entropy

MDPI

Article

Quantum Identity Authentication in the Counterfactual Quantum Key Distribution Protocol

Bin Liu [1,*], Zhifeng Gao [1], Di Xiao [1], Wei Huang [2,*], Zhiqing Zhang [3] and Bingjie Xu [2,*]

[1] Postdoctoral Station of Computer Science and Technology, College of Computer Science, Chongqing University, Chongqing 400044, China; Benny_commander@163.com (Z.G.); dixiao@cqu.edu.cn (D.X.)

[2] Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu 610041, China

[3] Chongqing University–Uninversity of Cincinnati Joint Co-op, Chongqing University, Chongqing 400044, China; zqzhang@cqu.edu.cn

* Correspondence: liubin31416@gmail.com (B.L.); huangwei096505@aliyun.com (W.H.); xbjpku@163.com (B.X.)

Received: 10 April 2019; Accepted: 20 May 2019; Published: 23 May 2019

Abstract: In this paper, a quantum identity authentication protocol is presented based on the counterfactual quantum key distribution system. Utilizing the proposed protocol, two participants can verify each other's identity through the counterfactual quantum communication system. The security of the protocol is proved against individual attacks. Furthermore, according to the characteristics of the counterfactual quantum key distribution system, we propose an authenticated counterfactual quantum key distribution protocol based on a novel strategy of mixing the two types of quantum cryptographic protocols randomly. The authenticated quantum key distribution can also be used to update the extent of the authentication keys.

Keywords: quantum identity authentication; quantum key distribution; counterfactual quantum communication

1. Introduction

Quantum mechanics has produced immense influence in information security. The widely used public key cryptography algorithms such as the RSA public key algorithm are facing serious threat of quantum computation [1]. Meanwhile, quantum computation also promotes new kinds of cryptographic protocols that can combat the powerful computation capability of quantum computer. Interestingly, quantum mechanics could be a sharp spear to break cryptographic systems and also a strong shield to protect our privacy. Research shows that quantum key distribution (QKD) can provide information theoretic security between two distant and authenticated parties [2–5]. Various QKD protocols have been proposed utilizing different quantum coding technologies, as well as the other types of quantum cryptographic protocol, such as quantum secure direct communication [6–11], quantum secret sharing [12–17], quantum private querying [18–23] and so on [24–26].

Counterfactual QKD protocols employ a very interesting coding method where the valid key bits are generated when no photons have been transmitted in the public channel. Since no photons to be intercepted and captured for the signals of the valid key bits, it is very difficult for the adversaries to carry on an effective attack. Because of the above characteristics, the counterfactual QKD has attracted a lot of attention since its first appearance. In 2009, Noh proposed a QKD protocol [27] inspired by the counterfactual phenomena in quantum world [28] and the counterfactual computation [29]. The next year, Sun et al. proposed a high efficiency version of counterfactual QKD utilizing more beam splitters [30]. The same year, Yin et al. proved the security of Noh's protocol strictly [31]. During the

next few years, many experiments on counterfactual QKD protocol have been performed [32–35]. In the theoretic study of counterfactual quantum communication technology, some scholars analyzed the security of counterfactual QKD on real environment [36–41], while others proposed other types of quantum cryptographic protocols with counterfactual quantum communication technology, such as direct quantum communication [42–44], quantum private query [45], and so on [46–53].

As described above, the counterfactual QKD protocol has been proven secure in theory [31], however, the security is based on several necessary conditions, such as the perfect quantum detectors, the perfect single-photon source, true random number generator and so on. Secure and reliable identity authentication is one of the key requirements of the security of the counterfactual QKD. Realizing identity authentication with quantum technology has many potential advantages such as higher security, higher efficiency and immunity to certain kinds of replay attacks. Therefore, we propose a quantum identity authentication (QIA) protocol that can be used in the counterfactual QKD protocol to identify the communication parties. Furthermore, due to the characteristics of the counterfactual quantum communication technology, the combined processes of the counterfactual QKD protocol and the proposed QIA protocol can be used to extend the length of authentication keys with almost arbitrary expanded proportion. This paper is organized as follows. In Section 2, we briefly review the processes of the counterfactual QKD and an alternative version, which our QIA protocol is based on. The specific process of the counterfactual QIA protocol is proposed in Section 3. With the QIA protocol in Section 3, we propose an authenticated counterfactual QKD protocol in Section 4. A brief conclusion is given in Section 5.

2. Review of the Counterfactual Quantum Key Distribution Protocol

The main purpose of this paper is to verify the participants' identities in the counterfactual QKD system. As a foundation protocol, the counterfactual QKD protocol [27] is briefly introduced in this section. Utilizing the interference system in Figure 1, the counterfactual QKD can help Alice and Bob generate a secure key based on the signals where no photons have traveled through the public channel. Note that, in Figure 1, C is the optical circulator; OD is the optical delay to make the two paths a and b be the same; OL is the optical loop and SW is the optical switch, which help Bob choose the pulse in specific polarization to the detector D_2; FM is the faraday mirror, which reflects the pulse while turns the state of the pulse to the orthogonal polarization; and D_1 can discriminate the polarizations of the pulse. The processes can be described as follows.

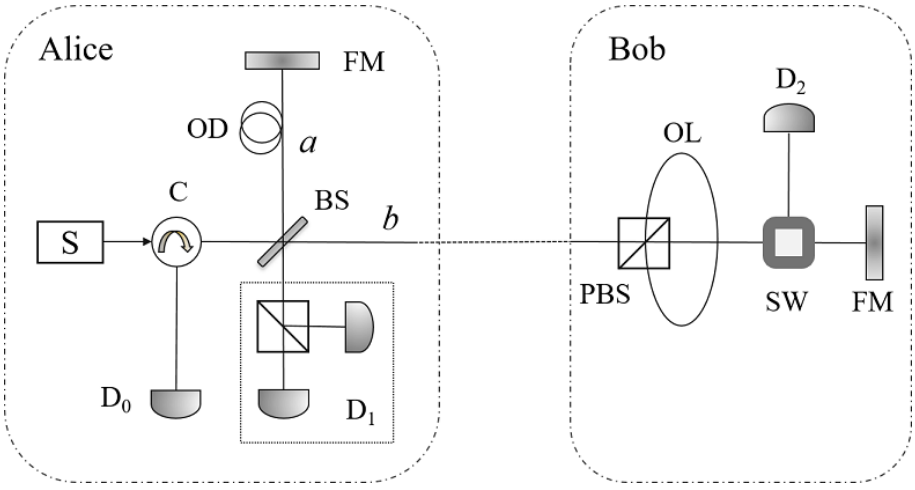

Figure 1. The schematic of the counterfactual QKD [27]. Here, C is the optical circulator; OD is the optical delay to make the two paths a and b be the same; OL is the optical loop and SW is the optical switch, which help Bob choose the pulse in specific polarization to the detector D_2; FM is the faraday mirror, which reflects the pulse while turns the state of the pulse to the orthogonal polarization; and D_1 can discriminate the polarizations of the pulse.

(1) At the beginning, Alice triggers the single-photon source S to emit a short optical pulse containing a single photon at a certain point in time. The photon is prepared in either horizontal polarization $|H\rangle$, which represents the classical bit 0, or vertical polarization $|V\rangle$, which represents 1. Afterwards, the pulse will be divided into two paths, a and b, when it passes the beam splitter (BS). The whole system can be described as one of the two orthogonal states

$$\sqrt{T}|0\rangle_a|V\rangle_b + \mathrm{i}\sqrt{R}|V\rangle_a|0\rangle_b, \tag{1}$$

$$\sqrt{T}|0\rangle_a|H\rangle_b + \mathrm{i}\sqrt{R}|H\rangle_a|0\rangle_b, \tag{2}$$

where R and T are the reflectivity and transmissivity of BS, and $R + T = 1$. The state $|0\rangle_k$ represents the vacuum state in the path k, where $k \in \{a, b\}$.

(2) Bob randomly chooses a bit 0 or 1 and, utilizing the polarizing beam splitter (PBS) and the optical loop (OL), switches different polarized pulse to the detector D_2 according to the above bit. Precisely, if Bob chooses 0 (1), he switches the pulse in the state $|H\rangle$ ($|V\rangle$) to the detector D_2. In fact, when the pulse in path b reaches the PBS at Bob's side, it would directly go to the optical switch (SW) if the pulse were horizontally polarized, and if the pulse were vertically polarized, it would be reflected by the PBS, pass through the OL, be reflected by PBS again, and then go to SW. Thus, if the pulse were in state $|V\rangle$, it would arrive at SW a certain period of time (L/c, where L is the length of OL and c is the speed of time) later than the situation of $|H\rangle$. Therefore, Bob can choose to switch different polarized states to the detector D_2 by the control of the switch time.

