entropy

MDPI

Article

A New Quantum Multiparty Simultaneous Identity Authentication Protocol with the Classical Third-Party

Xiang Li [1], Kejia Zhang [1,2,*], Long Zhang [1] and Xu Zhao [1]

[1] School of Mathematical Science, Heilongjiang University, Harbin 150080, China; 2190985@s.hlju.edu.cn (X.L.); lzhang@hlju.edu.cn (L.Z.); 2190972@s.hlju.edu.cn (X.Z.)

[2] State Key of Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China

* Correspondence: zhangkejia@hlju.edu.cn

Abstract: To guarantee information security in communication, quantum identity authentication plays a key role in politics, economy, finance, daily life and other fields. In this paper, a new quantum multiparty simultaneous identity authentication protocol with Greenberger–Home–Zeilinger (GHZ) state is presented. In this protocol, the authenticator and the certified parties are the participants with quantum ability, whereas the third party is a classical participant. Here, the third-party is honest and the other two parties may be dishonest. With the help of a classical third-party, a quantum authenticator and the multiple certified parties can implement two-way identity authentication at the same time. It reduces the quantum burden of participants and lowers down the trustworthiness, which makes the protocol be feasible in practice. Through further security analysis, the protocol can effectively prevent an illegal dishonest participant from obtaining a legitimate identity. It shows that the protocol is against impersonation attack, intercept-measure-resend attack and entangle-measure attack, etc. In all, the paper provides positive efforts for the subsequent security identity authentication in quantum network.

Keywords: quantum authentication; multiparty authentication; GHZ state; identity authentication

check for updates

Citation: Li, X.; Zhang, K.; Zhang, L.; Zhao, X. A New Quantum Multiparty Simultaneous Identity Authentication Protocol with the Classical Third-Party. *Entropy* **2022**, *24*, 483. https://doi.org/10.3390/e24040483

Academic Editors: Vladyslav Usenko, Stefano Olivares and Marcin Jarzyna

Received: 11 February 2022
Accepted: 28 March 2022
Published: 30 March 2022

1. Introduction

In the past few years, with the rapid development of quantum computing, existing cryptographic schemes face the security threat that the scheme can not resist quantum computing attacks. In order to solve this security problem, the idea of applying quantum technology to the cryptography scheme is proposed, and then quantum cryptography appears. In quantum cryptography, the security is guaranteed by the Heisenberg uncertainty principle, quantum non-cloning theorem and other quantum mechanics principles, which is no longer based on mathematical difficulties problems. With the development of quantum cryptography, various different types of quantum cryptography protocols have been proposed, which mainly involves Quantum Key Distribution (QKD) [1–3], Quantum Secure Direct Communication (QSDC) [4–6], Quantum Authentication (QA) [7–11], etc. Among them, quantum authentication is becoming an important branch and has attracted more and more attention. Quantum authentication can generally be divided into the following aspects: quantum message authentication (QMA) [12–14], quantum entity authentication (QEA) [11,15,16], quantum identity authentication (QIA) [17–20]. Since authentication is a prerequisite for completing many quantum protocols, it will have more important application prospects in practice.

In 1999, by combining quantum key distribution and classical identification procedure, Dušek et al. first designed a secure identity authentication system [21]. In 2000, Zeng et al. put forward a quantum key verification protocol, which quantum identity authentication occurs while completing the quantum key verification [22]. In 2002, Takashi et al. presented three types of quantum identification schemes [23]. They completed two quantum identifications by using the entangled states and introducing a trusted authority. Besides, a quantum message authentication scheme was proposed via combining the quantum cryptosystem with the ordinary authentication. Until then, most QIA schemes only involved simple authentication between two or three users, but few authentications involved multiple parties. In 2006, Wang et al. proposed a multiparty simultaneous identity authentication (MSQIA) protocol based on entanglement swapping [24]. All the users in the protocol can be authenticated by a trusted third party (TTP) simultaneously. In 2013, Yang et al. proposed a quantum protocol for (t,n)-threshold identity authentication based on GHZ States [25]. In the MSQIA protocol, the trusted third party (TTP) can authenticate the users simultaneously when and only when t or more users among n apply for authentication.

In 2017, Hong et al. presented a QIA protocol based on single photons [26]. The protocol does not require any quantum memory registration and quantum entangled states to complete the authentication. In 2019, Zawadzki et al. proposed an improved version with better security for the protocol of Hong et al. [27]. The improved protocol does not require an authenticated classic channel, Bob simply confirms or denies the entire authentication transaction. In the same year, Zhang et al. presented a quantum simultaneous identity authentication based on Bell states [28]. With the help of a third party, the mutual identity authentication protocol was designed by combining Bell states and Pauli operations. This protocol can prevent a third party from knowing the originally shared key. Then, Jiang et al. proposed a mutual simultaneous identity authentication protocol between quantum user and classical user by using Bell states in 2021, which did not require the third party or complicated operations [29]. In the protocol, only the single-qubit measurement and XOR operations were performed to complete the authentication. Nevertheless, the protocols mentioned above cannot achieve multiparty simultaneous authentication.

However, in real life, it is difficult for the third-party to have quantum capability. In this paper, a new quantum multiparty simultaneous identity authentication protocol based on $(r+1)$-particle GHZ state the classical third-party is presented. In the protocol, the third-party does not require to prepare any quantum resources during quantum authentication communication. Moreover, the third-party only perform certain operations in the initial registration and the final certification stage, and he does not participate in the following steps. Thus, the authority of third-party is reduced and the protocol is more reasonable in reality. Furthermore, in our protocol, authenticator randomly generates quantum resource, whereas the authenticated users require to conduct measurement and reflection operations, etc.

