sensors

MDPI

Article

Measurement-Device-Independent Two-Party Cryptography with Error Estimation

Zishuai Zhou [1,†], Qisheng Guang [1,†], Chaohui Gao [1], Dong Jiang [1,2] and Lijun Chen [1,*]

[1] State Key Laboratory for Novel Software Technology, Nanjing University, Nanjing 210046, China; mf1833107@smail.nju.edu.cn (Z.Z.); mg1733016@smail.nju.edu.cn (Q.G.); dz1833008@smail.nju.edu.cn (C.G.); jiangd@nju.edu.cn (D.J.)

[2] School of Internet, Anhui University, Hefei 230039, China

* Correspondence: chenlj@nju.edu.cn

† These authors contributed equally to this work.

Received: 26 September 2020; Accepted: 4 November 2020; Published: 7 November 2020

Abstract: We present an innovative method for quantum two-party cryptography. Our protocol introduces joint measurement and error estimation to improve the security of two-party cryptographic protocols. Our protocol removes the assumption of the attacker's limited power and catches the attacking actions through highly estimated bit error rate. Our protocol is formally proved to be secure against both eavesdroppers and dishonest communication parties. We also utilize our designed protocol to construct two specific two-party cryptographic applications: Quantum bit commitment and quantum password identification.

Keywords: quantum; two-party cryptography; measurement-device-independent

1. Introduction

Two-party cryptographic protocol is a significant branch of modern cryptography. It can realize communication between mutually distrustful parties [1–3]. However, the advent of a quantum computer will pose a huge threat to cryptographic protocols that originally rely on computational complexity. Fortunately, Bennett and Brassard proposed the first quantum cryptographic protocol in 1984, known as BB84 quantum key distribution (QKD) protocol [1]. BB84 protocol allows two mutually trusted parties to generate identical secret keys for encryption. Quantum cryptography, laying its foundation on quantum mechanics, can provide unconditional security in the communication process. Therefore, studies over quantum cryptography have aroused worldwide attention.

While QKD has gained extensive concern nowadays, researchers also consider introducing quantum technology into two-party cryptographic protocols. However, Lo and Mayers independently demonstrated that unconditionally secure two-party cryptographic protocol does not exist without restricting the attacker's ability [4–7]. Therefore, a perfect two-party cryptographic protocol is more difficult to be realized than key distribution. Even so, several solutions were proposed to seek more secure quantum two-party cryptographic schemes, among which there are mainly three types. The first solution introduces the relativity theory to restrain attacker's behavior [3,8–10]. The second solution weakens the demand for security. In other words, it gives up the pursuit of perfect security and allows the attacker's behavior to succeed with negligible probability. The most representative example is the cheat-sensitive quantum bit commitment (CSQBC) protocol [11–14]. The third solution is limiting the attacker's power to current technologies. For example, in 2005, Damgård demonstrated secure two-party cryptography under the assumption that the attacker's capability of storing quantum states was limited. In this so-called bounded storage model [15,16], the attacker is equipped with perfect quantum storage, but the storage capacity is limited because of unaffordable cost. Later, Schaffner

extended the model to the noisy storage model [2,17], where the attacker possesses quantum storage with unlimited capacity, but the noise increases over time.

Although Konig manifested secure two-party cryptographic protocols are feasible under noisy bounded model [2,17], we are still interested in designing two-party cryptographic protocols when the attacker possesses perfect quantum storage inspired by He's work [18]. We have discovered that two-party cryptographic protocols, like bit commitment, oblivious transfer, in Ref. [2,11,17] do not have the process of error estimation, which serves as a significant indicator of eavesdropping attack in QKD. The reasons are obvious: For one thing, the communication parties do not trust each other and for another, the information is asymmetric between parties during the communication process.

Inspired by the foundations of measurement-device-independent QKD (MDI-QKD) [19–21] and phase-matching QKD (PM-QKD) [22,23], we make it possible to introduce error estimation into two-party cryptographic protocols. In the QKD process, once there is an eavesdropper, the final key error rate will exceed the upper limit. Therefore, in encrypted communication between the two parties, if one party is dishonest, the information they previously negotiated will also have a higher error rate, which is difficult in avoiding detection by another party. In MDI-QKD, the measurement stage is independent of the final key. This de-emphasizes the assumptions for the attacker's quantum memory and enables us to discover the attacker by the increased quantum bit error rate during the estimation process.

In this paper, we introduce joint measurement method in MDI-QKD and PM-QKD, and error estimation into two-party cryptographic protocols, and raise our improved weak string erasure (WSE) protocol and 1-2 random oblivious transfer (ROT) protocol. These two protocols are significant for other TPC (two-party cryptographic protocols) applications. Compared with existing WSE and 1-2 ROT protocol, our protocol does not make any assumption on the attacker's devices. Instead, we restrict the attacking behavior by the protocol itself, which offers greater security. In our protocol, the honest party does not need quantum storage devices and the devices are compatible with mainstream QKD platforms.

The paper is organized as follows. Section 2 introduces the foundations of our research. Section 3, and Section 4 discuss our proposed WSE and 1-2 ROT respectively, and demonstrate their security. In Section 5, we probe into applications of two-party cryptographic protocols and propose two important practices, quantum bit commitment and password-based identification. Finally, the paper ends with a conclusion.

2. Preliminaries

This section will introduce several fundamental concepts to our research, including entropy qualities, joint measurement, error estimation, and privacy amplification.

This paper follows the notations in Ref. [2], using $[n] := \{1, 2, ..., n\}$ for the set of nature number, and $2^{[n]} := \{\mathcal{S} | \mathcal{S} \subseteq [n]\}$ is the set of all possible subsets of $[n]$.

2.1. Entropy Qualities

Here, we present some crucial entropy qualities for our security proof. Bulleted lists look like this:

Definition 1 (Shannon entropy)**.** *$P(X)$ is the probability distribution function of a random variable X. The entropy $H(X)$ is defined as:*

$$\mathrm{H(X)} = -\sum_{\mathrm{X}} \mathrm{P(x)log_2P(x)}.$$

As same as Ref. [2,19], we define guessing probability:

$$\mathrm{p_{guess}(X|E)} = \max_{\mathrm{M_x}} \sum_{\mathrm{x}} \mathrm{P_X(x)Tr(M_x\rho_E^x)},$$

where $\mathrm{p_{guess}(X|E)}$ is the probability of guessing X when given register E, and its maximization is over all positive operate-valued measurements (POVMs) $\{M_x\}$ acting on register E. Then we can easily get that the conditional min-entropy of X given E is:

$$\mathrm{H_{min}(X|E)} = -\mathrm{log_2 p_{guess}(X|E)},$$

and also the definition of conditional smooth min-entropy is:

$$\mathrm{H_{min}}^{\varepsilon}(X|Y) = \max_{\mathcal{E}} \mathrm{H_{min}}(X\mathcal{E}|Y),$$

where for any event $\mathcal{E}$, we have:

$$\mathrm{p_{guess}}(X\mathcal{E}|Y) = \sum_{\mathrm{y}} \mathrm{P_Y(y)} \max_{x} \mathrm{P}_{X\mathcal{E}|Y}(x|y).$$

Next, we discuss min-entropy-splitting lemma used in Ref. [2,17] for the security proof of 1-2 ROT and WSE protocol.

