lett. A* **2013**, *377*, 1076–1087.
17. Lo, H.K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154.
18. Salvail, L.; Schaffner, C.; Sotakova, M. On the power of two-party quantum cryptography. In Proceedings of the 15th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT 2009), Tokyo, Japan, 6–10 December 2009; pp. 70–87.

19. Unruh, D. Universally composable quantum multi-party computation. In Proceedings of the 30th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO 2010), Santa Barbara, CA, USA, 15–19 August 2010; pp. 486–505.
20. Buhrman, H.; Christandl, M.; Schaffner, C. Complete insecurity of quantum protocols for classical two-party computation. *Phys. Rev. Lett.* **2012**, *109*, 160501.
21. Kent, A. Unconditionally secure bit commitment. *Phys. Rev. Lett.* **1999**, *83*, 1447–1450.
22. Kent, A. Secure classical bit commitment using fixed capacity communication channels. *J. Cryptol.* **2005**, *18*, 313–335.
23. Kent, A. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.* **2012**, *109*, 130501.
24. Adlam, E.; Kent, A. Device-independent relativistic quantum bit commitment. *Phys. Rev. A* **2015**, *92*, 022315.
25. Lunghi, T.; Kaniewski, J.; Bussieres, F.; Houlmann, 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.
26. 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.
27. Tanaka, K. Quantum bit-commitment for small storage based on quantum one-way permutations. *New Gener. Comput.* **2003**, *21*, 339–345.
28. Chailloux, A.; Iordanis, K.; Bill, R. Quantum commitments from complexity assumptions. In Proceedings of the 38th International Colloquium on Automata, Languages, and Programming (ICALP 2011), Zurich, Switzerland, 4–8 July 2011; pp. 73–85.
29. Unruh, D. Computationally Binding Quantum Commitments. In Proceedings of the 35th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT 2016), Vienna, Austria, 8–12 May 2016; pp. 497–527.
30. Damgard, I.; Fehr, S.; Salvail, L.; Schaffner, C. Cryptography in the bounded quantum-storage model. *SIAM J. Comput.* **2008**, *37*, 1865–1890.
31. Damgard, I.; Desmedt, Y.; Fitzi, M.; Nielsen, J.B. Secure protocols with asymmetric trust. In Proceedings of the 13th Annual International Cryptology Conference on Advances in Cryptology (ASIACRYPT 2007), Kuching, Malaysia, 2–6 December 2007; pp. 357–375.
32. Wehner, S.; Schaffner, C.; Terhal, B. Practical cryptography from noisy storage. *Phys. Rev. Lett.* **2008**, *100*, 220502.
33. Ng, N.H.Y.; Joshi, S.K.; Ming, C.C.; Kurtsiefer, C.; Wehner, S. Experimental implementation of bit commitment in the noisy-storage model. *Nat. Commun.* **2012**, *3*, 1326.
34. Konig, R.; Wehner, S.; Wullschleger, J. Unconditional security from noisy quantum storage. *IEEE Trans. Inf. Theory* **2012**, *58*, 1962–1984.
35. Danan, A.; Vaidman, L. Practical quantum bit commitment protocol. *Quantum Inf. Process.* **2012**, *11*, 769–775.
36. Hardy, L.; Kent, A. Cheat sensitive quantum bit commitment. *Phys. Rev. Lett.* **2004**, *92*, 157901.
37. Buhrman, H.; Christandl, M.; Hayden, P.; Lo, H.K.; Wehner, S. Possibility, impossibility, and cheat sensitivity of quantum-bit string commitment. *Phys. Rev. A* **2008**, *78*, 022316.
38. Li, Y.B.; Wen, Q.Y.; Li, Z.C.; Qin, S.J.; Yang, Y.T. Cheat sensitive quantum bit commitment via pre- and post-selected quantum states. *Quantum Inf. Process.* **2014**, *13*, 141–149.
39. He, G.P. Security bound of cheat sensitive quantum bit commitment. *Sci. Rep.* **2015**, *5*, 9398.
40. Zhou, L.; Sun, X.; Su, C.; Liu, Z.; Choo, K.K.R. Game theoretic security of quantum bit commitment. *Inf. Sci.* **2018**, doi:10.1016/j.ins.2018.03.046.
41. He, G.P. Quantum key distribution based on orthogonal states allows secure quantum bit commitment. *J. Phys. A* **2011**, *44*, 445305.
42. He, G.P. Simplified quantum bit commitment using single photon nonlocality. *Quantum Inf. Process.* **2014**, *13*, 2195–2211.
43. He, G.P. Unconditionally secure quantum bit commitment using infinite-dimensional systems. *arXiv* **2017**, arXiv:1709.01396.