(3) At last, Alice and Bob announce which detector clicks. If only D_1 detects a photon with the correct polarization, they establish a key bit, otherwise, the result will be used to detect eavesdropping. In fact, if Alice's and Bob's bits are identical, the pulse in path b will be absorbed by D_2, and the pulse in path a will be divided into two parts towards D_0 and D_1, respectively. In this situation, the three detectors D_0, D_1 and D_2 will click with the probabilities R^2, RT and T, respectively. If Alice's and Bob's bits are different, the pulse in path b will be reflected back to BS. The faraday mirror (FM) alters the state of the pulse to the orthogonal state while reflects it, therefore, the pulse will determinately pass the OL once and be reflected by the PBS twice, before or after the reflection of FM. The two paths a and b are set with the same length, so the two pulses will complete the interference at BS, with the same polarization state and a phase difference of π. In this situation, D_0 always clicks but D_1 never. Therefore, Alice and Bob would share an identical bit when only D_1 clicks. In ideal cases, the shared bit is secure since no photons have passed through the public channel if D_1 clicks alone.

Generally, to achieve the highest key rate, R and T are set to be $1/2$ and $1/2$. Considering the situation of 50:50 BS, there is an alternative version (see Figure 2) of the above protocol.

In this alternative version proposed by Brida et al. [33], Bob uses a half wave plate (HWP) and a PBS to accomplish the same task with that in the original protocol. The effect of the half wave plate can be described as follows,

$$U(\alpha) = \mathrm{i}\begin{bmatrix} \cos 2\alpha & \sin 2\alpha \\ \sin 2\alpha & -\cos 2\alpha \end{bmatrix}, \tag{3}$$

where α is the angle between the incident and the fast axis. The two faraday mirrors are replaced by two mirrors. In Step (1), by adjusting the angle of HWP_A, Alice randomly rotates the state of the single-photon pulse to $|H\rangle$ or $|V\rangle$. In Step (2), Bob randomly performs $U(0)$ or $U(\pi/4)$ to the coming pulse by adjusting the angle of HWP_B to be 0 or $\pi/4$, where

$$U(0) = \mathrm{i}|H\rangle\langle H| - \mathrm{i}|V\rangle\langle V|, \tag{4}$$

$$U(\pi/4) = \mathrm{i}|H\rangle\langle V| + \mathrm{i}|V\rangle\langle H|. \tag{5}$$

For convenience of reading, we list another two operations, which will be used later,

$$U(\pi/8) = \frac{\mathrm{i}}{\sqrt{2}}(|H\rangle\langle H| + |H\rangle\langle V| + |V\rangle\langle H| - |V\rangle\langle V|), \tag{6}$$

$$U(3\pi/8) = \frac{\mathrm{i}}{\sqrt{2}}(-|H\rangle\langle H| + |H\rangle\langle V| + |V\rangle\langle H| + |V\rangle\langle V|). \tag{7}$$

When the pulse passes BS the first time, the state becomes one of the following states,

$$\rho_{BS}(0) = -\frac{\mathrm{i}}{\sqrt{2}}|0\rangle_a|V\rangle_b + \frac{1}{\sqrt{2}}|V\rangle_a|0\rangle_b, \tag{8}$$

$$\rho_{BS}(\pi/4) = \frac{\mathrm{i}}{\sqrt{2}}|0\rangle_a|H\rangle_b - \frac{1}{\sqrt{2}}|H\rangle_a|0\rangle_b, \tag{9}$$

which are exactly the same with Equations (1) and (2), ignoring the global phase $-\mathrm{i}$ or i introduced by HWP_A. Here, we assume that S always emits a pulse in state $|V\rangle$. When Alice's and Bob's choices are 0 and $\pi/4$, respectively, the pulse in path b has been reflected back to BS at Alice's side, the state of the photon after the pulse passes BS the second time will become

$$\begin{aligned}\rho'_{BS}(0,\pi/4) &= -\frac{1}{\sqrt{2}}(\frac{1}{\sqrt{2}}|V\rangle_0|0\rangle_1|0\rangle_2 + \frac{\mathrm{i}}{\sqrt{2}}|0\rangle_0|V\rangle_1|0\rangle_2) + \frac{\mathrm{i}}{\sqrt{2}}(\frac{\mathrm{i}}{\sqrt{2}}|V\rangle_0|0\rangle_1|0\rangle_2 + \frac{1}{\sqrt{2}}|0\rangle_0|V\rangle_1|0\rangle_2) \\ &= -|V\rangle_0|0\rangle_1|0\rangle_2,\end{aligned} \tag{10}$$

or similarly when Alice's and Bob's choices are $\pi/4$ and 0, the state would be

$$\rho'_{BS}(\pi/4,0) = |H\rangle_0|0\rangle_1|0\rangle_2, \tag{11}$$

where the subscripts represent the path leading to the corresponding detectors. Thus, the same as the original protocol, D_0 always clicks in this situation. Correspondingly, the key should be generated when D_1 clicks.

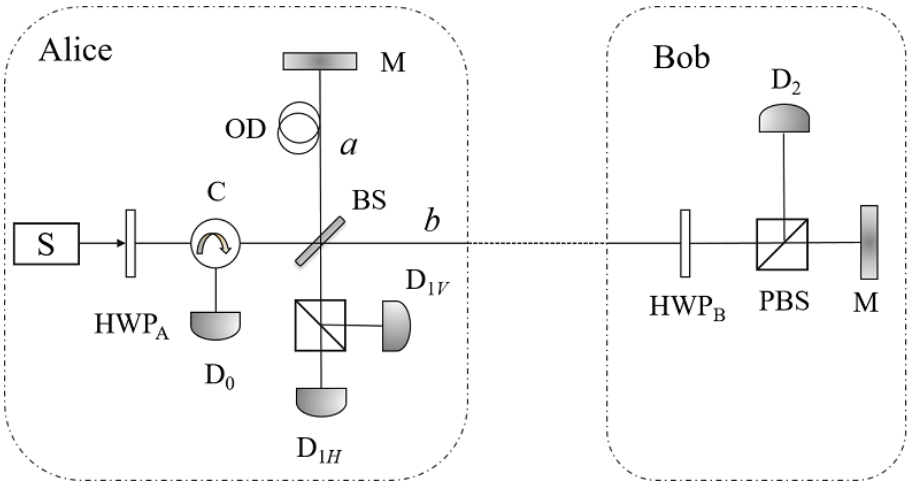

Figure 2. The schematic of the alternative version of the counterfactual QKD [33]. The alternative version uses two half wave plates HWP_A and HWP_B, instead of the OL and SW, to implement the random choices of the participants. Another difference is that the alternative version uses mirrors (M) instead of faraday mirrors in the original one.

3. QIA in the Counterfactual QKD System

In this section, we propose a QIA protocol, where two participants, utilizing a pre-shared classical authentication key, can verify each other's identity through the counterfactual QKD system. The communication system we adopt here is the alternative version, which is more convenient

to introduce a conjugate basis to complete the task of identity authentication. Here, we make a minor modification that the half wave plate on Alice's side, i.e., HPB_A is set at the right side of BS (see Figure 3).

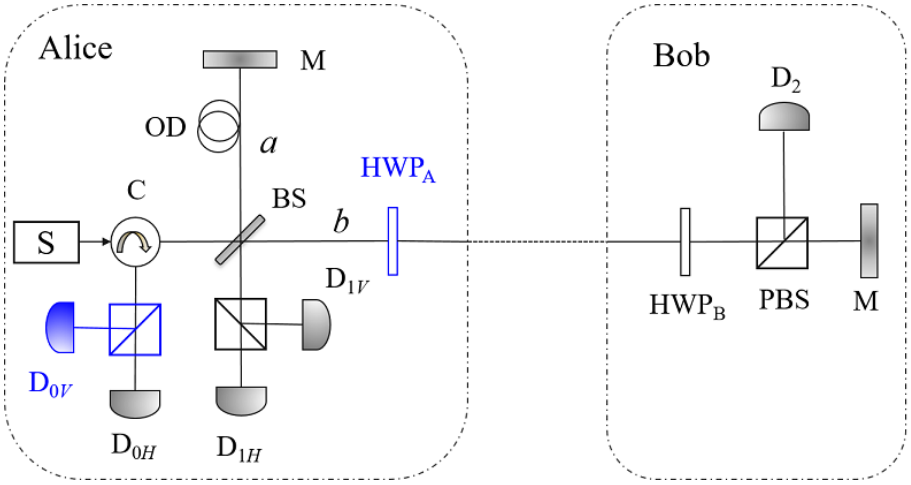

Figure 3. The schematic of the proposed QIA protocol and the authenticated QKD protocol. HWP_A is set at right side of BS in our protocol instead of left in the alternative version. Since the polarizations of the pulses detected by D_0 is also used to detect the adversary in our protocol, we add a PBS and an additional detector in the D_0.

Thus, the states of the photons back to Alice's side should always be the same with their original states, and the key bits should be generated from the signals where D_0 clicks alone.