Lemma 1 (Entropy splitting [2,17])**.** *Let $\varepsilon \geq 0$, and $\mathrm{X_1, X_2, \ldots, X_m}$ and Z are random variables subjected to $\mathrm{H}^{\varepsilon}_{\min}(X_i X_j|Z) \geq \alpha$ $(i \neq j)$. There exists a random variable $V \subseteq \{1, \ldots, m\}$ such that for any independent random variable $W \subseteq \{1, \ldots, m\}$ with $H_{\min}(W) \geq 1$,*

$$\mathrm{H}^{2m\varepsilon}_{\min}(X_W|VWZ, V \neq W) \geq \frac{\alpha}{2} - \log_2(m) - 1.$$

Lemma 2 (Min-entropy splitting [2,17])**.** *Let $\varepsilon \geq 0$, and X_0, X_1, and Z are random variables subjected to $\mathrm{H}^{\varepsilon}_{\min} \geq \alpha$. Then there exists a random variable $D \in \{0, 1\}$, such that:*

$$\mathrm{H}^{\varepsilon}_{\min}(X_D|DZ) \geq \frac{\alpha}{2} - 1.$$

Finally, we introduce quantum uncertainty relation as the core of security proof for our redesigned protocol.

Theorem 1 (Quantum uncertainty relation [24])**.** *Suppose Q is an arbitrary fixed n-qubit state, and θ is a random basis ($\theta \in_R \{0, 1\}$), and $X \in_R \{0, 1\}^n$ is a random variable for the outcome of measuring Q in basis θ^n, then it has $\delta > 0$, and the conditional smooth min-entropy has a lower bound such that:*

$$\mathrm{H}^{\varepsilon}_{\min}(X|\theta^n) \geq (\frac{1}{2} - 2\delta)n.$$

Here,

$$\varepsilon = 2\mathrm{exp}\left(-\frac{(\frac{\delta}{4})^2}{32(2 + log_2 \frac{4}{\delta})^2}\right).$$

2.2. Joint Measurement

Joint measurement and phase-matching are widely used in QKD, and we introduce them to our two-party cryptographic protocol. Next, we explain these two methods.

Prior to 2012, most quantum cryptographic protocols, including QKD and many two-party cryptography protocols, used single-state measurement. The earliest application of joint measurement to quantum protocols is introduced by Hoi-Kwong Lo [19]. In Ref. [19], he presented the idea of MDI-QKD using joint measurement. The measurement method is shown in Figure 1.

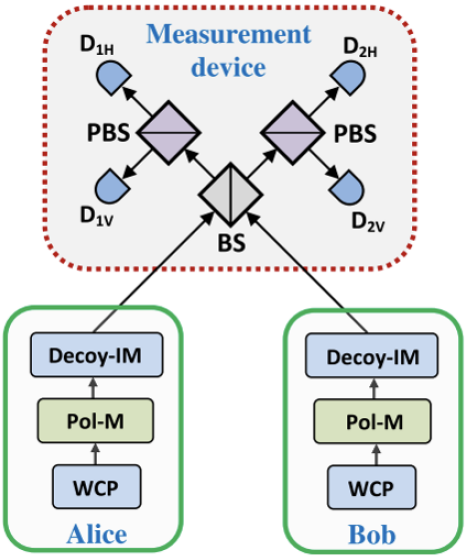

Figure 1. The basic setup of a measurement-device-independent QKD (MDI-QKD) protocol is in Ref. [19]. Alice and Bob use three devices to prepare their photons, and the third party will make a joint measurement and announce measurement output.

In Figure 1, Alice and Bob will prepare a single quantum state and send it to the third party, Charlie. Charlie will measure those quantum states in Bell basis. The state $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|HV\rangle - |VH\rangle)$ is joint by a click in D_{1H} and D_{2V} or D_{1V} and D_{2H}, and $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|HV\rangle + |VH\rangle)$ is joint by a click in D_{1H} and D_{1V} or D_{2H} and D_{2V}. Therefore, Alice and Bob can get the raw key based on measurement outcomes and prepared basis, which is shown in Table 1.

Table 1. Alice or Bob flip their key based on the outcomes of measurement and announced prepared basis [19].

Alice & Bob Basis	Relay Output $\|\phi^-\rangle$	Relay Output $\|\phi^+\rangle$
$+$	Bit flip	Bit flip
$\times$	Bit flip	No bit flip

Another joint measurement method uses phase coding, which is generally used in the continuous variable QKD. The representative protocols are PM-QKD [22] and TF-QKD [23]. The measurement method is shown in Figure 2. Phase-matching QKD uses coherent state to send information. We define that $\delta_a = |\sqrt{\mu_a}e^{i(\phi_a+\pi k_a)}\rangle$ and $\delta_b = |\sqrt{\mu_b}e^{i(\phi_b+\pi k_b)}\rangle$, where $\phi_a, \phi_b \in \{0, \frac{\pi}{2}\}$ are the basis phase chosen by Alice and Bob.

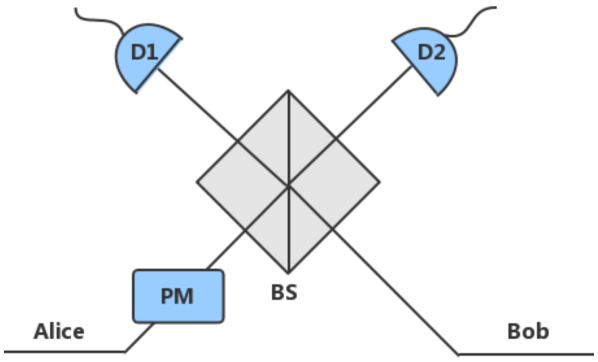

Figure 2. Mesurement setup used in phase-matching QKD (PM-QKD).

According to Mach–Zehnder interference, the detector D_1 clicks when the phase difference of δ_a and δ_b is an even multiple of π, and the detector D_2 clicks when the phase difference of δ_a and δ_b is an odd multiple of π. When a phase difference of δ_a and δ_b is not a multiple of π, a random click occurs. Bob will flip his key when detector D_2 click because only $|k_a - k_b| = 1$ will cause the phase difference to be an odd multiple of π.

2.3. Error Estimation

Error estimation is one of the most important methods to ensure security in quantum cryptographic protocols. However, so far, in the two-party quantum encryption protocol, no method to improve the security of the protocol by error estimation has been seen. This is due to the asymmetry of the information in the two-party encryption protocols and the coupling between the measurement results and final key. We find that joint measurement reduces this coupling and try to introduce the error estimation method into the two-party encryption protocol. In this paper, because of the asymmetry of the information, we use the random sampling method for error estimation.

