hv photonics

IMPACT FACTOR 2.536

CITESCORE 2.3

Article

Quantum Secure Multi-Party Summation with Identity Authentication Based on Commutative Encryption

Ning Wang, Xinying Tian, Xiaodong Zhang and Song Lin

Special Issue

Quantum Communications: Technologies and Applications

Edited by

Dr. Bin Liu and Dr. Zhiwei Sun

MDPI

https://doi.org/10.3390/photonics10050558

photonics

MDPI

Article

Quantum Secure Multi-Party Summation with Identity Authentication Based on Commutative Encryption

Ning Wang [1,2], Xinying Tian [1], Xiaodong Zhang [1] and Song Lin [1,*]

[1] College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350007, China
[2] School of Information Science and Technology, Zhengzhou Normal University, Zhengzhou 450044, China
* Correspondence: lins95@fjnu.edu.cn

Abstract: In quantum secure multi-party summation protocols, some attackers can impersonate legitimate participants in the summation process, and easily steal the summation results from the participants. This is often overlooked for existing secure multi-party summation protocols, thus rendering them insecure. Based on commutative encryption, a quantum secure multi-party summation protocol with identity authentication is proposed in this paper. In the protocol, each participant encodes a secret integer on photons via unitary operations. At the same time, a one-way hash function technique with a key is utilized to perform identity authentication operations for each participant. Finally, the summation is calculated with the help of a semi-trusted third party. The analysis of the protocol shows that the proposed protocol is correct and resistant to common and impersonation attacks. Compared to related protocols, the use and measurement of single photons makes the protocol easier to implement into existing technology. Furthermore, the simulation experiments on the IBM Q Experience cloud platform demonstrate the effectiveness of the presented protocol.

Keywords: quantum cryptography; commutative encryption; quantum secure multi-party summation; identity authentication

check for updates

Citation: Wang, N.; Tian, X.; Zhang, X.; Li, S. Quantum Secure Multi-Party Summation with Identity Authentication Based on Commutative Encryption. *Photonics* **2023**, *10*, 558. https://doi.org/10.3390/photonics10050558

Received: 11 March 2023
Revised: 1 May 2023
Accepted: 5 May 2023
Published: 10 May 2023

Copyright: © 2023 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

With the rapid development of information technology, the demand for security and privacy of information transmission is increasing. The confidentiality of encryption is no longer reliable as classical communication encryption methods are gradually being breached. In order to ensure the security of information, quantum information and quantum computing have gradually become a hot topic of concern. Quantum mechanics, as the theoretical foundation of this information transmission method, is significantly different from classical physics. Its basic principles include the uncertainty principle, non-cloning, superposition principle, and quantum entanglement, etc. These principles provide theoretical support for quantum communication. Photons are the most versatile quantum carrier as they are easy to generate, manipulate, and transmit over long distances through free-space or fiber channels [1]. Moreover, they have unique properties such as non-cloning and measurement interference. The control and measurement of photon states are crucial to ensure the security and reliable transmission of information. Therefore, the role of photons in quantum communication is of great significance. Quantum communication includes various protocols and applications, such as quantum key distribution (QKD) [2–12], quantum secret sharing (QSS) [13–15], quantum key agreement (QKA) [16–18], quantum private query (QPQ) [19–21], quantum multi-party computation (QMC) [22–26], and so on.

Secure multi-party summation (SMS) is a special primitive of secure multi-party computing (MPC), which was proposed by Goldreich [27] in 1987. It aims to accomplish the task of correctly calculating the sum of the secret integers of multiple participants without exposing the secret integers. Heinrich et al. first studied sequence summation

in the quantum environment [28–30]. Since then, an increasing number of researchers have begun to explore this topic, and various quantum secure multi-party summation (QSMS) protocols have been proposed [31–46]. In 2006, Hillery et al. [31] put forward the first multi-party summation protocol using two-particle n-dimensional entangled states. Later, Chen et al. [32] presented a secure summation protocol based on multi-particle GHZ entangled states. The protocol encodes the Bell-based measurements of all participants into a single classical bit, which reduces the overhead of the classical channel. In 2014, Zhang et al. [33] designed a quantum summation protocol based on single photons in both polarization and spatial-mode degrees of freedom. In the protocol, participants can independently encode their private information on the polarisation and spatial-mode states of single photons. Shi et al. [34] proposed summation and multiplication protocols using quantum Fourier transform in 2016. These two protocols utilized entangled state as information carrier, and also makes use of CNOT gates and oracle operators to implement modulo d operation. Subsequently, Liu et al. [37] presented a quantum secure summation, which utilizes 2-particle Bell states as information carrier. Immediately afterwards, Yang et al. [39] proposed a quantum security summation protocol using n-particle d-dimensional entangled states. In this protocol, the first participant is semi-honest. Unfortunately, Zhang et al. [42] pointed out that the protocol was insecure and proposed an improved protocol. Recently, depending on some properties of Grover's search algorithm, Zhang et al. [45] put forward a quantum secure multi-party summation protocol. In this protocol, each participant's secret input is encoded onto a unitary operation on the travelling two-qubit state, and a summation is achieved with the help of a semi-trusted third party.