The rest of the paper is organized as follows: in Section 2, some preliminaries are presented in this section. In Section 3, a quantum multiparty simultaneous identification protocol is proposed. In Section 4, the security analysis is described in detail. Finally, a conclusion is given in Section 5.

2. Preliminaries

The following basic theories needed to complete the authentication protocol. The $(r+1)$-particle GHZ state is widely used in quantum communication, it can be expressed as:

$$|G_{\pm}\rangle_{12\cdots r(r+1)} = \frac{1}{\sqrt{2}}(|\underbrace{g_0 g_1 \cdots g_r}_{r+1}\rangle \pm |\underbrace{(g_0 \oplus 1)(g_1 \oplus 1) \cdots (g_r \oplus 1)}_{r+1}\rangle) \tag{1}$$

where $g_i \in \{0,1\}(i = 0,1,\cdots,r)$, $\oplus$ is the XOR operation, $|1\rangle$ and $|0\rangle$ are the two eigenstates of the Z-basis.

3. Quantum Multiparty Identity Authentication Protocol

In this section, we will introduce the details of our multi-party simultaneous identity authentication protocol. *Alice* is an authenticator, whereas $Bob_1, Bob_2, \cdots, Bob_r$ are the certified users. We suppose that a third party, *Trent*, can help user *Alice* to simultaneously authenticate the identity of r legal users $Bob_1, Bob_2, \cdots, Bob_r$. The process of identity authentication protocol is shown in Figure 1. There are no noise and losses in the quantum channel.

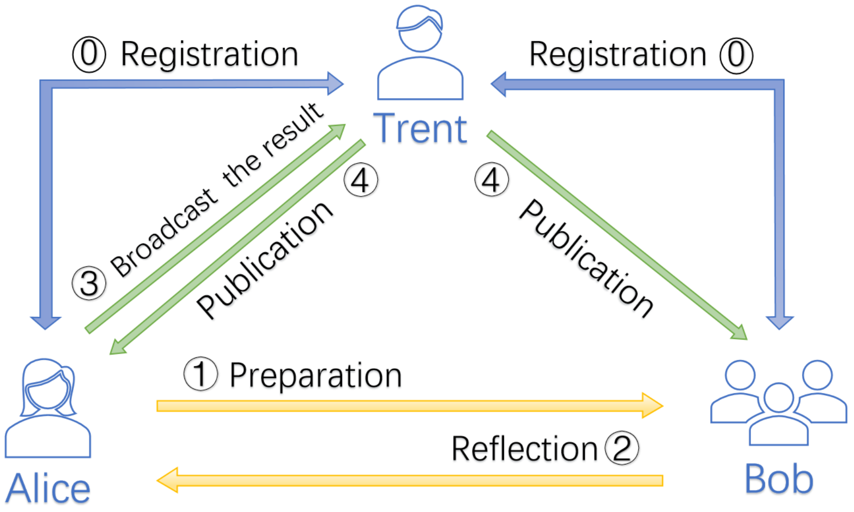

Figure 1. The process of quantum multiparty identity authentication protocol. (**0**): *Trent* shares secret keys with other users during the registration phase. (**1**): *Alice* sends quantum sequences to the $Bob_1, Bob_2, \cdots, Bob_r$ separately during the preparation phase. (**2**): $Bob_1, Bob_2, \cdots, Bob_r$ send the measured and operated particles to *Alice*, respectively. (**3**): At this stage, *Alice* announces her calculation results to *Trent*. (**4**): Finally, *Trent* compares the results to determine whether the authentication is successful and announces it to all users at the same time. At this point, the agreement is complete. In addition, the figure omits detecting eavesdropping stages for easy viewing. Nonetheless, these steps is essential in the protocol.

3.1. Registration

In the beginning, *Alice* and Bob_i $(i = 1, 2, \cdots, r)$ are registered with *Trent*, then their legal identification will be determined, respectively. In other words, each of them shares a secret identity number K with *Trent*. The secret identity number $K_{A_0}, K_{B_1}, K_{B_2}, \cdots, K_{B_r}$ between *Trent* and *Alice* or $Bob_1, Bob_2, \cdots, Bob_r$ are represented by

$$\begin{cases} K_{A_0} = \{K_{A_{01}}, K_{A_{02}}, \cdots, K_{A_{0N}}\} \\ K_{B_1} = \{K_{B_{11}}, K_{B_{12}}, \cdots, K_{B_{1N}}\} \\ K_{B_2} = \{K_{B_{21}}, K_{B_{22}}, \cdots, K_{B_{2N}}\} \\ \vdots \\ K_{B_r} = \{K_{B_{r1}}, K_{B_{r2}}, \cdots, K_{B_{rN}}\} \end{cases} \tag{2}$$

where $K_{A_{0i}} \in \{0,1\}(i = 1, 2, \cdots, N)$ and $K_{B_{i1}}, K_{B_{i2}}, \cdots, K_{B_{iN}} \in \{0,1\}(i = 1, 2, \cdots, r)$.