3.1. The QIA Protocol Based on the Counterfactual QKD

For the sake of description of the proposed QIA protocol, we first expound some basic concepts about the protocol and the devices in Figure 3. Before the protocol, two participants are required to pre-share a sequence of authentication keys $\{K_1, K_2, ..., K_l\}$. Each of the above keys has $m + n$ bits, where the first m bits would be used for Alice to verify Bob's identity, and the last n bits are for Bob to verify Alice's identity. Alice and Bob also record the statuses of their keys, originally "valid".

The single-photon source S in Figure 3 is supposed to always emit a pulse in state $|V\rangle$, and Alice can choose to keep its state or flip it to $|H\rangle$ utilizing HWP_A. Ignoring the global phases, if Alice adjusts α_A, the angle of HWP_A, to 0, the state of the pulse remains $|V\rangle$, and if Alice adjusts α_A to $\pi/4$, the state changes to $|H\rangle$. Bob also randomly chooses to flip the state of the coming pulse or not, utilizing HWP_B. The above processes are just the alternative version of the counterfactual QKD protocol.

To complete the task of identity authentication, the participants use the authentication key as the control bits in the manner that, if the ith bit of the authentication key is 1, Alice and Bob both rotate an additional angle of $\pi/8$ to their half wave plates, otherwise, they do nothing additionally. Thus, only the legal participants who have the authentication key can perform complete the QIA protocol legally. The concrete processes of the proposed QIA protocol are as follows.

1. Key status exchange. Alice and Bob exchange the status of their pre-shared authentication keys and choose the one with the smallest subscript among those keys which are "valid" on both Alice's and Bob's sides. We denote the bits of this key K as

$$\{b_1, b_2, ..., b_m, a_1, a_2, ..., a_n\}. \tag{12}$$

2. Authentication of Bob's identity. The first m pulses are used to authenticate Bob's identity in the manner that Alice chooses her bit randomly and Bob always chooses bit 0, and both of the above choices are under control of the first m bits of K.

2.1 Alice generates a random string R_A with m bits

$$\{r_1, r_2, ..., r_m\}. \tag{13}$$

2.2 For the ith pulse Alice emits into the system, she sets the angle of HWP_A as

$$\frac{\pi}{4} \times r_i + \frac{\pi}{8} \times b_i. \tag{14}$$

2.3 For the ith coming pulse, Bob sets the angle of HWP_B as

$$\frac{\pi}{8} \times b_i. \tag{15}$$

2.4 Alice checks the results of D_0 and D_1. If D_1 clicks with the probability of 100% for the pulses where $r_i = 1$, and for those $r_i = 0$, D_0 and D_1 click with the probability about 25% and 25%, respectively, Alice believes Bob's identity and they go on to Step 3, otherwise, Alice skips to the last step.

3. Authentication of Alice's identity. In this step, Bob checks Alice's identity with the help of the last n bits of K.

3.1 Bob generates a random string R_A with m bits

$$\{s_1, s_2, ..., s_m\}. \tag{16}$$

3.2 For the $(m + j)$th pulse, Alice sets the angle of HWP_A as

$$\frac{\pi}{8} \times a_i. \tag{17}$$

3.3 For the $(m + j)$th coming pulse, Bob sets the angle of HWP_B as

$$\frac{\pi}{4} \times s_i + \frac{\pi}{8} \times a_i. \tag{18}$$

3.4 Bob checks results of D_2. If D_2 never clicks when $s_i = 0$ and clicks with the probability of 50% for both the two cases that $\{s_i = 1, a_i = 0\}$ and $\{s_i = 1, a_i = 1\}$, Bob believes Alice's identity.

4. Key status update. Alice and Bob update the statuses of K as "invalid".

3.2. Correctness of the Proposed QIA Protocol

For the legal Alice and Bob, they can verify each other's identity following the above processes. The unitary operations of the HWPs in different cases are shown in Equations (4)–(7). In the processes of Step 2, there are four cases about Alice's and Bob's choices of $\{\alpha_A, \alpha_B\}$: $\{0, 0\}$, $\{\pi/4, 0\}$, $\{\pi/8, \pi/8\}$, and $\{3\pi/8, \pi/8\}$. For the situation of $\{0, 0\}$, the state of the whole pulse when it first passes BS and HWP_A is

$$\rho_{HA}(0) = -\frac{\mathrm{i}}{\sqrt{2}}|0\rangle_a|V\rangle_b + \frac{\mathrm{i}}{\sqrt{2}}|V\rangle_a|0\rangle_b. \tag{19}$$

The final state, i.e., the state of the polarization and the position of the photon after (part of) it passes BS the second time, is

$$\begin{aligned} \rho'_{BS}(0,0) &= -\frac{1}{\sqrt{2}}\left(\frac{\mathrm{i}}{\sqrt{2}}|V\rangle_0|0\rangle_1|0\rangle_2 + \frac{1}{\sqrt{2}}|0\rangle_0|V\rangle_1|0\rangle_2\right) - \frac{\mathrm{i}}{\sqrt{2}}|0\rangle_0|0\rangle_1|V\rangle_2 & (20)\\ &= -\frac{\mathrm{i}}{2}|V\rangle_0|0\rangle_1|0\rangle_2 - \frac{1}{2}|0\rangle_0|V\rangle_1|0\rangle_2 - \frac{\mathrm{i}}{\sqrt{2}}|0\rangle_0|0\rangle_1|V\rangle_2. & (21) \end{aligned}$$

Here, we use $\rho_{HA}(\alpha)$ to denote the state of the pulse when it first passes BS and HWP$_A$ in the situation that $\alpha_A = \alpha$, $\rho_{PBS}(\alpha_1, \alpha_2)$ to denote the state when the pulse first passes PBS in the situation that $\alpha_A = \alpha_1$ and $\alpha_B = \alpha_2$, and $\rho'_{BS}(\alpha_1, \alpha_2)$ to denote the state when the pulse passes BS the second time. For the situation of $\{\pi/8, \pi/8\}$,

$$\rho_{HA}(\pi/8) \quad = \quad \frac{\mathrm{i}}{\sqrt{2}}|0\rangle_a|-\rangle_b + \frac{\mathrm{i}}{\sqrt{2}}|V\rangle_a|0\rangle_b, \tag{22}$$

where

$$|-\rangle = \frac{1}{\sqrt{2}}(|H\rangle - |V\rangle). \tag{23}$$

and

$$\rho_{PBS}(\pi/8, \pi/8) = -\frac{1}{\sqrt{2}}|0\rangle_a|V\rangle_b + \frac{\mathrm{i}}{\sqrt{2}}|V\rangle_a|0\rangle_b. \tag{24}$$

Thus, the final state of this case would be

$$\rho'_{BS}(\pi/8, \pi/8) = -\frac{\mathrm{i}}{2}|V\rangle_0|0\rangle_1|0\rangle_2 - \frac{1}{2}|0\rangle_0|V\rangle_1|0\rangle_2 - \frac{\mathrm{i}}{\sqrt{2}}|0\rangle_0|0\rangle_1|V\rangle_2. \tag{25}$$

For both above cases of Equations (21) and (25), D_0, D_1 and D_2 would click with the probabilities of 25%, 25% and 50%, respectively. Similarly, we can calculate that

$$\rho'_{BS}(\pi/4, 0) = \rho'_{BS}(3\pi/8, \pi/8) = -|0\rangle_0|V\rangle_1|0\rangle_2. \tag{26}$$

D_1 always clicks in these two cases. The calculations on the four cases coincide with the judgements at the end of Step 2.

The four possible final states in the processes of Step 3 are $\rho'_{BS}(0, 0)$, $\rho'_{BS}(0, \pi/4)$, $\rho'_{BS}(\pi/8, \pi/8)$, and $\rho'_{BS}(\pi/8, 3\pi/8)$. Here, $\rho'_{BS}(0, 0)$ and $\rho'_{BS}(\pi/8, \pi/8)$ are considered in Equations (21) and (25), and

$$\rho'_{BS}(0, \pi/4) = \rho'_{BS}(\pi/8, 3\pi/8) = -|0\rangle_0|V\rangle_1|0\rangle_2. \tag{27}$$

The calculations on these four final states in Step 3 coincide with the judgements in Step 3, too. Therefore, for the legal participants who have the authentication key K, they can always authenticate each other's identities correctly.