In QKD, the operation process of the random sampling method can be described as follows: Among the raw key $(k_0, \ldots, k_{l-1})_A$ and $(k_0, \ldots, k_{l-1})_B$ owned by Alice and Bob, randomly extract a certain percentage p of the key at the corresponding positions and publishing these bits through the classical channel with trusted authentication. The inconsistency rate of the sampling key can be regarded as the code error rate of the raw key (since the extracted key has been published, it cannot be used in subsequent processing steps and needs to be discarded). In the two-party quantum cryptographic protocol, due to the asymmetry of information (for example, in the ROT protocol, after performing base matching, Bob does not discard the key that failed to match, but performs key separation according to his chosen c), Alice will perform random sampling from all keys, and require that the preparation base and key of the sampling part be made public, and then calculate the code error rate.

Assume that the error rate of the raw key owned by Alice and Bob is e and the key length is l, compared with the Alice's key, Bob's raw key has el errors. The amount of randomly extracted key bits is pl and satisfies $el < pl$, that is, $e < p$. Assume that there are m bit errors in the extracted pl keys, then consider that the error rate of the raw key is:

$$e' = \frac{m}{pl}.$$

In this paper, in order to ensure the security of the two-party encryption protocol, we put the error estimation process before the base matching. Thus, we can get:

$$e' = \frac{\mathrm{num}(x_i \neq y_i | \theta_{B_i} = \theta_{A_i})}{\mathrm{num}(\theta_{B_i} = \theta_{A_i})}.$$

2.4. Privacy Amplification

Generally speaking, we will use two-universal hash function for privacy amplification. The definition of two-universal hash function is as follows:

Definition 2 (Two-universal hash function)**.** *Let $\mathcal{F}$ be a cluster of functions $f : \{0,1\}^n \to \{0,1\}^l$ ($l \leq n$). If for all $x \neq y \in_R \{0,1\}^n$, we have:*

$$Pr_{f \in_R \mathcal{F}}[f(x) = f(y)] \leq 2^{-l}.$$

Then we say that $\mathcal{F}$ is two-universal.

Using two-universal hash function for privacy amplification, we also have privacy amplification theorem [2].

Firstly, we know the security of a key is defined with respect to its L1-distance from a perfect key which is uniformly distributed and independent of the adversary's state. Then the L1-distance from uniform of ρ_{XQ} given Q is :

$$\mathrm{d}(\rho_{XQ}|Q) := ||\rho_{XQ} - \rho_U \otimes \rho_Q||$$

where ρ_U is the fully mixed state .

Theorem 2 (Privacy amplification [25]). *Given a set of two-universal hash functions $\mathcal{F} : \{0,1\}^n \otimes \mathcal{R} \to \{0,1\}^l$, and a hash function $F \in_R \mathcal{F}$, let ρ_{XQ} be a classical-quantum state, then for any $\varepsilon \geq 0$. we have:*

$$\mathrm{d}[F(X)|F,Q] \leq 2^{-\frac{1}{2}\left[H_{\min}^{\varepsilon}(X|Q)-l\right]-1} + \varepsilon.$$

3. Weak String Erasure

In order to better demonstrate the application of joint measurement and error estimation technology in two-party cryptographic protocols, we first discuss its enhancement to the security performance of weak string erasure (WSE), which was originally proposed by Konig [2], and studied as the basic protocol of other two-party cryptographic protocols.

3.1. Definition

Before introducing our redesigned WSE protocol, we first introduce its definition. WSE is a basic two-party cryptographic protocol between Alice and Bob that can be used to construct other two-party cryptographic protocols, such as bit commitment, oblivious transfer, etc. The ideal functionality of WSE is shown in Figure 3 [2].

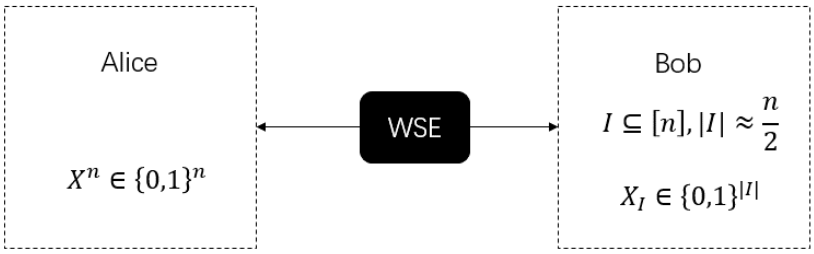

Figure 3. The ideal functionality of weak string erasure (WSE).

The process of WSE can be seen as a black box, with no inputs from Alice and Bob. As outputs, Alice gets a randomly chosen bits string X^n and Bob obtains a randomly chosen subset of indices $I \subseteq [n]$ and the bits $X_I \in \{0,1\}^{|I|}$. Next, we denote A and B as honest Alice and Bob, and A' and B' as dishonest Alice and Bob. ρ represents the joint state generated in the actual protocol operation, and σ represents the state generated in the ideal protocol operation.

The specific definition of WSE is as follows [2]:

Definition 3 (Weak string erasure [2]). *A $(n, \lambda, \varepsilon)$-weak string erasure (WSE) scheme is a protocol between Alice and Bob satisfying the following properties:*

1. *Correctness: If both parties are honest, then for any attack strategy of the third-party attacker, Alice always gets a uniformly distributed string $X^n \in_R \{0,1\}^n$and Bob will get an index $I \in [n]$ and $X_I \in \{0,1\}^{|I|}$;*
2. *Security for Alice: If Alice is honest, then for any attack strategy of dishonest Bob, we have:*

$$\frac{1}{n}\mathrm{H}_{\min}^{\varepsilon}(X^n|B') \geq \lambda.$$

3. *Security for Bob: If Bob is honest, then for any attack strategy of dishonest Alice, there exists* $\alpha \geq 0$*:*

$$\mathrm{H}_{\min}(I|A') \geq \alpha.$$

3.2. Protocol

In the previous protocol, there is a no error estimation process because the measurement results of the BB84 protocol are directly related to the final key. We redesign the WSE protocol by using the independence of key and measurement results of the MDI-QKD and PM-QKD protocols, adding a error estimation process to improve the security of the protocol.

The specific agreement is as follows:

1. Alice chooses a string $x^n \in_R \{0,1\}^n$ and bases the specifying string $\theta_A^n \in_R \{+,\times\}^n$ randomly. She encodes each bit x_i in the basis given by θ_{A_i} (as $H^{\theta_{A_i}}|x_i\rangle$) and sends it to the third party Charlie;
2. Similarly to Alice, Bob chooses a string $y^n \in_R \{0,1\}^n$ and bases specifying string $\theta_B^n \in_R \{+,\times\}^n$ randomly. He encodes each bit y_i in the basis given by θ_{B_i} (as $H^{\theta_{B_i}}|y_i\rangle$), and sends it to the third party Charlie;
3. Charlie performs a Bell measurement, and announces the outcome;
4. Alice selects a subset of the measurement outcome as the error estimator (about m qubits) and sends a subset of the measurement outcome I_{check} to Bob. Bob sends $\theta_{B_{check}}$ and a subset of the measurement outcome y_{check} ($y_{check}, \theta_{B_{check}} = \{y_i, \theta_{B_i} | i \in I_{check}\}$) to Alice. Then, they initiate error estimation process and compute:

$$Q_u = \frac{\mathrm{num}(x_i \neq y_i | \theta_{B_i} = \theta_{A_i})}{\mathrm{num}(\theta_{B_i} = \theta_{A_i})};$$

5. If $Q_u > e_r$, the communication is terminated, otherwise, the process continues;
6. Alice sends the remaining bases θ_A^{n-m} to Bob and outputs the remaining string x^{n-m};
7. Bob computes $I := \{i \in [n] | i \notin I_{check} \wedge \theta_{A_i} = \theta_{B_i}\}$ and outputs $(I, z^{|I|}) := (I, y_I)$.