3.2. Authentication

3.2.1. Preparation

Alice randomly generates a sequence of N $(r+1)$-particle GHZ states quantum systems, each of which is in the form

$$\begin{cases} |G_1\rangle = \frac{1}{\sqrt{2}}\left(|S_{A_{01}}S_{B_{11}} \cdots S_{B_{r1}}\rangle + |(S_{A_{01}} \oplus 1)(S_{B_{11}} \oplus 1) \cdots (S_{B_{r1}} \oplus 1)\rangle\right)_{A_{01}B_{11}\cdots B_{r1}} \\ |G_2\rangle = \frac{1}{\sqrt{2}}\left(|S_{A_{02}}S_{B_{12}} \cdots S_{B_{r2}}\rangle + |(S_{A_{02}} \oplus 1)(S_{B_{12}} \oplus 1) \cdots (S_{B_{r2}} \oplus 1)\rangle\right)_{A_{02}B_{12}\cdots B_{r2}} \\ \vdots \\ |G_N\rangle = \frac{1}{\sqrt{2}}\left(|S_{A_{0N}}S_{B_{1N}} \cdots S_{B_{rN}}\rangle + |(S_{A_{0N}} \oplus 1)(S_{B_{1N}} \oplus 1) \cdots (S_{B_{rN}} \oplus 1)\rangle\right)_{A_{0N}B_{1N}\cdots B_{rN}} \end{cases} \tag{3}$$

where the subscripts $A_{0m}B_{1m}B_{2m} \cdots B_{rm}$ $(m = 1, 2, \cdots, N)$ represent the $(r+1)$-particles of the m-th GHZ states. *Alice* divides all the particle of these GHZ states into $(r+1)$ ordered sequences $S_{A_0}, S_{B_1}, S_{B_2}, \cdots, S_{B_r}$. Next, *Alice* randomly generates rN decoy photons from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and inserts N decoy photons into $S_{B_1}, S_{B_2}, \cdots, S_{B_r}$, respectively. Finally, $Alice$ holds sequence S_{A_0} and transmits the sequences $S_{B_1}, S_{B_2}, \cdots, S_{B_r}$ to $Bob_1, Bob_2, \cdots, Bob_r$, respectively.

3.2.2. The First Eavesdropping Detection

Once $Bob_1, Bob_2, \cdots, Bob_r$ received sequences $S_{B_1}, S_{B_2}, \cdots, S_{B_r}$, $Alice$ announces the initial positions of the rN decoy qubits. Afterwards, $Bob_1, Bob_2, \cdots, Bob_r$ store the sequence briefly. Then they select a subset of N decoy particles to perform the following operations: measuring the decoy photons on the Z-bases or X-bases randomly; preparing states which are same to the measured results; transmitting these decoy states from $S_{B_1}, S_{B_2}, \cdots, S_{B_r}$ to $Alice$, respectively.

Once confirming that $Alice$ has received the states, $Bob_1, Bob_2, \cdots, Bob_r$ publish the positions, measurement results and measurement bases of the corresponding decoy photons sequence, respectively. $Alice$ will measure these particles by using the same basis and get the measured result R , then compare R with the measured result of her initial prepared state and checks whether the results are correct.

At last, $Alice$ computes the total error rate. If the error rate of these particles is acceptable, the protocol will continue. Otherwise, they will give up continuing to authenticate.

3.2.3. Measurement and Operation

$Bob_1, Bob_2, \cdots, Bob_r$ separately make Z-basis measurements on the $S_{B_1}, \cdots, S_{B_r}$ sequences and record the measurement results $R_{B_1}, R_{B_2}, \cdots, R_{B_r}$. Then they perform the following operation in order according to the secret identity number $K_{A_0}, K_{B_1}, \cdots, K_{B_r}$, respectively. If the bit of authentication key is 0, $Bob_1, Bob_2, \cdots, Bob_r$ will perform X operation on the particles which are in the sequences $S_{B_1}, S_{B_2}, \cdots, S_{B_r}$, respectively. If the bit of authentication key is 1, $Bob_1, Bob_2, \cdots, Bob_r$ will implement Y operation on the corresponding particles of sequences $S_{B_1}, S_{B_2}, \cdots, S_{B_r}$. The specific operations and corresponding conversion results are shown in Table 1.

Table 1. The conversion mode of measurement result.

Quantum Bit	Opreation	Conversion Mode
bit = 0	X: Measuring the received particles and preparing the same particles.	$\|0\rangle \longrightarrow \|0\rangle$ $\|1\rangle \longrightarrow \|1\rangle$
bit = 1	Y: Measuring the received particles and preparing the opposite particles.	$\|0\rangle \longrightarrow \|1\rangle$ $\|1\rangle \longrightarrow \|0\rangle$

Next, $Bob_1, Bob_2, \cdots, Bob_r$ insert N decoy photons from $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ into the sequence $R_{B_1}, R_{B_2}, \cdots, R_{B_r}$, respectively. At this point, sequence $R_{B_1}, R_{B_2}, \cdots, R_{B_r}$ is converted to sequence $R'_{B_1}, R'_{B_2}, \cdots, R'_{B_r}$. At last, $Bob_1, Bob_2, \cdots, Bob_r$ transfer the sequences $R'_{B_1}, R'_{B_2}, \cdots, R'_{B_r}$ to $Alice$.

3.2.4. The Second Eavesdropping Detection

Firstly, $Bob_1, Bob_2, \cdots, Bob_r$ confirm that $Alice$ has received the sequence $R'_{B_1}, R'_{B_2}, \cdots, R'_{B_r}$. Then they announce the positions, measurement results and measurement bases of the corresponding N decoy photons in the sequences, respectively. After that, $Alice$ performs the same operation as the first detection eavesdrop. Finally, $Alice$ counts the total error rate. If the error rate exceeds the security threshold, the protocol will be terminated. Otherwise, they will continue to authenticate.