However, the above proposed QSMS protocols ignore the issue of authentication in their design process. In an unauthenticated SMS protocol, a malicious attacker can impersonate a legitimate participant to execute the protocol together and send a forged message to the legitimate participant, thus stealing the summation result or the secret information of the other participants. This results in the disclosure of secret information and reduces the security of the protocol. Therefore, authentication is also an important part of ensuring the secure execution of SMS protocols. Various authentication schemes have been proposed in classical SMS or SMC protocols, such as [47,48]. Similarly, when exploiting quantum properties to improve the security of SMS protocols, the authentication security of the participants is also urgent to be enhanced. Furthermore, the above QSMS protocol utilises multi-particle entangled states in calculating the sum of participant secrets, and its preparation and storage is undoubtedly difficult with current technology. Consequently, it is worthwhile to investigate how to design a secure multi-party summation protocol with authentication and easy implementation in the current quantum technology background.

Considering existing technical conditions, we propose an authenticated QSMS protocol based on exchange encryption in this paper. In this protocol, each participant has an identification and shares an encryption key with a semi-trusted third party, who prepares single photos as information carriers. First, the third party performs an identity encoding operation on the photos using a one-way hash function technique with a key. Then, all participants encode the secret integer and perform the identity authentication operation on photons in order. Finally, with the help of the semi-trusted third party, the participants complete their identity authentication and obtain the summation result of their secret integers. Compared to related protocols, the proposed protocol is not only feasible with current technology, but can also resist impersonation attacks, which increases the practicality of the protocol.

The rest of the paper is organized as follows. In Section 2, we briefly introduce the idea of commutative encryption. Then, an authenticated QSMS protocol based on commutative encryption is described and given as an example in Section 3. In Section 4, the correctness and security of the proposed protocol are analyzed, and our protocol is compared with the existing protocols. In Section 5, simulation experiments are conducted on the IBM Q Experience cloud platform to confirm the feasibility of the proposed protocol. Finally, a brief conclusion is given in Section 6.

2. Quantum Commutative Encryption

In this section, we introduce the idea of quantum commutative encryption [49], which will be used in the proposed quantum secure multi-party summation protocol. In our protocol, the horizontally polarised photon $|0\rangle$ signifies binary 0, the vertically polarised photon $|1\rangle$ denotes binary 1. All transmitted polarised photons are encrypted before they are transmitted. The encryption key is defined as a set of angles $K=\{\omega_j{:}0 \leq \omega_j \leq 2\pi, j = 1, 2, \ldots, N\}$ for an N-bit message. Here the subscript j indicates the position in the message where the encryption with the angle ω_j is applied, and the encryption is defined as a rotation operation. $E_K[M]$ represents data M is encrypted with a secret key K. In order to obtain the correct initial photon, the receiver has to rotate the encrypted photon with the opposite angle of ω_j to decrypt the encrypted photon. $D_K[M]$ indicates the decryption of the data M using a secret key K. The process of encryption and decryption is described mathematically as follows.

For simplicity, we assume that the message M is a single photon encoded as $M : |\varphi\rangle = |0\rangle$. The rotation operation used can be represented by the following matrix.

$$G(\omega) = \begin{pmatrix} \sin\frac{\omega}{2} & i\cos\frac{\omega}{2} \\ i\cos\frac{\omega}{2} & \sin\frac{\omega}{2} \end{pmatrix} \tag{1}$$

After encrypting the quantum state $|\varphi\rangle$ with ω, we get the quantum state

$$\begin{aligned} |\varphi\rangle_1 = E_K[M] = G(\omega)|0\rangle &= \begin{pmatrix} \sin\frac{\omega}{2} & i\cos\frac{\omega}{2} \\ i\cos\frac{\omega}{2} & \sin\frac{\omega}{2} \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} \\ &= \begin{pmatrix} \sin\frac{\omega}{2} \\ i\cos\frac{\omega}{2} \end{pmatrix} = \sin\frac{\omega}{2}|0\rangle + i\cos\frac{\omega}{2}|1\rangle \end{aligned}, \tag{2}$$

where $|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$. In order to recover the message M, we need to rotate the photon $|\varphi\rangle_1$ by the angle in the opposite direction of ω, and the decryption process is shown below.

$$D_K[M] = G(-\omega)|\varphi\rangle_1 = \begin{pmatrix} -\sin\frac{\omega}{2} & i\cos\frac{\omega}{2} \\ i\cos\frac{\omega}{2} & -\sin\frac{\omega}{2} \end{pmatrix}\begin{pmatrix} \sin\frac{\omega}{2} \\ i\cos\frac{\omega}{2} \end{pmatrix} = -|0\rangle. \tag{3}$$

Since - is a global phase which has no observable effect on the quantum state, it is neglected in the paper. Thus, Equation (3) can eventually be abbreviated to $D_K[M] = |0\rangle$. That is, the decryption is carried out to obtain the initial quantum state $|\varphi\rangle$.