3.3. Security Proof of WSE

Before analyzing the security of WSE protocol, we need to explain the constraint of Bob's storage capacity under joint state measurement and error estimation. When we remove any assumption about storage devices, we need other approaches to limit Bob's ability to store quantum states sent by Alice. Due to the constraints of the protocol process, we naturally think that Bob would cause the error rate increasement of the final key when he stores the quantum state and the error estimation is used to detect this attack. Next, we need to explain an important conception of the error correction upper bound of any channel error correction code. From [26] we know that:

$$\mathrm{f} = \frac{1 - \mathrm{R}}{\mathrm{h(e)}}$$

where f is the reconciliation efficiency which is given by the redundancy of disclosed information to the theoretical limit necessary for successful error correction, R is the code rate of a given channel error correction code, e is the error rate, and function h is the Shannon binary entropy. Then we can get the error correction upper bound when f approaches 1, i.e., its Shannon limit:

$$\mathrm{e_r} = \lim_{\mathrm{f}\to 1} \mathrm{e} = \lim_{\mathrm{f}\to 1} \mathrm{h}^{-1}\left(\frac{1-\mathrm{R}}{\mathrm{f}}\right).$$

where h^{-1} is the inverse function of h.

We consider when Bob stores the quantum state because the joint measurement cannot be performed and the published detection results are random. The increasement of error rate is explained the Lemma 3.

Lemma 3. *Assume that Bob has a perfect and unlimited capacity of quantum memory. Our protocol has a storage rate* v *, where* $v \leq 2e_r$.

Proof. In our protocol, the measurement outcomes are jointly measured by a third party in the bell state and published before Alice sends the bases θ_A. Alice will ask Bob to publish partial information for error estimation before sending bases θ_A. Now, we assume that Bob's storage rate is v, which means Bob will store vn quantum state in his memory. If Bob stores the quantum states, it means that he can not measure these quantum states, because quantum mechanics tells us that the measurement will cause the collapse of the quantum states and the loss of information. Therefore, Bob can publish a random fake outcome, and we have error rate introduced by this:

$$Q_u = \frac{n(1-v)e_c + \frac{1}{2}nv}{n} \leq e_r,$$

and we have:

$$v \leq 2e_r,$$

where e_c is error rate that caused by channel noise. □

In fact, with Lemma 3, we can easily convert our protocol into a WSE protocol under the bounded-storage model. Therefore, we can use the proof methods and results in Ref. [2,17] to prove the security of our protocol.

Lemma 4 (Security for Alice)**.** *Fix* $\delta \in [0, \frac{1}{4}]$*, and let,*

$$\varepsilon = 2\exp\left(-\frac{(\frac{\delta}{4})^2}{32(2+\log_2\frac{4}{\delta})^2}\right),$$

then for any attack strategy of dishonest Bob with any storage model $\mathcal{F} : \mathcal{B}(\mathrm{H_{in}}) \to \mathcal{B}(\mathrm{H_{out}})$*, we have:*
$\mathrm{H}^{\varepsilon}_{\min}(X^n|B')_\sigma \geq n(\frac{1}{2} - \delta - v) > 0.$

Proof. According to the conclusion in Ref. [2], we have:

$$\frac{1}{n}\mathrm{H}^{\varepsilon}_{\min}(X^n|B')_\sigma \geq -\frac{1}{n} log P^{\mathcal{F}}_{\mathrm{succ}}\left(\left(\frac{1}{2}-\delta\right)n\right) \geq v\gamma^{\mathcal{N}}\left(\frac{\frac{1}{2}-\delta}{v}\right),$$

where we have:

$$\gamma^{\mathcal{N}}(R) = \max_{\alpha\geq 1}\frac{\alpha-1}{\alpha}\left\{R - \log_2 d + \frac{1}{1-\alpha}\log_2\left[\left(r+\frac{1-r}{d}\right)^{\alpha} + (d-1)\left(\frac{1-r}{r}\right)^{\alpha}\right]\right\},$$

and in our protocol, we have parameters $\delta \in [0, \frac{1}{4}]$, $v = 2e_r$,$C_{\mathcal{N}} = 1$, $r = 1$, and $d = 2$. So, we have:

$$\gamma^{\mathcal{N}}(R) = \max_{\alpha\geq 1}\frac{\alpha-1}{\alpha}(R-1),$$

then,

$$\begin{aligned} \mathrm{H}_{\min}^{\varepsilon}(X^n|B')_{\delta} &\geq nv\gamma^{\mathcal{N}}\left(\frac{\frac{1}{2}-\delta}{v}\right) \\ &= nv\max_{\alpha\geq 1}\frac{\alpha-1}{\alpha}\left(\frac{\frac{1}{2}-\delta}{v}-1\right) \\ &\geq n\left(\frac{1}{2}-\delta-v\right)\geq 0. \end{aligned}$$

□

Next, we will discuss the security for Bob. Proving the security for Bob is relatively simple because Bob has no other leaked information besides his quantum state information during the protocol.

Lemma 5 (Security for Bob). *According to [2,27], for any attack of dishonest Alice with any storage model* $\mathcal{F}:\mathcal{B}(\mathrm{H_{in}})\to\mathcal{B}(\mathrm{H_{out}})$*, then we have:*

$$\mathrm{H}_{\min}(y^n|A')\geq -n\log_2\left(\frac{1}{2}+\frac{1}{2\sqrt{2}}\right),$$

4. 1-2 Random Oblivious Transfer

In this section, we further investigate 1-2 random oblivious transfer (ROT), which is also a basic two-party cryptographic protocol as WSE. Similarly, we give its definition first and then propose our protocol based on joint measurement and error estimation followed by its security proof.

4.1. Definition

As in Figure 4, like the WSE protocol, the 1-2 random oblivious transfer (ROT) protocol is also a basic two-party cryptographic protocol and is a random version of the 1-2 oblivious transfer (OT). Based on the 1-2 ROT protocol, we can easily implement the 1-2 OT protocol and the bit commitment (BC) protocol. In the 1-2 ROT protocol, instead of inputting two information strings $m_0, m_1 \in \{0,1\}^l$, Alice obtains two random key strings $S_0, S_1 \in \{0,1\}^l$. At the same time, Bob obtains the random key string S_c according to its input c. If we want to implement the 1-2 OT protocol, just after running the 1-2 ROT protocol, Alice encrypts the information strings m_0 and m_1 with the two strings of keys S_0 and S_1 obtained by ROT protocol. Bob can use S_c for decryption to obtain m_c.