3.2.5. Verification

After passing the second eavesdropping detection, sequences $R'_{B_1}, R'_{B_2}, \cdots, R'_{B_r}$ are restored to $R_{B_1}, R_{B_2}, \cdots, R_{B_r}$ by $Alice$. Then she performs Z-basis measurement on the qubits at the corresponding positions of $S_{A_0}, R_{B_1}, R_{B_2}, \cdots, R_{B_r}$. After the measurement, according to the conversion rules are shown in Table 2, the measurement results are converted into classical results $x, \bar{R}_{B_1}, \bar{R}_{B_2}, \cdots, \bar{R}_{B_r}$, which can be denoted as

$$\begin{cases} x = [x_1, x_2, \cdots, x_N] \\ \bar{R}_{B_1} = \left[R_{B_{11}}, R_{B_{12}}, \cdots, R_{B_{1N}}\right] \\ \bar{R}_{B_2} = \left[R_{B_{21}}, R_{B_{22}}, \cdots, R_{B_{2N}}\right] \\ \vdots \\ \bar{R}_{B_r} = \left[R_{B_{r1}}, R_{B_{r2}}, \cdots, R_{B_{rN}}\right] \end{cases} \tag{4}$$

Then *Alice* publishes the results of $Q_j = x_j \oplus y_j \oplus z_j$, where x_j is the measurement result of $S_{A_0}, y_j = R_{B_{1j}} \oplus R_{B_{2j}} \oplus \cdots \oplus R_{B_{rj}}$, $z_j = S_{A_{0j}} \oplus S_{B_{1j}} \oplus S_{B_{2j}} \oplus \cdots \oplus S_{B_{rj}}$ ($j = 1, 2, \cdots, N$ and $\oplus$ is the XOR operation). Afterward, *Trent* calculates $Q'_j = K_{A_{0j}} \oplus K_{B_{1j}} \oplus \cdots \oplus K_{B_{rj}}$. If $Q'_j = Q_j$, *Alice* and $Bob_1, Bob_2, \cdots, Bob_r$ will be seen as legitimate participants. Otherwise, there will be illegal communicators in the protocol. Finally, *Trent* announces to *Alice* and $Bob_1, Bob_2, \cdots, Bob_r$ whether the certification is successful.

Table 2. The conversion rule of measurement result.

Measurement Result	Classical Result
$\vert 0\rangle$	0
$\vert 1\rangle$	1

4. Security Analysis

Security is the most important part of quantum communication protocols. In this section, the security of the multiparty identity authentication protocol is discussed. During the transmitting procedure of quantum signals, there may be an eavesdropper who wants to pass the identity authentication by illegal operations. In general, eavesdroppers are divided into two situations, which are internal eavesdropper and external eavesdropper. Next, the security of the protocol is analyzed for both aspects.

4.1. Internal Attack

4.1.1. Impersonation Attack

In the proposed quantum multiparty identity authentication protocol, *Alice* is the authenticator and resource provider, whereas $Bob_1, \cdots, Bob_r$ play the authenticated roles. In this subsection, Bob_e is one of $Bob_1, \cdots, Bob_r$ and he may have two methods to execute the impersonation attack.

On the one hand, we suppose that attacker Bob_e attempts to impersonate verifier *Alice*. Bob_e randomly generates quantum states and allocates entangled particles to $Bob_1, \cdots, Bob_r$. In the paper, Bob_e can follow the protocol steps faithfully, but he tries to extract the authentication keys between *Trent* and *Alice*. When Bob_e proceeded to the Section 3.2.5, he could only perform random XOR operations on qubits due to his ignorance of the pre-shared key K_{A_0}. He also does not know the measurement results x of sequence S_{A_0}. If Bob wants to publish the calculation results Q_i, he will need to randomly choose one of the classical bit values of 0 or 1 to perform the XOR operations. Therefore, the probability that Bob_e can successfully impersonate *Alice* is $\frac{1}{2^N}$. As shown on the left of Figure 2, when the number N of particles is large enough, the probability $P_1 = 1 - \frac{1}{2^N}$ of failure of Bob_e approximates 1.

On the other hand, attacker Bob_e may impersonate the legitimate user $Bob_j (e \neq j)$. Firstly, Bob_j has previously registered his identity information with *Trent*. That is, he has shared the secret identity key with *Trent*. In Section 3.2.3, Bob_e requires to perform corresponding operation on the measurement result R_{B_j} by combining Bob_j's identity numbers K_{B_j} and the transition rules of Table 1. Next, although Bob_e knows the conversion rules, he is ignorant of Bob_j's identity K_{B_j}. Hence he can perform X or Y operations on the received sequence randomly. The probability of choosing either the correct operation or the incorrect operation is $\frac{1}{2}$. Besides, the probability that the Bob_e gets the correct conversion result is $\frac{1}{2^N}$. Finally, the probability $P_2 = 1 - \frac{1}{2} \times \frac{1}{2^N}$ of Bob_e's attack being found tends to be 1 in the Figure 2. Therefore, the protocol can effectively resist impersonation attacks.