3.3. The Security Analysis for No-Error Cases

In fact, the security of Bob's identity is protected by the first part of K, i.e., $\{b_1, b_2, ..., b_m\}$. The operations Bob's operations in the first part is $U(0)$ if $b_i = 0$ and $U(\pi/8)$ if $b_i = 1$. According to the theorems on operation discrimination, the above two operations cannot be discriminated with no error probability (see Appendix A for details). If the adversary, who is forging Bob's identity to communicate with Alice, performs an error operation on the received pulse, Alice would get a wrong measurement result. Therefore, the adversary cannot always gives Alice a correct response to pass Alice's tests. Correspondingly, the security of Alice's identity is protected by the second part of K, i.e., $\{a_1, a_2, ..., a_n\}$. Since the second part of the protocol only executed when the communicating peer passes Alice's tests, the adversary cannot get any information about the string $\{a_1, a_2, ..., a_n\}$ from Alice's side. Therefore, the adversary has to face Bob's tests without any information on the authentication key. Considering that Bob chooses his angles from $\{0, \pi/8\, \pi/4, 3\pi/8\}$ randomly, the measurement results would be random if he is communicating with the adversary who has no information about $\{a_1, a_2, ..., a_n\}$. That is, the adversary cannot pass Bob's tests without introducing

any error. Above all, we can get a conclusion that the adversary cannot forge either Alice's identity or Bob's identity in the no-error cases.

For the more general cases, the security analysis of the proposed protocol are described in Appendix A. Specifically, for each signal, we calculate a relaxed lower bound of the minimum error probability that the adversary has to introduce in Alice's test while forging Bob,

$$P_b = \frac{1}{2}(1 - \frac{\sqrt{5-2\sqrt{2}}}{16\sqrt{2}-8}) > 2.8\%, \tag{28}$$

and a relaxed lower bound of the minimum error probability that the adversary has to introduce in Bob's test while forging Alice,

$$P_a > 6.5\%. \tag{29}$$

We believe that the tight bounds would be much larger, since we have made many relaxations during the derivation procedure to simplify the difficulty.

4. Authenticated Counterfactual QKD Protocol

In this section, we propose an authenticated counterfactual QKD protocol utilizing the proposed QIA protocol. The basic idea is mixing the process of the QIA protocol into the QKD protocol according to the random data generated in the QKD protocol, which can be recorded identically for the two participants without any communication. In the following authenticated QKD protocol, the length of original authentication key is independent with the length of the new generated key. Suppose the length of the key that the participants expect to generate is m, and the length of the authentication key K_A which meets the requirement of security is n. Then, the mixing parameter of the authenticated counterfactual QKD protocol is

$$r = \lfloor \frac{4m}{n} \rfloor. \tag{30}$$

With the definition of r, the main processes of the authenticated QKD protocol can be briefly described as follows: once Bob's detector has clicked r times, Alice and Bob insert one round of the QIA process presented in last section. Specifically, utilizing the devices and circuit in Figure 3, the participants can implement the authenticated counterfactual QKD protocol as follows. For convenience of the following description, we use p_i to denote the probability that the ith signal is used for the process of QIA.

***a*. Set-up**. For the main processes described above, p_i is convergent when i gets larger, however it is much smaller than the convergence value for small is. For example, $p_i = 0$ when $i \leq r$. If the adversary only attacks these signals with smaller p_i, he is more likely to pass the participant's test. Therefore, before the formal steps of the protocol, Alice and Bob should equalize p_i for different is. l_r pulses would be used in this stage, where

$$l_r = 2\lceil \log(4r+1) \rceil. \tag{31}$$

a_1 Alice emits l_r single-photon pulses to the system one by one. For each pulse, Alice (Bob) randomly choose the angle of HWP_A (HWP_B) to be one of $\{0, \pi/8, \pi/4, 3\pi/8\}$.

a_2 If the photon goes to Bob's detector, i.e., D_2 clicks and D_0 and D_1 do not, they record a classical bit 1. If the photon goes back to Alice, i.e., D_0 or D_1 clicks and D_2 does not, they record a classical bit 0.

a_3 After all the l_r pulses have been detected by the three detectors, Alice and Bob get a l_r bit binary number. Then, they use a hash function to uniformly map the above number into the set $\{0, 1, ..., 4r\}$, and denote the result as f_r. Note that, for one single binary bit, the uncertainty is

$$-\frac{1}{4}\log(\frac{1}{4}) - \frac{3}{4}\log(\frac{3}{4}) \approx 0.56. \tag{32}$$

Alice and Bob produce l_r signals here so that the uncertainty of the l_r bits is larger than $\log(4r+1)$, to make the value of f_r totally random.

***b*. Signal transmission and identity authentication**. Utilizing the random number f_r generated in last step, the participants start to distribute a new key while authenticate each other's identity.

b_1 For the first f_r pulses in this step, Alice and Bob perform the QKD process, i.e., they both randomly alter the angles of HWP_A and HWP_B to be 0 or $\pi/4$ and record the clicking situation of each detector and the state of the photon if the detector has clicked.

b_2 The $(f_r{+}1)$th pulse is the first pulse for identity authentication. As in Steps 2.2 and 2.3 in the above QIA protocol, Alice alters the angle of HWP_A to be $\pi/4 * r_1 + \pi/8 * b_1$ and Bob alters the angle of HWP_B to be $\pi/8 * b_1$, where b_1 is the first bit of the authentication key and r_i is a random bit.

b_3 From the $(f_r + 2)$th pulse, the participants start to insert the process of QIA into the QKD according to the random data of the clicks of the detectors. Precisely, each time the click times of D_2 reaches an integral multiple of r, they insert one round of the QIA process immediately until the authentication process for Bob's identity has finished.

b_4 Alice checks Bob's identity according to Step 2.4.

b_{5-8} If the test for Bob's identity passes, they continue to transmit the rest QKD signals and authenticate Alice's identity by repeating the processes from b_1 to b_4 but perform the operations in Steps 3.2–3.4 instead of these in Steps 2.2–2.4, respectively.

***c*. Eavesdropping detection**. Alice and Bob first check the validity of each other's identity. If the identity authentication passes, they continue to the rest part of the counterfactual QKD protocol to generate a new key and use part of the new key to update the authentication keys.

In the above protocol, the processes of QIA and QKD are mixed randomly; however, they are performed independently. More specifically, the sequence of the signals for QIA and ones for QKD are random for the adversaries. On the other hand, each signal is either used for QIA or for QKD, but never for both. Because of such independence, the correctness of the above protocol is obliviously established considering the correctness of the counterfactual QKD protocol [27,31] and the counterfactual QIA protocol presented in the last section, as is the security of the process of QIA and the process of QKD. The only new factor which may influence the security of the whole protocol is that the adversary may discriminate the two type of signals, i.e., the signals for QKD and the signals for QIA, and then only attack the signals for QKD. Next, we proved that the adversary cannot discriminate the two type of signals.

Firstly, the two types of signals cannot be discriminated precisely. For a QKD signal, Alice randomly sets her angle as 0 or $\pi/4$, and the reduced density matrix for the state in path b is

$$\begin{aligned} \rho_{QKD} &= \frac{1}{2}(\frac{1}{2}(|0\rangle\langle 0| + |V\rangle\langle V|) + \frac{1}{2}(|0\rangle\langle 0| + |H\rangle\langle H|)) \\ &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{4}I. \end{aligned} \tag{33}$$

For a QIA signal in the first part, Alice's operation set is $\{0, \pi/8, \pi/4, 3\pi/8\}$, and the reduced density matrix for the state in path b is

$$\begin{aligned}\rho_{QIA_B} &= \frac{1}{4}(\frac{1}{2}(|0\rangle\langle 0| + |V\rangle\langle V|) + \frac{1}{2}(|0\rangle\langle 0| + |H\rangle\langle H|) \\ &\quad + \frac{1}{2}(|0\rangle\langle 0| + |+\rangle\langle +|) + \frac{1}{2}(|0\rangle\langle 0| + |-\rangle\langle -|)) \\ &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{4}I, \end{aligned} \tag{34}$$

which is the same as ρ_{QKD}. For the second part of QIA, Alice's operation set is $\{0, \pi/8\}$, and the reduced density matrix for the state in path b is

$$\begin{aligned}\rho_{QKA_A} &= \frac{1}{2}(\frac{1}{2}(|0\rangle\langle 0| + |V\rangle\langle V|) + \frac{1}{2}(|0\rangle\langle 0| + |-\rangle\langle -|)) \\ &= \frac{1}{2}|0\rangle\langle 0| + \frac{1}{4}(|V\rangle\langle V| + |-\rangle\langle -|) \end{aligned} \tag{35}$$

The minimum error probability to discriminating ρ_{QKD} and ρ_{QKA_A} is

$$\frac{1}{2} - \frac{\sqrt{2}}{16} \approx 0.41, \tag{36}$$

which is close to $1/2$, the probability of random guess. Furthermore, the discrimination operation will inevitably disturb the pulse in path b and introduce errors in the authentication process or the detection mode of QKD.