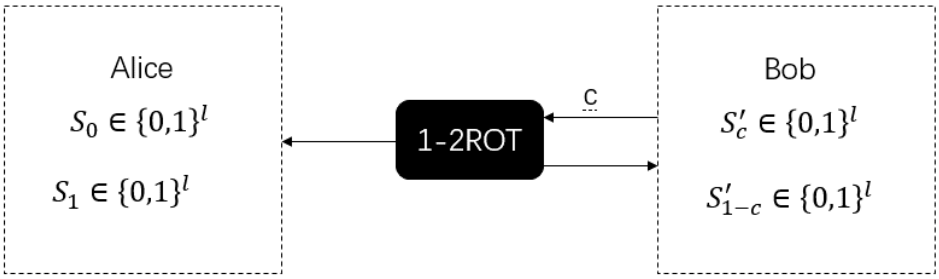

Figure 4. The ideal functionality of 1-2 random oblivious transfer (ROT). Bob has input c, Alice gets S_0, S_1, and Bob gets outputs S'_c, S'_{1-c} with $S_c = S'_c$ and $S_{1-c} \neq S'_{1-c}$.

In the security definition of the 1-2 ROT protocol, Alice cannot obtain Bob's input c, and Bob cannot obtain another string of keys S_{1-c} except S_c. The specific definition of security is as follows:

Definition 4. *An ε - secure 1-2 ROT is a protocol between Alice and Bob, where Bob has input* $c \in \{0,1\}$*, and Alice has no input, satisfying:*

1. *Correctness: If Alice and Bob are honest, then for any distribution of Bob's input c which is unknown to Alice, Alice gets outputs* $S_0, S_1 \in \{0,1\}^l$ *which are ε-close to randomness and independent of c, and Bob obtains* $Y = S_c$ *with probability ε;*
2. *Security for Alice: If Alice is honest, then for any cheating strategy of Bob resulting in his state* ρ_B*, there exists a random variable* $D \in \{0,1\}$*, and* $\lambda > 0$ *such that:*

$$\mathrm{H}_{\min}(S_{1-D}|B') \geq \lambda,$$

and

$$\mathrm{d}(S_{1-D}|B') \leq \varepsilon;$$

3. *Security for Bob: If Bob is honest and obtains output Y, then for any cheating strategy of Alice resulting in her state* ρ_A*, there exists a random variable* $D \in \{0,1\}$*, such that:*

$$\mathrm{H}_{\min}(D|A') \geq 1 - \varepsilon,$$

and

$$\Pr(\mathrm{Y} = \mathrm{S}'_{\mathrm{c}}) \leq \varepsilon.$$

4.2. Protocol

We now give the specific 1-2 ROT protocol using error estimation as follows:

1. Preparation: Alice chooses $x^n \in_R \{0,1\}^n$ and $\theta_A^n \in_R \{+,\times\}^n$, and Bob chooses $y^n \in_R \{0,1\}^n$ and $\theta_B^n \in_R \{+,\times\}^n$. Both parties send the encoding quantum state $|x\rangle_{\theta_A}^n$ or $|y\rangle_{\theta_B}^n$ to third party Charlie;
2. Measurement: Charlie measures $|x\rangle_{\theta_A}^n$ and $|y\rangle_{\theta_B}^n$ with Bell measurement, and announces the outcome;
3. Error estimation: Alice chooses $I_{check} \in_R 2^{[n]}$ and $|I_{check}| = m$, and sends I_{check} to Bob. Bob sends y_{check}, and $\theta_{B_{Check}} = \{y_i, \theta_{B_i} | i \in I_{check}\}$ to Alice. Then Alice calculates the error rate:

$$Q_u = \frac{\mathrm{num}(x_i \neq y_i | \theta_{B_i} = \theta_{A_i})}{\mathrm{num}(\theta_{B_i} = \theta_{A_i})}.$$

   If $Q_u > e_r$, they stop communication, otherwise they continue where e_r is the error correction upper bound;
4. Key division: Both parties discard the data that used in error estimation. Alice sends θ_A^{n-m} to Bob, Bob divides the key according to θ_A^{n-m}, θ_B^{n-m}, where $I_c = \{i | \theta_{A_i} = \theta_{B_i}\}$ and $I_{1-c} = \{i | \theta_{A_i} \neq \theta_{B_i}\}$. Bob sends I_0, I_1 to Alice;
5. Post processing: Alice chooses two hash function $f_0, f_1 \in_R \mathcal{F}_h$, and calculates $syn(X|I_0), syn(X|I_1)$. Alice passes f_0, f_1, $syn(X|I_0)$, and $syn(X|I_1)$ to Bob. Bob corrects the errors and outputs $S_c = f_c(Y|I_c)$. Alice outputs $S_0 = f_0(X|I_0)$ and $S_1 = f_1(X|I_1)$.

4.3. Security Proof of 1-2 ROT

According to the definition, we will prove the security of our proposed ROT protocol from the perspective of correctness, security for Alice, and security for Bob successively.

For correctness, if both parties are honest, Bob can calculate I_0, I_1 according to c, and S_c, and Alice can also get S_0, S_1. The focus is mainly on security for Alice and Bob.

Lemma 6 (Security for Alice)**.** *In 1-2 ROT protocol, n represents the number of bits transmitted during the protocol.* $\sigma_{B'X^n}$ *represents the state generated in the ideal protocol operation which consists of dishonest Bob and the variable* X^n *of n transmitted bits.* $\rho_{X_n B'}$ *represents the joint state generated in the actual protocol operation which consists of dishonest Bob and the variable* x_n *of n transmitted bits. If Alice is honest,* $n \to \infty$ *and the*

trace distance between these two states $||\sigma_{B'X^n} - \rho_{B'X^n}|| \leq \varepsilon$ *with* $\varepsilon = 2\exp\left(-\frac{\delta^2}{32(2+\log_2\delta)^2}\right)$. *Then we fix* $\delta \in \{0, \frac{1}{4}\}$, *we can get :*

1) $\mathrm{H}_{\min}(S_{1-D}|B') \geq (\frac{1}{4} - \delta - v)n - 1$,

2) $l \leq \left(\frac{1}{4} - \delta - 2e_r\right)n + 1 - \log_2\frac{1}{\epsilon^2}$.