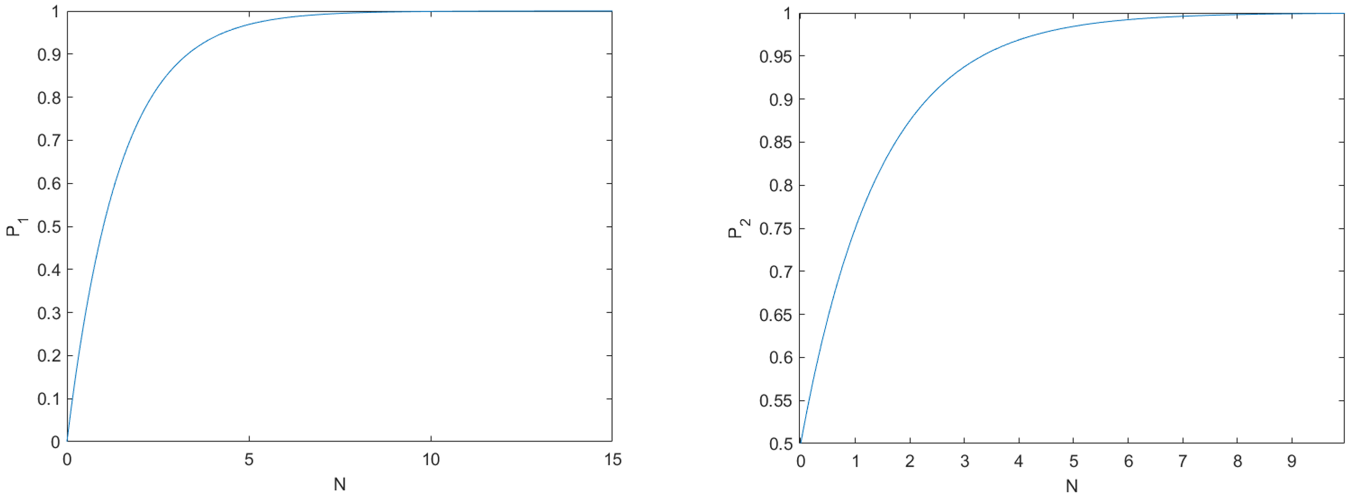

Figure 2. (**Left**) the probability P_1 of Bob_e being detected. (**Right**) the probability P_2 of Bob_e being detected.

4.1.2. Entangle and Measure Attack

Moreover, we discuss whether some illegal users can get secret information through entanglement measurement attack in the process of information interaction. When the qubits are sent from $Alice$ to Bob_j, we suppose Bob_E performs operation U_E on the system composed of decoy photons $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$and the ancillary state which is prepared by Bob_E as U_E . We can get

$$\begin{aligned} U_E|0\rangle|e\rangle &= a|0\rangle|e_{00}\rangle + b|1\rangle|e_{01}\rangle \\ U_E|1\rangle|e\rangle &= c|0\rangle|e_{10}\rangle + d|1\rangle|e_{11}\rangle \end{aligned} \tag{5}$$

$$\begin{aligned} &U_E|+\rangle|e\rangle = \frac{1}{\sqrt{2}}[|0\rangle(a|e_{00}\rangle + c|e_{10}\rangle) + |1\rangle(b|e_{01}\rangle + d|e_{11}\rangle)] \\ &= \frac{1}{2}[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle + c|e_{10}\rangle + d|e_{11}\rangle) + |-\rangle(a|e_{00}\rangle - b|e_{01}\rangle + c|e_{10}\rangle - d|e_{11}\rangle)] \end{aligned} \tag{6}$$

$$\begin{aligned} &U_E|-\rangle|e\rangle = \frac{1}{\sqrt{2}}[|0\rangle(a|e_{00}\rangle - c|e_{10}\rangle) + |1\rangle(b|e_{01}\rangle - d|e_{11}\rangle)] \\ &= \frac{1}{2}[|+\rangle(a|e_{00}\rangle + b|e_{01}\rangle - c|e_{10}\rangle - d|e_{11}\rangle) + |-\rangle(a|e_{00}\rangle - b|e_{01}\rangle - c|e_{10}\rangle + d|e_{11}\rangle)] \end{aligned} \tag{7}$$

where $|e_{00}\rangle, |e_{01}\rangle, |e_{10}\rangle, |e_{11}\rangle$ belong to the Hilbert space of Bob_E's probes and$|a|^2 + |b|^2 + |c|^2 + |d|^2 = 1$. After transmission, Bob_E measures ancillary qubit to get Bob_j's operations. In order to pass the eavesdropping detection without introducing any errors, he should perform the following actions:

$$\begin{cases} b = c = 0 \\ a|e_{00}\rangle + b|e_{01}\rangle - c|e_{10}\rangle - d|e_{11}\rangle = 0 \\ a|e_{00}\rangle - b|e_{01}\rangle - c|e_{10}\rangle + d|e_{11}\rangle = 0 \end{cases} \tag{8}$$

However, if $b = c = 0$, it means $a|e_{00}\rangle = d|e_{11}\rangle$. It shows that Bob_E cannot distinguish between $a|e_{00}\rangle$ and $d|e_{11}\rangle$. Hence, the proposed protocol can resist the entangle-measure attack.

4.1.3. Intercept–Measure–Resend Attack

Actually, Bob_e as one of $Bob_1, \cdots, Bob_r$ can only get his identity number from the third party $Trent$. Now, we consider whether he can get the identity of $Bob_j (e \neq j)$. First of all, he could not have obtained any related information about the identity of Bob_j by accessing

Trent since the third party is absolutely honest with our protocol. Furthermore, he also can't get the true identity of Bob_j through the intercept–measure–resend attack.