Secondly, we analyze the probability of being a QIA pulse for each signal. The expectation of the above probability can be deduced by calculating the average interval of two QIA signals, which is

$$D = \sum_{j=r}^{\infty} jp\mathrm{C}_{j-1}^{r-1}p^{r-1}(1-p)^{j-r}. \tag{37}$$

$$= p^r \sum_{k=0}^{\infty}(r+k)\mathrm{C}_{r+k-1}^{k}(1-p)^k. \tag{38}$$

Then, both sides of the above equation are multiplied by $(1-p)$,

$$(1-p)D = p^r \sum_{k=0}^{\infty}(r+k-1)\mathrm{C}_{r+k-2}^{k-1}(1-p)^k. \tag{39}$$

By subtracting the two equations, we have

$$\begin{aligned} pD &= p^r \sum_{k=1}^{\infty}(r+k-1)\left(\mathrm{C}_{r+k-1}^{k} - \mathrm{C}_{r+k-2}^{k-1}\right)(1-p)^k + rp^r + +p^r \sum_{k=1}^{\infty}\mathrm{C}_{r+k-2}^{k-1}(1-p)^k \\ &= rp^r + p^r \sum_{k=1}^{\infty}(1-p)^k\left((r+k)\mathrm{C}_{r+k-2}^{k} + \mathrm{C}_{r+k-2}^{k-1}\right) \\ &= rp^r + rp^r \sum_{k=1}^{\infty}\mathrm{C}_{r+k-1}^{k}(1-p)^k. \end{aligned} \tag{40}$$

Suppose

$$D_i = \sum_{k=i}^{\infty}\mathrm{C}_{r+k-i}^{k}(1-p)^k. \tag{41}$$

Then,

$$(1-p)D_i = \sum_{k=i}^{\infty} C_{r+k-i}^{k}(1-p)^{k+1} = \sum_{k=i+1}^{\infty} C_{r+k-(i+1)}^{k-1}(1-p)^{k}. \quad (42)$$

We can get

$$pD_i = (1-p)^i C_r^i + D_{i+1}. \quad (43)$$

So that,

$$\begin{aligned} D_1 &= \sum_{k=1}^{\infty} C_{r+k-1}^{k}(1-p)^{k} \\ &= \sum_{j=1}^{r} C_r^j (1-\frac{1}{p})^j + \frac{1}{p^r}\sum_{k=r}^{\infty} C_{k-1}^{k}(1-p)^{k} \\ &= \frac{1}{p^r} - 1. \end{aligned} \quad (44)$$

Substituting Equation (44) into Equation (40), we have

$$D = \frac{r}{p}, \quad (45)$$

where $p = 1/4$. This implies that every $D+1$ signals contain one QIA signal on average. Therefore, the average probability for a pulse to be a QIA signal is

$$\overline{p} = \frac{1}{4r+1}, \quad (46)$$

However, it is difficult to propose a strategy where the above probability is totally identical for each signal. As for the proposed protocol, the probability of the lth signal to be a QIA one is

$$P_r(l) = \overline{p}\sum_{k=1}^{4r+1}\sum_{j=1}^{\lfloor \frac{l}{r+1} \rfloor} C_{l-1-i-k}^{rj-1}(\frac{1}{4})^{rj}(\frac{3}{4})^{l-rj-j-k}. \quad (47)$$

The the graphs of function $p_r(l)$ for different values of r are given in Figure 4.

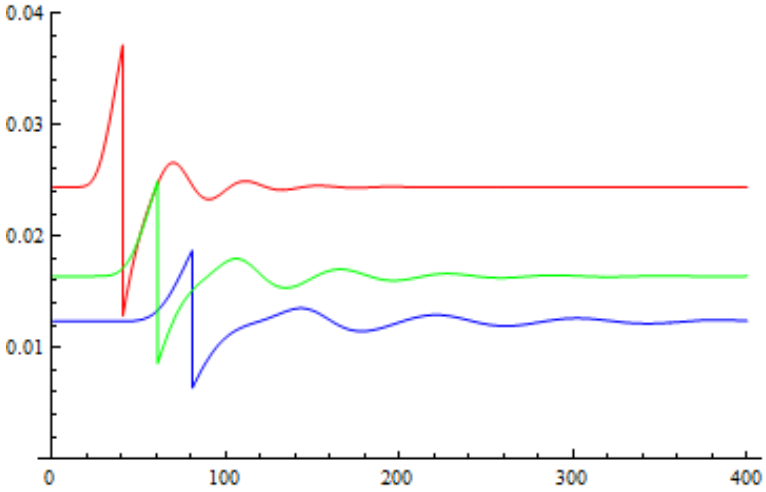

Figure 4. The graphs of function $p_r(l)$ when $r = 10$ (the red line), 15 (the green line), and 20 (the blue ine).

We can see that the probability p_l tends to be stable when l is larger than $8r$. The adversary cannot effectively reduce the error rate introduced by his attack utilizing the probability distribution of the type of the signals. Therefore, if the adversary wants to attack a proportion of the QKD signals, she will have to disturb a similar proportion of the QIA signals, which will cause a failure result in the QIA part.

5. Conclusions

In this paper, we first propose a quantum identity authentication protocol that can be realized in the counterfactual quantum communication system. Then, we propose an authenticated counterfactual QKD protocol by mixing the processes of the proposed QIA protocol and the counterfactual QKD protocol in [33]. In this authenticated counterfactual QKD protocol, the two independent processes of QKD and QIA mixed randomly for any third party except the two participants, therefore, the adversaries cannot discriminate between a QIA signal and a QKD signal. Any attempts to perform a man-in-the-middle attack to the process of QKD will disturb the signal in the QIA process and cause a failure result in the identity authentication. Since the two processes are independent, the length of the authentication key is only related to the expected confidence degree for the participants' identities, and is not concerned with length of the newly generated key in QKD. Therefore, the key expansion in our protocol can be extremely high in theory. The problem is that the proposed protocol can only be performed in noiseless channels since any channel loss or dark count would mess up the whole process of the protocol. Once a channel loss or dark count happens, Alice and Bob cannot synchronize the random data to control the signal type. Despite this, we think the idea of identity authentication in this paper is promising in theory and might inspire practical QIA protocols and authenticated QKD protocols designed in similar ways. The theory of high key-expand-ability QIA protocols in noisy channel will also be our future work.

Author Contributions: Conceptualization, B.L. and W.H.; Formal analysis, B.L.; Funding acquisition, B.L., D.X., W.H., Z.Z. and B.X.; Investigation, Z.G.; Methodology, B.L. and Z.G.; Project administration, B.L.; Resources, D.X., W.H. and B.X.; Supervision, D.X.; Validation, W.H.; Writing—Original draft, B.L.; and Writing—Review and editing, Z.Z.

Acknowledgments: This work was supported by National Natural Science Foundation of China (Grant Nos. 61702061, 61702469, 61771439, 61572089, and 61802037), China Postdoctoral Science Foundation Funded Project (Grant No. 2017M612912), Chongqing Postdoctoral Science Foundation funded project (Grant No. Xm2017041), Fundamental Research Funds for the Central Universities (rant Nos. 106112016CDJXY180001 and 2018CDJSK04XK09), National Cryptography Development Fund (Grant No. MMJJ20170120), Sichuan Youth Science and Technology Foundation (Grant No. 2017JQ0045), and Natural Science Foundation Project of CQ (Grant No. cstc2017rgzn-zdyfX0042).

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

Appendix A. Security of the Counterfactual QIA Protocol

Appendix A.1. Security of Bob's Identity

Here, we first analyze the security of the protocol against an adversary who attempts to counterfeit Bob's identity. Suppose the adversary's system is prepared in the state of $|e\rangle$. Furthermore, considering the situation that the adversary knows no information of the authentication key K, we suppose his attack operation is O, where

$$O|H\rangle|e\rangle = |H\rangle|hh\rangle + |V\rangle|hv\rangle + |0\rangle|h0\rangle, \quad \text{(A1)}$$

$$O|V\rangle|e\rangle = |H\rangle|vh\rangle + |V\rangle|vv\rangle + |0\rangle|v0\rangle, \quad \text{(A2)}$$

$$O|0\rangle|e\rangle = |0\rangle|00\rangle. \quad \text{(A3)}$$

In the above equations, the states for the adversary's system are non-normalized and satisfy

$$\langle hh|hh\rangle + \langle hv|hv\rangle + \langle h0|h0\rangle = 1, \tag{A4}$$
$$\langle vh|vh\rangle + \langle vv|vv\rangle + \langle v0|v0\rangle = 1. \tag{A5}$$

To avoid multiple responses in Alice's detectors, when the state in path b is empty state $|0\rangle$, the adversary should keep it empty, therefore $\langle 00|00\rangle = 1$.