Proof. With uncertainty relation theorem, we have:

$$\mathrm{H}^{\varepsilon}_{\min}(X^n|M\theta^n_A) \geq \left(\frac{1}{2} - 2\delta\right)n,$$

where M is the outcome that announced by Charlie. According to entropy sampling theorem:

$$\mathrm{H}^{\varepsilon}_{\min}(X_{1-D}|DM\theta^n_A) \geq \left(\frac{1}{4} - \delta\right)n - 1,$$

and in our protocol, according to Lemma 3, we have the storage rate $v = 2e_r$, then:

$$\mathrm{H}^{\varepsilon}_{\min}(X_{1-D}|DM\theta^n_A Q(\rho_A)) \geq \mathrm{H}^{\varepsilon}_{\min}(X_{1-D}|DM\theta^n_A) - vn = (\frac{1}{4} - \delta - v)n - 1$$

By using privacy amplification theorem:

$$\mathrm{d}(f_{1-D}(S_{1-D})|D\theta_A f_D \rho_A MQ(\rho_A)) \leq 2^{-\frac{1}{2}\left[\left(\frac{1}{4}-\delta-2e_r\right)-1-l\right]-1} + \varepsilon,$$

and let the above formula be less than 2ε, we can get:

$$l \leq \left(\frac{1}{4} - \delta - 2e_r\right)n + 1 - \log_2\frac{1}{\varepsilon^2}.$$

□

Lemma 7 (Security for Bob)**.** *In 1-2 ROT protocol, n represents the number of bits transmitted during the protocol.* $\sigma_{A'c}$ *represents the state generated in the ideal protocol operation which consists of dishonest Alice and commit bit c.* $\rho_{A'} \otimes \tau\{0,1\}$ *represents the joint state generated in the actual protocol operation which consists of dishonest Alice and commit bit c that is uniformly distributed on* $\{0,1\}$. *If Bob is honest,* $n \to \infty$ *and the trace distance between these two states* $||(\sigma_{A'c}) - \rho_{A'} \otimes \tau\{0,1\}|| \leq \varepsilon$, *and there exits* $\varepsilon \geq 0$, *then the conditional entropy with respect to c and* A', *we have:*

(1) $\mathrm{H}(c|A') \geq 1 - \varepsilon$

Proof. According to the definition of ROT protocol, if Alice is dishonest, then her purpose is to get c chosen by Bob. In our protocol, Bob's information leakage to Alice are $\rho_B, y_{check}, \theta_{check}, I_0$ and I_1. We have:

$$\Pr(c|y_{check}\theta_{check}I_0I_1\rho_B) = \Pr(c|I_0I_1\rho_B).$$

As $\Pr(c|I_0I_1x^ny^n) = 1$, we can argue that:

$$\Pr(c|I_0I_1\rho_B) = \Pr(y^n|I_0I_1\rho_B) = \max(\Pr(y^n|\rho_B), \frac{1}{2}),$$

and with the uncertainty relation theorem:

$$\mathrm{H}(y^n|\rho_B) = -n\log_2(\frac{1}{2} + \frac{1}{2\sqrt{2}}),$$

we can get:

$$\Pr(y^n|\rho_B) = 2^{-\mathrm{H}(y^n|\rho_B)} = \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^n.$$

when $n \to \infty$, $\Pr(c|I_0 I_1 \rho_B) = \max(\Pr(y^n|\rho_B), \frac{1}{2}) = \frac{1}{2}$, so we can get $\mathrm{H}(c|A') = -\sum_{k=0,1} p(c = k|A')\log_2 p(c = k|A') = 1$. Namely, exists $\varepsilon \geq 0$, $\mathrm{H}(c|A') \geq 1 - \varepsilon$. □

5. Applications for Two Party Cryptography

In this section, we redesign two specific two-party cryptographic protocols using a joint measurement method and briefly analyze their security. The first protocol is bit commitment which is proposed by [1]. The second protocol is password-based identification, which allows us to use passwords for authentication without revealing passwords.

5.1. Bit Commitment

In this subsection, we redesign bit commitment protocol using joint measurement and prove the security of this protocol. Quantum bit commitment protocol is one of the earliest proposed quantum two-party encryption protocols. The original version of quantum bit commitment is a variant of quantum coin tossing proposed by Bennett and Brassard [1]. In fact, quantum bit commitment is easy to adapt from 1-2 ROT protocol.

5.1.1. Definition and Protocol

Informally, a standard bit commitment scheme consists of two sub-protocols called commitment protocol and revealing protocol. First, Alice and Bob execute the commitment protocol. Alice has commit bit $c \in \{0, 1\}$ as input, and Bob has no input. As a result of this protocol, Bob will get some evidence about c. In the second phase, Alice and Bob execute the revealing protocol, where Alice has an input for remaining evidence and commit bit c and Bob also has no input. At the end of this protocol, Bob will output accept or reject according to Alice's inputs from the commitment protocol and revealing protocol.

If both parties are honest, Bob always accepts the bit c. If Alice is dishonest, however, Bob should not output accept. If Bob is dishonest, he should not be able to gain any information about c before the revealing protocol is executed. The definition of security in bit commitment protocol is as follows.

Definition 5 (Bit commitment [17])**.** *An ε-secure bit commitment is a protocol between Alice and Bob, where Alice has input $c \in \{0, 1\}$, and Bob has no input.*

1. *Correctness: If both parties are honest, then the ideal state δ_{cans} is defined as:*

   The distribution of commit bit c for Bob is uniform when Bob gets no information about distribution of c besides the information leakage by this protocol, and Bob accepts the commitment:

   $$\delta_{cans} = \tau_{\{0,1\}} \otimes |\mathrm{accept}\rangle\langle\mathrm{accept}|.$$

2. *Security for Alice (ε-hiding): If Alice is honest, then for any joint state $\rho_{cB'}$ created by the commit protocol, Bob does not learn c. Here,*

   $$\rho_{cB'} \approx_\varepsilon \tau_{\{0,1\}} \otimes \rho_{B'},$$

   and the entropy of c:

   $$\mathrm{H}_{\min}(c|B') \geq 1 - \varepsilon.$$

3. *Security for Bob (ε-Binding): If Bob is honest, then there exists an ideal cq-state $\delta_{cA'V}$ such that for all operations for ρ'_A, we have:*

   $$\Pr[\mathrm{outputs} = \mathrm{accept}|\mathrm{A}'] \leq \varepsilon.$$

We have rewritten the QBC agreement based on the contents of the ROT agreement as shown below.

Bit commitment - commit phase: The input is commit bit $c \in \{0,1\}$ for Alice. The output are $S_c \in \{0,1\}^l$ to Alice, and $S_0', S_1' \in \{0,1\}^l$ to Bob.