44. Yuen, H.P. An unconditionally secure quantum bit commitment protocol. *arXiv* **2012**, arXiv:1212.0938.
45. Cheung, C.Y. Quantum bit commitment using wheeler's delayed choice experiment. *arXiv* **2015**, arXiv:1504.05551.

46. Srikanth, R. Quantum bit commitment and the reality of the quantum state. *Found. Phys.* **2018**, *48*, 92–109.
47. Yang, L.; Xiang, C.; Li, B. Quantum-string-based bit commitment protocols with physical security. *arXiv* **2010**, arXiv:1011.5099.
48. Yang, L. Bit commitment protocol based on random oblivious transfer via quantum channel. *arXiv* **2013**, arXiv:1306.5863.
49. Mirza, I.M.; van Enk, S.J.; Kimble, H.J. Single-photon time-dependent spectra in coupled cavity arrays. *JOSA B* **2013**, *30*, 2640–2649.
50. Cui, G.; Raymer, M.G. Emission spectra and quantum efficiency of single-photon sources in the cavity-QED strong-coupling regime. *Phys. Rev. A* **2006**, *73*, 053807.
51. Lo, H.K.; Curty, M.; Tamaki, K. Secure quantum key distribution. *Nat. Photonics* **2014**, *8*, 595.
52. Mirza, I.M.; Schotland, J.C. Influence of disorder on electromagnetically induced transparency in chiral waveguide quantum electrodynamics. *JOSA B* **2018**, *35*, 1149–1158.
53. Mirza, I.M.; Hoskins, J.G.; Schotland, J.C. Chirality, band structure, and localization in waveguide quantum electrodynamics. *Phys. Rev. A* **2017**, *96*, 053804.
54. Marsili, F.; Verma V.B.; Stern, J.A.; Harrington, S.; Lita, A.E.; Gerrits, T.; Vayshenker, I.; Baek, B.; Shaw, M.D.; Mirin, R.P.; et al. Detecting single infrared photons with 93% system efficiency. *Nat. Photonics* **2013**, *7*, 210.
55. Takesue, H.; Dyer, S.D.; Stevens, M.J.; Verma, V.; Mirin, R.P.; Nam, S.W. Quantum teleportation over 100 km of fiber using highly efficient superconducting nanowire single-photon detectors. *Optica* **2015**, *2*, 832–835.
56. Ivanovic, I.D. How to differentiate between non-orthogonal states. *Phys. Lett. A* **1987**, *123*, 257–259.
57. Peres, A. How to differentiate between non-orthogonal states. *Phys. Lett. A* **1988**, *128*, 119.
58. Huttner, B.; Muller, A.; Gautier, J.D.; Zbinden, H.; Gisin, N. Unambiguous quantum measurement of nonorthogonal states? *Phys. Rev. A* **1996**, *54*, 3783–3789.
59. Crépeau, C. Equivalence between Two Flavours of Oblivious Transfers. In Proceedings of the Annual International Cryptology Conference on Advances in Cryptology (CRYPTO'87), Santa Barbara, CA, USA, 16–20 August 1987; Springer: Berlin/Heidelberg, Germnay, 1987; pp. 350–354.
60. Yang, L.; Li, Z. One-way information reconciliation schemes of quantum key distribution. *arXiv* **2012**, arXiv:1201.1196
61. He, G.P.; Wang, Z.D. The relationship between two flavors of oblivious transfer at the quantum level. *Phys. Rev. A* **2006**, *73*, 044304.
62. Bennett, C.; Mor, T.; Smolin, J. Parity bit in quantum cryptography. *Phys. Rev. A* **1996**, *54*, 2675–2684.
63. Armata, F.; Calajo, G.; Jaako, T.; Kim, M.S.; Rabl, P. Harvesting multiqubit entanglement from ultrastrong interactions in circuit quantum electrodynamics. *Phys. Rev. Lett.* **2017**, *119*, 183602.
64. Paulisch, V.; Kimble, H.J.; Gonzalez-Tudela, A. Universal quantum computation in waveguide QED using decoherence free subspaces. *New J. Phys.* **2016**, *18*, 043041.
65. Xia, K.; Twamley, J. Generating spin squeezing states and Greenberger-Horne-Zeilinger entanglement using a hybrid phonon-spin ensemble in diamond. *Phys. Rev. B* **2016**, *94*, 205118.
66. Gonzalez-Ballestero, C.; Moreno, E.; Garcia-Vidal, F.J. Generation, manipulation, and detection of two-qubit entanglement in waveguide QED. *Phys. Rev. A* **2014**, *89*, 042328.
67. Jozsa, R.; Schumacher, B. A new proof of the quantum noiseless coding theorem. *J. Mod. Opt.* **1994**, *41*, 2343–2349.