In Section 3.2.1, *Alice* inserts rN decoy photons into the sequences $S_{B_1}, S_{B_2}, \cdots, S_{B_r}$ each for the eavesdropping detection, respectively. However, Bob_e does not know the initial positions and initial states of the decoy particles in the sequence *Alice* sent to Bob_j. Bob_e is a quantum participant who can perform measurement operations on the Z-basis and X-basis. Therefore, if he wants to intercept the particle that *Alice* is transmitting to Bob_j in Section 3.2.1, the measurement based on Z-bases and X-bases randomly can be performed. There are four measurements for these bases, $|1\rangle$, $|0\rangle$, $|+\rangle$and$|-\rangle$. Furthermore, it is difficult to just select the correct N position in the $2N$ sequence. His probability of success is $\frac{1}{2} \times \frac{1}{4^N} = \frac{1}{8^N}$.

As shown on the left of Figure 3, when N is large enough, the probability $P_3 = 1 - \frac{1}{8^N}$ is approximate to 1. Therefore, it is almost impossible for illegal behavior of Bob_e not to be detected.

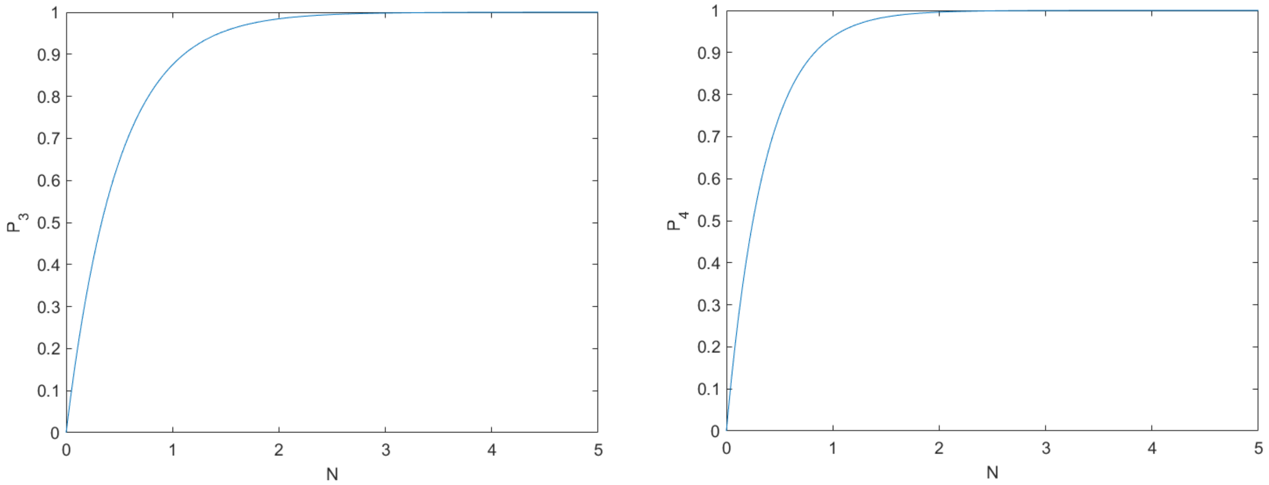

Figure 3. (**Left**) the probability P_3 of Bob_e being detected. (**Right**) the probability P_4 of *Eve* being detected.

4.2. External Attack

Unlike internal attackers, external attackers are illegal eavesdroppers from the outside. *Eve* is an eavesdropper who wishes to obtain some secret information to pass the identity authentication. *Eve* often uses the impersonation attack, the entangle and measure attack and the intercept–measure–resend attack, etc. The security of some attacks is analyzed below.

We assume that *Eve* tries to impersonate $Bob_i (i = 1, 2, \cdots, r)$. In the Section 3.2.2, *Alice* inserted rN decoy particles into the sequence and sent them to $Bob_1, Bob_2, \cdots, Bob_r$ for detection eavesdropping, respectively. After *Eve* receives the particles, she randomly measures and sends the qubits to Alice. Moreover, *Eve* randomly measures particles based on Z-basis or X-basis since she dose not know the authentication key sequence S_{B_i} shared only by *Alice* and Bob_i. The probability of her choosing the right operation is $\frac{1}{2}$ and the probability of picking the correct N particles from $2N$ sequence is $\frac{1}{3}$. Hence the probability of *Eve* being detected is P_4=$1 - \frac{1}{2} \times \frac{1}{2} \times \frac{1}{4^N}$. As shown on the right side of Figure 3, if N is large enough, the probability P_4 approximates to 1. Therefore, it is difficult for *Eve* to pass the eavesdropping detection.

Similar to impersonation attacks, *Eve* is an external attacker while in the entangle and measure attack and the intercept–measure–resend attack. *Eve* has less information than an internal attacker, hence the probabilities of failure are higher.

5. Further Discussion

In this section, we compare different models to demonstrate that our protocol may be more plausible, then comparing and summarizing the quantum authentication protocols in Table 3. Through the following comparison, it can be found that most of the existing quantum authentication protocols with the third party(TP) and our proposed protocol are two different models.

Model 1: The model of a quantum authentication protocol with a third party is simplified as follows [11,28]: Suppose *Alice* and *Bob* are two legitimate participants who want to authenticate each other, and the TP is a third party that helps them authenticate. Before the authentication protocol begins, the legitimate *Alice* and the legitimate *Bob* share a key in advance. During the authentication process, the TP will generate the quantum states and distribute them to the participants, *Alice* and *Bob* will perform operations according to the keys. Finally, the participants confirm the identity of the other party by comparing the results published by the other party.