1. Preparation: Alice chooses $x^n \in_R \{0,1\}^n$ and $\theta_A^n \in_R \{+,\times\}^n$ furthermore, Bob chooses $y^n \in_R \{0,1\}^n$ and $\theta_B^n \in_R \{+,\times\}^n$. Both parties send the encoding quantum state $|x\rangle_{\theta_A}^n$ or $|y\rangle_{\theta_B}^n$ to the third party Charlie;
2. Measurement: Charlie measures $|x\rangle_{\theta_A}^n$ and $|y\rangle_{\theta_B}^n$ with Bell basis, and announces the outcome;
3. Error estimation: Bob chooses $I_{check} \in_R 2^{[n]}$ and $|I_{check}| = m$, and sends I_{check} to Alice. Alice sends $x_{check}, \theta_{A_{Check}} = \{x_i, \theta_{A_i} | i \in I_{check}\}$ to Bob. Bob calculates the error rate Q_u:

$$Q_u = \frac{\text{num}(x_i \neq y_i | \theta_{B_i} = \theta_{A_i})}{\text{num}(\theta_{B_i} = \theta_{A_i})}.$$

   If $Q_u > e_r$, they stop communication, else they continue. Here e_r is error correction upper bound;
4. Key division: Both parties discard the bits that used in error estimation. Bob sends θ_B^{n-m} to Alice. Alice divides the key according to $\theta_A^{n-m}, \theta_B^{n-m}$, where $I_c = \{i | \theta_{A_i} = \theta_{B_i}\}$ and $I_{1-c} = \{i | \theta_{A_i} \neq \theta_{B_i}\}$, and sends I_0, I_1 to Bob;
5. Post processing: Bob chooses two hash functions $f_0, f_1 \in_R \mathcal{F}_h$, and calculates two syndromes $\text{syn}(X|I_0), \text{syn}(X|I_1)$. Bob sends $f_0, f_1, \text{syn}(X|I_0), \text{syn}(X|I_1)$ to Alice. Alice corrects errors and outputs $S_c = f_c(Y|I_c)$. Bob outputs $S_0' = f_0(X|I_0), S_1' = f_1(X|I_1)$.

Bit commitment–revealing phase: The input is S_c for Alice. The outputs are $c \in \{0,1\}$ and $\text{ans} \in \{\text{accept}, \text{reject}\}$ to Bob.

1. Alice: Alice sends S_c and c to Bob;
2. Bob: If $S_c = S_c'$, then Bob obtains c and $ans = accept$. Otherwise, he outputs $ans = reject$.

5.1.2. Security Analysis

The correctness of the protocol does not need to be proven because the protocol is designed according to the definition of bit commitment protocol. Its ε-hiding is guaranteed by the security of the ROT protocol.

Lemma 8 (Security for Alice)**.** *n represents the number of bits transmitted during the protocol. Let $n \to \infty$, we have:*

(1) $\delta_{cB'} \approx_\varepsilon \tau_{\{0,1\}} \otimes \rho_{B'}$,
(2) $\text{H}_{\min}(c|B') \geq 1 - \varepsilon$.

Proof. Our Commitment protocol is adopted from the 1-2 ROT, and according to Definition 5, we have $\text{H}_{\min}(c|B') \geq 1 - \varepsilon$. □

Lemma 9 (Security for Bob)**.** *n represents the number of bits transmitted during the protocol. Fix $\delta \in [0, \frac{1}{4}]$, and exist $\varepsilon \to 0$, we have:*

$\Pr(\text{ans} = \text{accept}|\text{A}') \leq \varepsilon$.

Proof. According to Lemma 5,

$$\text{H}_{\min}(y^n|A') \geq -n\log_2\left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right),$$

because

$$\Pr(\text{y}^\text{n}|\text{A}') = 2^{-\text{H}_{\min}(\text{y}^\text{n}|\text{A}')} \leq \left(\frac{1}{2} + \frac{1}{2\sqrt{2}}\right)^\text{n}.$$

we can easily get $\Pr(\text{ans} = \text{accept})|\mathrm{A}') \leq \varepsilon$. □

5.2. Password-Based Identification

In this subsection, we introduce the joint measurement method to password-based protocol from [15].

Password-based identification (PID) so far is one of the most widely-used authentication methods. In this protocol, the user and server share a series of keys and the user logs in the system server by verifying the keys. Its security definition contains two points. The first is that users who do not know the password cannot log into the system server successfully and cannot learn other users' password through this protocol. The second is that the dishonest server (eg. scam server) cannot learn the password holds by honest users. For the convenience of description, in the following, we use Alice instead of user and Bob instead of server. Formally, security is defined as follows.

Definition 6 ($(n, \lambda, \varepsilon)$-secure PID)**.** *An $(n, \lambda, \varepsilon)$-secure PID is a protocol between Alice and Bob, where Alice and Bob has input password $w \in \{0,1\}^l$.*

1. *Correctness: If both parties are honest, Bob will always output "accept" at the end of the protocol;*
2. *Security for Alice: If Alice is honest, then for any cheating strategy of Bob resulting in his state ρ_B, we have $\lambda \geq 0$, and:*
$$\mathrm{H}_{\min}^{\varepsilon}(w|B') \geq \lambda;$$
3. *Security for Bob: If Bob is honest, then for any cheating strategy of Alice resulting in her state ρ_A, there exists $\varepsilon \geq 0$, we have:*
$$\Pr(\text{outputs} = \text{accept}|\mathrm{A}') \leq \varepsilon.$$

Next, we give our PID protocol. The input is $w \in \{0,1\}^l$ for Alice and the output is $ans \in \{accept, reject\}$ for Bob.

1. Preparation: Alice chooses $x^n \in_R \{0,1\}^n$ and $\theta_A^n \in_R \{+,\times\}^n$, and Bob also chooses $y^n \in_R \{0,1\}^n$ and $\theta_B^n \in_R \{+,\times\}^n$. Both parties send the encoding quantum state $|x\rangle_{\theta_A}^n$ or $|y\rangle_{\theta_B}^n$ to the third party, Charlie;
2. Measurement: Charlie measures $|x\rangle_{\theta_A}^n$ and $|y\rangle_{\theta_B}^n$ with Bell measurement, and announces the outcome;
3. Error estimation: Alice chooses $I_{check} \in_R 2^{[n]}$ and $|I_{check} = m$, and sends I_{check} to Bob. Bob sends $y_{check}, \theta_{B_{Check}} = \{y_i, \theta_{B_i} | i \in I_{check}\}$ to Alice. Alice calculates the error rate Q_u:
$$Q_u = \frac{\text{num}(x_i \neq y_i | \theta_{B_i} = \theta_{A_i})}{\text{num}(\theta_{B_i} = \theta_{A_i})}.$$
If $Q_u > e_r$, they stop communication, else they continue. Here, e_r is the error correction upper bound;
4. Key shifting: Bob calculates a string $\kappa \in \{0,1\}^n$ such that $\kappa = c(w) \oplus \theta_B^n$($\kappa_i = 0$ means basis is $+$, anyone else). He sends the string κ to Alice, and they define the shifted code $\hat{\theta}_B^n = c(w) \oplus \kappa$. Alice sends θ_A^n and a hash function $f \in_R \mathcal{F}$ to Bob. Both computes $I_w = \{i | \theta_{A_i} = \hat{\theta}_{B_i}\}$;
5. Identification: Bob sends $g \in_R \mathcal{G}$ to Alice. Alice sends $z = f(x|I_w) \oplus g(w)$ to Bob. Bob accepts if and only if $z = f(y|I_w) \oplus g(w)$.

We omit the proof part because the process is roughly similar to Ref. [17].

6. Conclusions

In this paper, we proposed several two-party cryptographic protocols based on joint measurement and error estimation, including WSE, 1-2 ROT, and other protocols, and demonstrated their security.

Compared with the protocol mentioned in [2,17,28,29], our protocols discarded the assumption that the attacker's storage device was defective, but instead employed a combination of joint measurement and error estimation to limit the quantum storage of the attacker. Our protocols had no assumptions, were more secure, and had wider applicability. The two basic two-party cryptographic protocols mentioned in this paper could easily be extended to other two-party encryption protocols, such as 1-2 OT and quantum identification protocols.