When the pulse in path b arrives at the adversary's side, the whole state of path a, path b and the adversary's system E is

$$\frac{1}{\sqrt{2}}(|0\rangle_a|V_\alpha\rangle_b|e\rangle_E + \mathrm{i}|V\rangle_a|0\rangle_b|e\rangle_E), \tag{A6}$$

where

$$|V_\alpha\rangle = U(\alpha)|V\rangle. \tag{A7}$$

For the situation $\alpha = 0$, the state after the adversary's operation is

$$-\frac{\mathrm{i}}{\sqrt{2}}|0\rangle_a(|H\rangle_b|vh\rangle_E + |V\rangle_b|vv\rangle_E + |0\rangle_b|v0\rangle_E) + \frac{\mathrm{i}}{\sqrt{2}}|V\rangle_a|0\rangle_b|00\rangle_E. \tag{A8}$$

When the pulse in path b passed HWP_A the second time, the state turns to

$$\frac{1}{\sqrt{2}}|0\rangle_a(|H\rangle_b|vh\rangle_E - |V\rangle_b|vv\rangle_E - \mathrm{i}|0\rangle_b|v0\rangle_E) - \frac{1}{\sqrt{2}}|V\rangle_a|0\rangle_b|00\rangle_E. \tag{A9}$$

Further, when the two pulses in paths a and b pass BS the second time, the state becomes

$$\begin{aligned}\rho_E(0) &= \frac{1}{2}(|H\rangle_0|0\rangle_1|vh\rangle_E + \mathrm{i}|0\rangle_0|H\rangle_1|vh\rangle_E) - \frac{1}{2}(|V\rangle_0|0\rangle_1|vv\rangle_E + \mathrm{i}|0\rangle_0|V\rangle_1|vv\rangle_E)\\ &\quad -\frac{1}{2}(\mathrm{i}|V\rangle_0|0\rangle_1|00\rangle_E + |0\rangle_0|V\rangle_1|00\rangle_E) - \frac{\mathrm{i}}{\sqrt{2}}|0\rangle_a|0\rangle_b|v0\rangle_E.\end{aligned} \tag{A10}$$

After a simple transformation, we can get

$$\begin{aligned}\rho_E(0) &= \frac{1}{2}|V\rangle_0|0\rangle_1(-\mathrm{i}|00\rangle - |vv\rangle)_E + \frac{1}{2}|0\rangle_0|V\rangle_1(-|00\rangle - \mathrm{i}|vv\rangle)_E\\ &\quad +\frac{1}{2}|H\rangle_0|0\rangle_1|vh\rangle_E + \frac{\mathrm{i}}{2}|0\rangle_0|H\rangle_1|vh\rangle_E + \frac{1}{\sqrt{2}}|0\rangle_0|0\rangle_1|v0\rangle_E.\end{aligned} \tag{A11}$$

Similarly, we can get the states of whole system when the two pulses pass BS the second time

$$\begin{aligned}\rho_E(\frac{\pi}{8}) &= \frac{1}{2}|V\rangle_0|0\rangle_1(-\mathrm{i}|00\rangle - |S_{+--+}\rangle)_E + \frac{1}{2}|0\rangle_0|V\rangle_1(-|00\rangle - \mathrm{i}|S_{+--+}\rangle)_E\\ &\quad -\frac{1}{2}|H\rangle_0|0\rangle_1|S_{++--}\rangle_E - \frac{\mathrm{i}}{2}|0\rangle_0|H\rangle_1|S_{++--}\rangle_E - \frac{1}{2}|0\rangle_0|0\rangle_1(|h0\rangle - |v0\rangle)_E,\end{aligned} \tag{A12}$$

$$\begin{aligned}\rho_E(\frac{\pi}{4}) &= \frac{1}{2}|V\rangle_0|0\rangle_1(-\mathrm{i}|00\rangle + |hh\rangle)_E + \frac{1}{2}|0\rangle_0|V\rangle_1(-|00\rangle + \mathrm{i}|hh\rangle)_E\\ &\quad -\frac{1}{2}|H\rangle_0|0\rangle_1|hv\rangle_E - \frac{\mathrm{i}}{2}|0\rangle_0|H\rangle_1|hv\rangle_E - \frac{1}{\sqrt{2}}|0\rangle_0|0\rangle_1|h0\rangle_E,\end{aligned} \tag{A13}$$

and

$$\begin{aligned}\rho_E(\frac{3\pi}{8}) &= \frac{1}{2}|V\rangle_0|0\rangle_1(-\mathrm{i}|00\rangle - |S_{+-+-}\rangle)_E + \frac{1}{2}|0\rangle_0|V\rangle_1(-|00\rangle - \mathrm{i}|S_{+-+-}\rangle)_E\\ &\quad -\frac{1}{2}|H\rangle_0|0\rangle_1|S_{++++}\rangle_E - \frac{\mathrm{i}}{2}|0\rangle_0|H\rangle_1|S_{++++}\rangle_E - \frac{1}{2}|0\rangle_0|0\rangle_1(|h0\rangle + |v0\rangle)_E,\end{aligned} \tag{A14}$$

where

$$|S_{+--+}\rangle = \frac{1}{2}(|hh\rangle - |hv\rangle - |vh\rangle + |vv\rangle), \quad \text{(A15)}$$

$$|S_{++--}\rangle = \frac{1}{2}(|hh\rangle + |hv\rangle - |vh\rangle - |vv\rangle), \quad \text{(A16)}$$

$$|S_{+-+-}\rangle = \frac{1}{2}(|hh\rangle - |hv\rangle + |vh\rangle - |vv\rangle), \quad \text{(A17)}$$

$$|S_{++++}\rangle = \frac{1}{2}(|hh\rangle + |hv\rangle + |vh\rangle + |vv\rangle). \quad \text{(A18)}$$

Alice would notice the existence of the adversaries if she has detected a photon in horizontal polarization or the clicking probabilities of D_0 and D_1 are not correct. We divide the probability that the adversary would be found into four parts. The first part is the probability that Alice detects a horizontal polarized photon,

$$P_1 = \frac{1}{8}(\langle vh|vh\rangle + \langle S_{++--}|S_{++--}\rangle + \langle hv|hv\rangle + \langle S_{++++}|S_{++++}\rangle). \quad \text{(A19)}$$

The second part is the probability that Alice has not detected any photon when $r_i = 1$,

$$P_2 = \frac{1}{16}[2\langle h0|h0\rangle + (\langle h0| + \langle v0|)(|h0\rangle + |v0\rangle)]. \quad \text{(A20)}$$

The third part is the probability that Alice detects a vertical polarized photon at D_0 when $r_i = 1$,

$$P_3 = \frac{1}{16}[(\mathrm{i}\langle 00| + \langle hh|)(-\mathrm{i}|00\rangle + |hh\rangle) + (\mathrm{i}\langle 00| + \langle S_{+-+-}|)(-\mathrm{i}|00\rangle + |S_{+-+-}\rangle)]. \quad \text{(A21)}$$

The fourth part is about the scales of the clicks of D_0 and D_1, and this part is related with the length of the authentication key and the required confidence of the users' identities in the actual applications.

We consider only the first two parts, and we have

$$\begin{aligned} P &\geq P_1 + P_2 \\ &= \frac{1}{16}[2\langle vh|vh\rangle + 2\langle S_{++--}|S_{++--}\rangle + 2\langle hv|hv\rangle + 2\langle S_{++++}|S_{++++}\rangle \\ &\quad +2\langle h0|h0\rangle + (\langle h0| + \langle v0|)(|h0\rangle + |v0\rangle)] \\ &= \frac{1}{16}[2\langle hv|hv\rangle + (\langle hh| + \langle hv|)(|hh\rangle + |hv\rangle) + 2\langle vh|vh\rangle + (\langle vv| + \langle vh|)(|vv\rangle + |vh\rangle) \\ &\quad +2\langle h0|h0\rangle + (\langle h0| + \langle v0|)(|h0\rangle + |v0\rangle)]. \end{aligned} \quad \text{(A22)}$$

Obviously, a necessary condition for the minimum of $P_1 + P_2$ is that the two vectors in each of the three pairs $\{|hv\rangle, |hh\rangle\}$, $\{|vv\rangle, |vh\rangle\}$ and $\{|h0\rangle, |v0\rangle\}$ are reversed. Under this condition, we can figure out the minimum value of $P_1 + P_2$ by Lagrange multiplier,

$$P > P_1 + P_2 \geq \frac{2 - \sqrt{2}}{8}. \quad \text{(A23)}$$

Thus, in the situation that the adversary knows nothing about the authentication key, he would be discovered by Alice with a probability that is larger than

$$1 - (\frac{6 + \sqrt{2}}{8})^m. \quad \text{(A24)}$$

Next, we analyze the situation that the adversary first communicates with Bob to pry into the authentication key, and then forges Bob's identity with the information about the authentication key

he got from Bob. Similar to the processes above, we assume that the adversary prepares the following state and sends the system T to Bob,

$$|e_h\rangle_R|H\rangle_T + |e_v\rangle_R|V\rangle_T + |e_0\rangle_R|0\rangle_T, \tag{A25}$$

where $\langle e_h|e_h\rangle + \langle e_v|e_v\rangle + \langle e_0|e_0\rangle = 1$. Bob can prevent the adversary from sending multi-photon system to him by add a beam splitter and an additional detector before D_2. If the authentication key bit is 0, after Bob's operation, the whole state would become

$$|\phi_0\rangle \quad = \quad -|e_h\rangle_R|H\rangle_T|0\rangle_2 - \mathrm{i}|e_v\rangle_R|0\rangle_T|V\rangle_2 + |e_0\rangle_R|0\rangle_T|0\rangle_2. \tag{A26}$$