Model 2: Our proposed protocol model is simplified as follows (for the convenience of comparison, the multi-party protocol is simplified to two parties): Suppose *Alice* and *Bob* are two legitimate participants who want to authenticate each other, and the TP is a third party that helps them authenticate. Before the authentication protocol begins, *Alice* and *Bob* register their legal identities with the TP. That is, they share the secret keys with the TP, respectively. During the authentication process, *Alice* will generate the quantum states and distribute them to herself and *Bob*, and then *Alice* and *Bob* will perform certain operations based on the keys. Finally, The TP confirms the identity of the participants by comparing the calculation results of itself and *Alice*, and announces the results to the participants.

In practice, Model 2 is more suitable for quantum multi-party authentication than Model 1. If *Alice* and $Bob_1, Bob_2, \cdots, Bob_r$ want to share keys, any two parties must share keys, which will increase a lot of unnecessary work. It is a very complicated process for each participant to share keys with each other, so we introduce a third party to actually conduct centralized key management, which simplifies the process of key distribution. Moreover, even if TP is not introduced, Model 1 can complete the mutual authentication. For example, Ref. [26] and Ref. [27] accomplish mutual authentication without introducing a third party. Therefore, in fact, our model makes more sense in practice.

Furthermore, we compare and summarize the quantum authentication protocols in Table 3. Compared with the previous quantum identity authentication, we extend the two-party authentication to multi-party authentication, which does not require all communicators to own quantum capacity. In this paper, quantum *Alice* and $Bob_1, Bob_2, \cdots, Bob_r$ are able to complete identity authentication simultaneously based on $(r+1)$-particle GHZ states with the help of classical *Trent*. Only the initial registration and the final certification stage require him to perform some classical operations, and he does not participate in the rest of the time. In other words, the rights of the third party are better reduced.

Table 3. Comparison among some different quantum authentication protocols.

Protocol	Participants	The Third Party	Quantum Resource
Wang et al. [24]	Multipartite	Quantum third party	GHZ state
Yang et al. [25]	Multipartite	Quantum third party	GHZ state
Zhang et al. [28]	Mutual	Quantum third party	Bell state
Jiang et al. [29]	Mutual	No third party	Bell state
Wu et al. [30]	Multipartite	Quantum third party	Bell state and GHZ state
Our protocol	Multipartite	Classical third party	GHZ state

6. Conclusions

In this paper, with the help of a classical third-party, a quantum multiparty simultaneous identity authentication protocol with GHZ state is presented. A trusted third-party centrally manages the keys of the participants, and $Alice$ and $Bob_1, Bob_2, \cdots, Bob_r$ complete authentication at the same time. The analysis of this protocol can effectively prevent illegal participants or attackers from obtaining legal identity information, and it can resist all kinds of ordinary attacks from the inside and outside. In addition, similar with the previous quantum multiparty simultaneous identity authentication protocol, the security analysis is based on the case of "no noise and no loss" in quantum channels [9,24,31]. In this case, our paper is also designed against the assumption of "no noise and no loss" in quantum channels. However, we need to make it clear that the security analysis under different noise rates is indeed an important content. We hope that this protocol have better application scenarios in the future.

Author Contributions: Conceptualization, X.L. and K.Z.; methodology, X.L.; software, X.L.; validation, X.L., K.Z., L.Z. and X.Z.; writing—original draft preparation, X.L.; writing—review and editing, X.L.and K.Z. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the National Natural Science Foundation of China under Grant No. 61802118, the Heilongjiang Provincial Natural Science Foundation of China under Grant No. YQ2020F013, the Open Foundation of State key Laboratory of Networking and Switching Technology (BUPT) under Grant No. SKLNST-2018-1-07. The Outstanding Youth Fund of Heilongjiang University supported Kejia Zhang.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

Abbreviations

The following abbreviations are used in this manuscript:

GHZ	Greenberger–Home–Zeilinger
QIA	Quantum Identity Authentication
QKD	Quantum Key Distribution
TTP	trusted third party

References

1. Deng, F.G.; Long, G.L. Bidirectional quantum key distribution protocol with practical faint laser pulses. *Phys. Rev. A* **2005**, *70*, 012311. [CrossRef]
2. Wang, X.; Hu, J. Quantum key distribution with the decoy-state method. *Sci. Sin. Phys. Mech. Astron.* **2011**, *41*, 459–465. [CrossRef]
3. Wu, J.Z.; Yan, L. Quantum Key Distribution Protocol Based on GHZ Like State and Bell State. In *International Conference on Artificial Intelligence and Security*; Springer: Cham, Switzerland, 2020; pp. 298–306.
4. Wang, C.; Deng, F.G.; Li, Y.S.; Liu, X.S.; Long, G.L. Quantum secure direct communication with high dimension quantum superdense coding. *Phys. Rev. A* **2005**, *71*, 044305. [CrossRef]
5. Yu, C.H.; De Guo, G.; Lin, S. Quantum secure direct communication with authentication using two nonorthogonal states. *Int. J. Theor. Phys.* **2013**, *52*, 1937–1945. [CrossRef]
6. Jin, X.R.; Ji, X.; Zhang, Y.Q.; Shou, Z.; Hong, S.K.; Yeon, K.H. Three-party quantum secure direct communication based on GHZ states. *Phys. Lett. A* **2006**, *354*, 67–70. [CrossRef]
7. Gao, T.F.; Yan, L.; Wang, Z.X. Controlled quantum teleportation and secure direct communication. *Chin. Phys.* **2005**, *14*, 893–897.
8. Lee, H.; Lim, J.; Yang, H.J. Quantum direct communication with authentication. *Phys. Rev. A* **2006**, *73*, 042305. [CrossRef]
9. Yang, Y.G.; Wen, Q.Y. Economical multiparty simultaneous quantum identity authentication based on Greenberger–Horne–Zeilinger states. *Chin. Phys. B* **2009**, *18*, 3233–3236.
10. Kang, M.S.; Choi, Y.H.; Kim, Y.S.; Cho, Y.W.; Lee, S.Y.; Han, S.W.,; Moon, S. Quantum message authentication scheme based on remote state preparation. *Phys. Scripta* **2018**, *93*, 115102. [CrossRef]