We eliminated the assumption that the attack was bounded by the attacker's technology, and employed the technique of joint measurement and error estimation to improve two basic quantum two-party cryptographic protocols. We demonstrated that our improved protocols offered stronger security and is applicable to many specific quantum two-party cryptographic protocols such as BC and PID.

Inspired by [30,31], we learned that quantum coherence plays an important role in quantum key distribution and quantum random number generation, and this might also be used to improve our work. Future work will also begin with this aspect.

Author Contributions: Conceptualization: Z.Z.; methodology: Z.Z.; validation: Q.G.; formal analysis: Q.G. and Z.Z.; writing—original draft preparation: Z.Z.; writing—review and editing: Q.G., C.G.; project administration: D.J.; funding acquisition: L.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research is supported by the National Natural Science Foundation of China (No. 61771236), National Key Research and Development Program of China (No. 2017YFA0303700), Major Program of National Natural Science Foundation of China (No. 11690030,11690032), and Excellence Research Program of Nanjing University.

Conflicts of Interest: The study claims no conflict of interest.

References

1. Bennett, C.-H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. *arXiv* **2020**, arXiv:2003.06557.
2. Konig, R.; Wehner, S.; Wullschleger, J. Unconditional security from noisy quantum storage. *IEEE Trans. Inf. Theory* **2012**, *58*, 1962–1984. [CrossRef]
3. Kent, A. Unconditionally secure bit commitment. *Phys. Rev. Lett.* **1999**, *83*, 1447. [CrossRef]
4. Lo, H.-K.; Chau, H.-F. Why quantum bit commitment and ideal quantum coin tossing are impossible. *Phys. D Nonlinear Phenom.* **1998**, *120*, 177–187. [CrossRef]
5. Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **1997**, *78*, 3414–3417. [CrossRef]
6. Lo, H.-K.; Chau, H.-F. Is quantum bit commitment really possible? *Phys. Rev. Lett.* **1997**, *78*, 3410–3413. [CrossRef]
7. 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. [CrossRef]
8. Peres, A.; Terno, D.-R. Quantum information and relativity theory. *Rev. Mod. Phys.* **2004**, *76*, 93–123. [CrossRef]
9. Kent, A. Unconditionally secure bit commitment by transmitting measurement outcomes. *Phys. Rev. Lett.* **2012**, *109*, 130501. [CrossRef]
10. Liu, Y.; Cao, Y.; Curty, M.; Liao, S.-K.; Wang, J.; Cui, K.; Li, Y.-H.; Lin, Z.-H.; Sun, Q.-C.; Li, D.-D.; et al. Experimental unconditionally secure bit commitment. *Phys. Rev. Lett.* **2014**, *112*, 010504. [CrossRef]
11. Hardy, L.; Kent, A. Cheat sensitive quantum bit commitment. *Phys. Rev. Lett.* **2004**, *92*, 157901. [CrossRef] [PubMed]
12. Li, Y.-B.; Xu, S.-W.; Huang, W.; Wan, Z.-J. Quantum bit commitment with cheat sensitive binding and approximate sealing. *J. Phys. A Math. Theor.* **2015**, *48*, 135302. [CrossRef]
13. 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. [CrossRef]
14. Shimizu, K.; Fukasaka, H.; Tamaki, K.; Imoto, N. Cheat-sensitive commitment of a classical bit coded in a block of m × n round-trip qubits. *Phys. Rev. A* **2011**, *84*, 022308. [CrossRef]

15. Damgård, I.B.; Fehr, S.; Salvail, L.; Schaffner, C. Secure identification and qkd in the bounded-quantum-storage model. In *Advances in Cryptology-CRYPTO 2007*; Menezes, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2007; pp. 342–359.
16. Wehner, S.; Wullschleger, J. Composable security in the bounded-quantum-storage model. *arXiv* **2007**, arXiv:0709.0492.
17. Schaffner, C. Simple protocols for oblivious transfer and secure identi-fication in the noisy-quantum-storage model. *Phys. Rev. A* **2010**, *82*, 032308. [CrossRef]
18. He, G.-P. Quantum key distribution based on orthogonal states allows secure quantum bit commitment. *J. Phys. A Math. Theor.* **2011**, *44*, 445305. [CrossRef]
19. Lo, H.-K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
20. Yin, H.-L.; Chen, T.-Y.; Yu, Z.-W.; Liu, H.; You, L.-X.; Zhou, Y.-H.; Chen, S.-J.; Mao, Y.; Huang, M.-Q.; Zhang, W.-J.; et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **2016**, *117*, 190501. [CrossRef]
21. Liu, Y.; Chen, T.-Y.; Wang, L.-J.; Liang, H.; Shentu, G.-L.; Wang, J.; Cui, K.; Yin, H.-L.; Liu, N.-L.; Li, L.; et al. Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2013**, *111*, 130502. [CrossRef]
22. Ma, X.; Zeng, P.; Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **2018**, *8*, 031043. [CrossRef]
23. Lucamarini, M.; Yuan, Z.-L.; Dynes, J.-F.; Shields, A.-J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400. [CrossRef]
24. Damgård, I.B.; Fehr, S.; Renner, R.; Salvail, L.; Schaffner, C. A tight high-order entropic quantum uncertainty relation with applications. In *Advances in Cryptology—CRYPTO 2007*; Menezes, A., Ed.; Springer: Berlin/Heidelberg, Germany, 2007; pp. 360–378.
25. Renner, R. Security of Quantum Key Distribution. Ph.D. Thesis, ETH Zurich, Zurich, Switzerland, 2005.
26. Kiktenko, E.-O.; Trushechkin, A.-S.; Lim, C.-C.-W.; Kurochkin, Y.V.; Fedorov, A.K. Symmetric blind information reconciliation for quantum key distribution. *Phys. Rev. Appl.* **2017**, *8*, 044017. [CrossRef]
27. Ballester, M.-A.; Wehner, S.; Winter, A. State discrimination with post-measurement information. *IEEE Trans. Inf. Theory* **2008**, *54*, 4183–4198. [CrossRef]
28. Kaniewski, J.; Wehner, S. Device-independent two-party cryptography secure against sequential attacks. *New J. Phys.* **2016**, *18*, 055004. [CrossRef]
29. Zhao, L.; Yin, Z.; Wang, S.; Chen, W.; Chen, H.; Guo, G.; Han, Z. Measurement-device-independent quantum coin tossing. *Phys. Rev. A* **2015**, *92*, 062327. [CrossRef]
30. Ma, J.; Zhou, Y.; Yuan, X.; Ma, X. Operational interpretation of coherence in quantum key distribution. *Phys. Rev. A* **2019**, *99*, 062325. [CrossRef]
31. Ma, J.; Hakande, A.; Yuan, X.; Ma, X. Coherence as a resource for source-independent quantum random-number generation. *Phys. Rev. A* **2019**, *99*, 022328. [CrossRef]