If the key bit is 1, the whole state would be

$$|\phi_1\rangle \quad = \quad -|e_+\rangle_R|+\rangle_T|0\rangle_2 + \mathrm{i}|e_-\rangle_R|0\rangle_T|V\rangle_2 + |e_0\rangle_R|0\rangle_T|0\rangle_2, \tag{A27}$$

where

$$|e_+\rangle = \frac{1}{\sqrt{2}}(|e_h\rangle + |e_v\rangle), \tag{A28}$$

$$|e_-\rangle = \frac{1}{\sqrt{2}}(|e_h\rangle - |e_v\rangle). \tag{A29}$$

To calculate an accurate result of the minimum error probability to discriminate $tr_2(|\phi_0\rangle\langle\phi_0|)$ and $tr_2(|\phi_1\rangle\langle\phi_1|)$ is difficult. Here, we pursue a lower bound by giving the adversary the power to access the system 2, i.e., we calculate the minimum error probability of the discrimination of $|\phi_0\rangle$ and $|\phi_1\rangle$ as a lower bound of the minimum error probability to discriminate $tr_2(|\phi_0\rangle\langle\phi_0|)$ and $tr_2(|\phi_1\rangle\langle\phi_1|)$. According to the known conclusions on quantum states discrimination, we find that

$$P_m \quad \geq \quad \frac{1}{2}(1 - \sqrt{1 - |\langle\phi_0|\phi_1\rangle|^2}). \tag{A30}$$

Now, the problem becomes finding the minimum value of $|\langle\phi_0|\phi_1\rangle|$. By substituting Equations (A26) and (A27) into the above formula, we get

$$\begin{aligned} \langle\phi_0|\phi_1\rangle &= \frac{1}{\sqrt{2}}\langle e_h|e_+\rangle - \langle e_v|e_-\rangle + \langle e_0|e_0\rangle \\ &= \frac{1}{2}\langle e_h|e_h\rangle + \frac{1}{2}\langle e_h|e_v\rangle - \frac{1}{\sqrt{2}}\langle e_v|e_h\rangle + \frac{1}{\sqrt{2}}\langle e_v|e_v\rangle + \langle e_0|e_0\rangle. \end{aligned} \tag{A31}$$

Assuming that

$$|e_h\rangle \quad = \quad (l_1\mathrm{e}^{\alpha_1\mathrm{i}}, l_2\mathrm{e}^{\alpha_2\mathrm{i}}, ...)^T, \tag{A32}$$

$$|e_v\rangle \quad = \quad (m_1\mathrm{e}^{\beta_1\mathrm{i}}, m_2\mathrm{e}^{\beta_2\mathrm{i}}, ...)^T. \tag{A33}$$

Then, Equation (A31) changes to

$$\langle\phi_0|\phi_1\rangle = \sum_k(\frac{l_k^2}{2} + \frac{m_k^2}{\sqrt{2}}) + \langle e_0|e_0\rangle + \sum_k(l_k m_k(\frac{1}{2}\mathrm{e}^{(\alpha_k-\beta_k)\mathrm{i}} - \frac{1}{\sqrt{2}}\mathrm{e}^{(\beta_k-\alpha_k)\mathrm{i}}). \tag{A34}$$

We can get the minimum of $|\langle\phi_0|\phi_1\rangle|$,

$$\frac{5\sqrt{2}-6}{8-4\sqrt{2}}, \tag{A35}$$

which appears when $\alpha_k - \beta_k = -\pi$ and $m_k = (\sqrt{2}-1)l_k$ for any k, and $\langle e_0|e_0\rangle = 0$. By further calculation, we can get the lower bound of the minimum error probability of the adversary guessing each bit of the first m authentication key,

$$p_e > \frac{1}{2}(1 - \frac{\sqrt{5-2\sqrt{2}}}{8\sqrt{2}-4}). \tag{A36}$$

Here, we did many relaxations to get the above result, and we think the tight lower bound is much larger than it. With the information about the authentication key he obtained from the above operation, the adversary could improve his attack. A relaxed lower bound of the minimum error probability the adversary introduced would be

$$P' = \frac{p_e}{2} > \frac{1}{2}(1 - \frac{\sqrt{5-2\sqrt{2}}}{16\sqrt{2}-8}) > 2.8\%. \tag{A37}$$

This means in the situation that the adversary knows nothing about the authentication key, he would be discovered by Alice with a probability that is larger than

$$1 - 0.97^m. \tag{A38}$$

Appendix A.2. Security of Alice's Identity

Since Alice only sends her communicating peer the last n signals when she has verified its identity, the adversaries cannot get any information about the last n bit of K. Therefore, the adversary can only attack without any information on K. Suppose the state the adversary sends to Bob is

$$|\phi_0\rangle_E|0\rangle_B + |\phi_H\rangle_E|H\rangle_B + |\phi_V\rangle_E|V\rangle_B, \tag{A39}$$

where $\langle\phi_0|\phi_0\rangle + \langle\phi_H|\phi_H\rangle + \langle\phi_V|\phi_V\rangle = 1$. When $s_i = 0$, for each signal, Bob will find the existence of the adversary when his detector clicks, with the probability

$$P' = \frac{\langle\phi_V|\phi_V\rangle}{4} + \frac{(-\mathrm{i}\rangle\phi_H + \mathrm{i}\rangle\phi_V|)(\mathrm{i}|\phi_H\rangle - \mathrm{i}|\phi_V\rangle)}{2}. \tag{A40}$$

When $s_i = 1$, the expectations of the probability that Bob's detector clicks are

$$\langle\phi_H|\phi_H\rangle, \tag{A41}$$

and

$$\frac{(\mathrm{i}\rangle\phi_H + \mathrm{i}\rangle\phi_V|)(\mathrm{i}|\phi_H\rangle - \mathrm{i}|\phi_V\rangle)}{2}, \tag{A42}$$

which should be about $1/2$. For simplicity, here we suppose that Bob would accept Alice's identity if both probabilities are in the interval of $[4/9, 5/9]$. Then, we can get a relaxed lower bound of the error probability that the adversary would introduce,

$$\frac{1}{2}(b^2 + \frac{(a-b)^2}{2}) = \frac{3}{2}((b - \frac{a}{2})^2 + \frac{2a^2}{9}) \geq 6.5\%, \tag{A43}$$

where $a = \langle\phi_H|\phi_H\rangle$ and $b = \langle\phi_V|\phi_V\rangle$.

References

1. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual IEEE Symposium on Foundations of Computer Science, Santa Fe, NM, USA, 20–22 November 1994.

2. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 9–12 December 1984.
3. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [CrossRef]
4. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef]
5. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dusek, M.; Luetkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
6. Long, G.-L.; Liu, X. Theoretically efficient high-capacity quantum key distribution scheme. *Phys. Rev. A* **2002**, *65*, 032302. [CrossRef]
7. Deng, F.-G.; Long, G.-L. Controlled order rearrangement encryption for quantum key distribution. *Phys. Rev. A* **2003**, *68*, 042315. [CrossRef]
8. Bostrom, K.; Felbinger, T. Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.* **2002**, *89*, 187902. [CrossRef] [PubMed]
9. Lin, S.; Wen, Q.-Y.; Zhu, F.-C. Quantum secure direct communication with x-type entangled states. *Phys. Rev. A* **2008**, *78*, 064304. [CrossRef]
10. Gao, F.; Qin, S.-J.; Wen, Q.-Y.; Zhu, F.-C. Cryptanalysis of multiparty controlled quantum secure direct communication using Greenberger-Horne-Zeilinger state. *Opt. Commun.* **2010**, *283*, 192. [CrossRef]
11. Huang, W.; Wen, Q.-Y.; Jia, H.-Y.; Qin, S.-J.; Gao, F. Fault tolerant quantum secure direct communication with quantum encryption against collective noise. *Chin. Phys. B* **2012**, *21*, 100308. [CrossRef]
12. Cleve, R.; Gottesman, D.; Lo, H.K. How to share a quantum secret. *Phys. Rev. Lett.* **1999**, *83*, 648–651. [CrossRef]
13. Hillery, M.; Buzek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829. [CrossRef]
14. Yang, Y.-G.; Wen, Q.-Y.; Zhang, X. Multiparty simultaneous quantum identity authentication with secret sharing. *Sci. China-Phys. Mech. Astron.* **2008**, *51*, 321–327. [CrossRef]
15. Qin, S.-J.; Gao, F.; Wen, Q.-Y.; Zhu, F.-C. Security of quantum secret sharing with two-particle entanglement against individual attacks. *Quant. Inf. Comput.* **2009**, *9*, 765–772.
16. Lin, S.; Wen, Q.-Y.; Qin, S.-J.; Zhu, F.-C. Multiparty quantum secret sharing with collective eavesdropping-check. *Opt. Commun.* **2009**, *282*, 4455–4459. [CrossRef]
17. Wang, T.-Y.; Wen, Q.-Y. Security of a kind of quantum secret sharing with single photons. *Quant. Inf. Comput.* **2011**, *11*, 434–443.
18. Giovannetti, V.; Lloyd, S.; Maccone, L. Quantum private queries. *Phys. Rev. Lett.* **2008**, *100*, 230502. [CrossRef] [PubMed]
19. Jakobi, M.; Simon, C.; Gisin, N.; Branciard, C.; Bancal, J.-D.; Walenta, N.; Zbinden, Z. Practical private database queries based on a quantum-key-distribution protocol. *Phys. Rev. A* **2011**, *83*, 022301. [CrossRef]
20. Gao, F.; Qin, S.; Huang, W.; Wen, Q.Y. Quantum private query: A new kind of practical quantum cryptographic protocol. *Sci. China Phys. Mech. Astron.* **2019**, *62*, 70301. [CrossRef]
21. Gao, F.; Liu, B.; Huang, W.; Wen, Q.Y. Postprocessing of the oblivious key in quantum private query. *IEEE J. Sel. Top. Quant.* **2015**, *21*, 6600111.
22. Liu, B.; Gao, F.; Huang, W.; Wen, Q.Y. QKD-based quantum private query without a failure probability. *Sci. China-Phys. Mech. Astron.* **2015**, *58*, 100301. [CrossRef]
23. Wei, C.-Y.; Cai, X.-Q.; Liu, B.; Wang, T.-Y.; Gao, F. A generic construction of quantum-oblivious-transfer-based private query with ideal database security and zero failure. *IEEE T Comput.* **2018**, *67*, 2–8. [CrossRef]
24. Huang, W.; Su, Q.; Xu, B.-J.; Liu, B.; Fan, F.; Jia, H.Y.; Yang, Y.H. Improved multiparty quantum key agreement in travelling mode. *Sci. China Phys. Mech. Astron.* **2016**, *59*, 120311. [CrossRef]
25. Huang, W.; Wen, Q.-Y.; Liu, B.; Su, Q.; Qin, S.-J.; Gao, F. Quantum anonymous ranking. *Phys. Rev. A* **2014**, *89*, 032325. [CrossRef]
26. Xu, B.-J.; Chen, Z.-Y.; Li, Z.-Y.; Yang, J.; Su, Q.; Huang, W.; Zhang, Y.; Guo, H. High speed continuous variable source-independent quantum random number generation. *Quantum Sci. Technol.* **2019**, *4*, 025013. [CrossRef]

27. Noh, T.-G. Counterfactual Quantum Cryptography. *Phys. Rev. Lett.* **2009**, *103*, 230501. [CrossRef]
28. Kwiat, P.G.; White, A.G.; Mitchell, J.R.; Nairz, O.; Weihs, G.; Weinfurter, H.; Zeilinger, A. High-efficiency quantum interrogation measurements via the quantum Zeno effect. *Phys. Rev. Lett.* **1999**, *83*, 4725–4728. [CrossRef]
29. Hosten, O.; Rakher, M.T.; Barreiro, J.T.; Peters, N.A.; Kwiat, P.G. Counterfactual quantum computation through quantum interrogation. *Nature* **2006**, *439*, 949–952. [CrossRef]
30. Sun, Y.; Wen, Q.-Y. Counterfactual quantum key distribution with high efficiency. *Phys. Rev. A* **2010**, *82*, 052318. [CrossRef]
31. Yin, Z.-Q.; Li, H.-W.; Chen, W.; Han, Z.-F.; Guo, G.-C. Security of counterfactual quantum cryptography. *Phys. Rev. A* **2010**, *82*, 042335. [CrossRef]
32. Ren, M.; Wu, G.; Wu, E.; Zeng, H. Experimental demonstration of counterfactual quantum key distribution. *Laser Phys.* **2011**, *21*, 755–760. [CrossRef]
33. Brida, G.; Cavanna, A.; Degiovanni, I.P.; Genovese, M.; Traina, P. Experimental realization of counterfactual quantum cryptography. *Laser Phys. Lett.* **2012**, *9*, 247–252. [CrossRef]
34. Liu, Y.; Ju, L.; Liang, X.-L.; Tang, S.-B.; Tu, G.-L.S.; Zhou, L.; Peng, C.-Z.; Chen, K.; Chen, T.Y.; Chen, Z.-B.; et al. Experimental Demonstration of Counterfactual Quantum Communication. *Phys. Rev. Lett.* **2012**, *109*, 030501. [CrossRef]
35. Yin, Z.-Q.; Li, H.-W.; Yao, Y.; Zhang, C.-M.; Wang, S.; Chen, W.; Guo, G.-C.; Han, Z.-F. Counterfactual quantum cryptography based on weak coherent states. *Phys. Rev. A* **2012**, *86*, 022313. [CrossRef]
36. Zhang, S.; Wang, J.; Tang, C.-J. Security proof of counterfactual quantum cryptography against general intercept-resend attacks and its vulnerability. *Chin. Phys. B* **2012**, *21*, 060303. [CrossRef]
37. Zhang, S.; Wang, J.; Tang, C.J. Counterfactual attack on counterfactual quantum key distribution. *Europhys. Lett.* **2012**, *98*, 30012. [CrossRef]
38. Li, Y.-B. Analysis of counterfactual quantum key distribution using error-correcting theory. *Quantum Inf. Process.* **2014**, *13*, 2325–2342. [CrossRef]
39. Liu, X.; Zhang, B.; Wang, J.; Tang, C.; Zhao, J.; Zhang, S. Eavesdropping on counterfactual quantum key distribution with finite resources. *Phys. Rev. A* **2014**, *90*, 022318. [CrossRef]
40. Chen, Y.; Gu, X.; Jiang, D.; Xie, L.; Chen, L. Counterfactual quantum cryptography network with untrusted relay. *Int. J. Mod. Phys. B* **2015**, *29*, 1550134. [CrossRef]
41. Yang, X.; Wei, K.; Ma, H.; Sun, S.; Du, Y.; Wu, L. Trojan horse attacks on counterfactual quantum key distribution. *Phys. Lett. A* **2016**, *380*, 1589–1592. [CrossRef]
42. Salih, H.; Li, Z.-H.; Al-Amri, M.; Zubairy, M.S. Protocol for Direct Counterfactual Quantum Communication. *Phys. Rev. Lett.* **2013**, *110*, 170502. [CrossRef]
43. Cao, Y.; Li, Y.-H.; Cao, Z.; Yin, J.; Chen, Y.-A.; Yin, H.-L.; Chen, T.Y.; Ma, X.; Peng, C.Z.; Pan, J.W. Direct counterfactual communication via quantum Zeno effect. *Proc. Natl. Acad. Sci. USA* **2017**, *114*, 4920–4924. [CrossRef]
44. Zhang, S. Probabilistic direct counterfactual quantum communication. *Chin. Phys. B* **2017**, *26*, 020304. [CrossRef]
45. Zhang, J.-L.; Guo, F.-Z.; Gao, F.; Liu, B.; Wen, Q.-Y. Private database queries based on counterfactual quantum key distribution. *Phys. Rev. A* **2013**, *88*, 022334. [CrossRef]
46. Zhang, S.; Wang, J.; Tang, C.-J. Counterfactual Quantum Deterministic Key Distributionl. *Commun. Theor. Phys.* **2013**, *59*, 27–31. [CrossRef]
47. Salih, H. Tripartite counterfactual quantum cryptography. *Phys. Rev. A* **2014**, *90*, 012333. [CrossRef]
48. Shenoy, A.H.; Srikanth, R.; Srinivas, T. Counterfactual quantum certificate authorization. *Phys. Rev. A* **2014**, *89*, 052307. [CrossRef]
49. Guo, Q.; Cheng, L.-Y.; Chen, L.; Wang, H.-F.; Zhang, S. Counterfactual quantum-information transfer without transmitting any physical particles. *Sci. Rep.* **2015**, *5*, 8516. [CrossRef] [PubMed]
50. Li, Z.-H.; Al-Amri, M.; Zubairy, M.S. Direct counterfactual transmission of a quantum state. *Phys. Rev. A* **2015**, *92*, 052315. [CrossRef]
51. Arvidsson-Shukur, D.R.M.; Barnes, C.H.W. Quantum counterfactual communication without a weak trace. *Phys. Rev. A* **2016**, *94*, 062303. [CrossRef]

52. Wang, T.-Y.; Li, Y.-P.; Zhang, R.-L. Analysis of Counterfactual Quantum Certificate Authorization. *Int. J. Theor. Phys.* **2016**, *55*, 5331–5335. [CrossRef]
53. Guo, Q.; Zhai, S.; Cheng, L.-Y.; Wang, H.-F.; Zhang, S. Counterfactual quantum cloning without transmitting any physical particles. *Phys. Rev. A* **2017**, *96*, 052335. [CrossRef]