11. Kang, M.S.; Heo, J.; Hong, C.H. Controlled mutual quantum entity authentication with an untrusted third party. *Quantum Inf. Process.* **2018**, *17*, 159. [CrossRef]
12. Curty, M.; Santos, D. Quantum authentication of classical messages. *Phys. Rev. A* **2012**, *64*, 168. [CrossRef]
13. Bartkiewicz, K.; Černoch, A.; Lemr, K. Using quantum routers to implement quantum message authentication and Bell-state manipulation. *Phys. Rev. A* **2014**, *90*, 022335. [CrossRef]
14. Lee, H.; Hong, C.; Kim, H.; Lim, J.; Yang, H.J. Arbitrated quantum signature scheme with message recovery. *Phys. Lett. A* **2004**, *321*, 295–300. [CrossRef]
15. Kang, M.S.; Hong, C.H.; Heo, J.; Lim, J.I. Controlled mutual quantum entity authentication using entanglement swapping. *Chin. Phys. B* **2015**, *24*, 120–128. [CrossRef]
16. Wang, Q.; Zhang, S.; Wang, S.L.; Shi, R.H. Comment on "Controlled mutual quantum entity authentication with an untrusted third party". *Quantum Inf. Process.* **2020**, *19*, 125. [CrossRef]
17. Yuan, H.; Liu, Y.M.; Pan, G.Z.; Zhang, G.; Zhou, J.; Zhang, Z.J. Quantum identity authentication based on ping-pong technique without entanglements. *Quantum Inf. Process.* **2014**, *13*, 2535–2549. [CrossRef]
18. Ma, H.; Huang, P.; Bao, W.; Zeng, G. Continuous-variable quantum identity authentication based on quantum teleportation. *Quantum Inf. Process.* **2016**, *15*, 2605–2620. [CrossRef]
19. Chen, Z.Y.; Zhou, K.L.; Liao, Q. Quantum identity authentication scheme of vehicular ad-hoc networks. *Int. J. Theor. Phys.* **2018**, *58*, 40–57. [CrossRef]
20. Liu, B.; Gao, Z.; Xiao, D.; Huang, W.; Zhang, Z.; Xu, B. Quantum identity authentication in the counterfactual quantum key distribution protocol. *Entropy.* **2019**, *21*, 518. [CrossRef]
21. Dušek, M.; Haderka, O.; Hendrych, M.; Myška, R. Quantum identification system. *Phys. Rev. A* **1999**, *60*, 149–156. [CrossRef]
22. Zeng, G.; Zhang, W. Identity verification in quantum key distribution. *Phys. Rev. A* **2000**, *61*, 22303. [CrossRef]
23. Mihara, T. Quantum identification schemes with entanglements. *Phys. Rev. A* **2002**, *65*, 52326. [CrossRef]
24. Wang, J.; Quan, Z.; Chao, J.T. Multiparty simultaneous quantum identity authentication based on entanglement swapping. *Chin. Phys. Lett.* **2006**, *23*, 2360–2363.
25. Yang, Y.G.; Wang, H.Y.; Jia, X.; Zhang, H. A quantum protocol for (t,n)-threshold identity authentication based on greenberger-horne-zeilinger states. *Int. J. Theor. Phys.* **2013**, *52*, 524–530. [CrossRef]
26. Hong, C.H.; Heo, J.; Jang, J.G.; Kwon, D. Quantum identity authentication with single photon. *Quantum Inf. Process.* **2017**, *16*, 236. [CrossRef]
27. Zawadzki, P. Quantum identity authentication without entanglement. *Quantum Inf. Process.* **2019**, *18*, 7. [CrossRef]
28. Zhang, S.; Chen, Z.K.; Shi, R.H.; Liang, F.Y. A novel quantum identity authentication based on bell states. *Int. J. Theor. Phys.* **2020**, *59*, 236–249. [CrossRef]
29. Jiang, S.Q.; Zhou, R.G.; Hu,W.W. Semi-quantum mutual identity authentication using Bell states. *Int. J. Theor. Phys.* **2019**, *60*, 3353–3362. [CrossRef]
30. Wu, Y.; Chang, H.; Guo, G.; Lin, S. Multi-party quantum key agreement protocol with authentication. *Mod. Phys. Lett. B* **2021**, *21*, 495. [CrossRef]
31. Yang, Y.G.; Wen, Q.; Xing, Z. Multiparty simultaneous quantum identity authentication with secret sharing. *Sci. China Ser. G Phys. Mech. Astron.* **2008**, *51*, 321–327. [CrossRef]