The main advantage of this encryption/decryption scheme is that when the quantum state is encrypted j ($j = 1, 2, \cdots, N$) times, we do not have to decrypt the ciphertext in exactly the opposite order as when it is encrypted with a different key, as follows.

$$\begin{aligned} &E_{\omega_1}[E_{\omega_2}[\cdots E_{\omega_{N-2}}[E_{\omega_{N-1}}[E_{\omega_N}[M]]]\cdots]] \\ &= E_{\omega_1}[E_{\omega_2}[\cdots E_{\omega_{N-2}}[E_{\omega_{N-1}}[G(\omega_N)|\varphi\rangle]]\ldots]] \\ &= E_{\omega_1}[E_{\omega_2}[\cdots E_{\omega_{N-2}}[G(\omega_{N-1})G(\omega_N)|\varphi\rangle]\ldots]] \\ &= E_{\omega_1}[E_{\omega_2}[\cdots E_{\omega_{N-2}}[G(\omega_{N-1}+\omega_N)|\varphi\rangle]\ldots]] \\ &= G(\sum_{j=1}^{N}\omega_j)|\varphi\rangle \end{aligned}. \tag{4}$$

Obviously, the encrypted data are independent of the order of encryption. The commutation relationship for decryption is also unimportant. In short, even if we first encrypt a message with ω_1 and then encrypt it with ω_2, when decrypting it, we can first decrypt the ciphertext with ω_1 and then decrypt it with ω_2, as shown in Equation (5).

$$D_{\omega_1}[D_{\omega_2}[E_{\omega_2}[E_{\omega_1}[M]]]] = D_{\omega_1}[D_{\omega_2}[E_{\omega_1}[E_{\omega_2}[M]]]] = M. \tag{5}$$

It should be noted that for Equation (4), we need to calculate the final resulting quantum state based on the parity of N , which has the following form.

$$|\Phi\rangle = \prod_{j=1}^{N} G(\omega_j)|\varphi\rangle = \begin{cases} \begin{pmatrix} \sin\frac{\sum_{j=1}^{N}\omega_j}{2} & i\cos\frac{\sum_{j=1}^{N}\omega_j}{2} \\ i\cos\frac{\sum_{j=1}^{N}\omega_j}{2} & \sin\frac{\sum_{j=1}^{N}\omega_j}{2} \end{pmatrix}|\varphi\rangle & N \text{ is odd} \\ \begin{pmatrix} -\cos\frac{\sum_{j=1}^{N}\omega_j}{2} & i\sin\frac{\sum_{j=1}^{N}\omega_j}{2} \\ i\sin\frac{\sum_{j=1}^{N}\omega_j}{2} & -\cos\frac{\sum_{j=1}^{N}\omega_j}{2} \end{pmatrix}|\varphi\rangle & N \text{ is even} \end{cases}. \tag{6}$$

Furthermore, there is a commutative relationship between the rotation operation $G(\omega)$ and the Pauli operator X:

$$XG(\omega) = G(\omega)X. \tag{7}$$

where $X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. It is worth noting that, when the values of ω are, respectively, 0, π, $\frac{\pi}{2}$, $\frac{3\pi}{2}$, there exist four special rotation operations, which are

$$\begin{aligned} G_{00} &= G(0) = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix} = iX, \\ G_{01} &= G(\frac{\pi}{2}) = \begin{pmatrix} \frac{\sqrt{2}}{2} & \frac{\sqrt{2}}{2}i \\ -\frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2} \end{pmatrix} = \frac{\sqrt{2}}{2}(iX + I), \\ G_{10} &= G(\pi) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I, \\ G_{11} &= G(\frac{3\pi}{2}) = \begin{pmatrix} \frac{\sqrt{2}}{2} & -\frac{\sqrt{2}}{2}i \\ -\frac{\sqrt{2}}{2}i & \frac{\sqrt{2}}{2} \end{pmatrix} = \frac{\sqrt{2}}{2}(-iX + I). \end{aligned} \tag{8}$$

There exists an interesting property of these four rotation operations. That is, when $d \neq d'$, any two operations G_{cd} and $G_{c'd'}$ are not fully distinguishable [50], where, $c, d, c', d' \in \{0, 1\}$. For example, two operations G_{00} and G_{10} are required to be discriminated. We can assume that $|\psi\rangle$ is a given input state. According to the Refs. [51,52], it can be known that the minimum error probability of distinguishing G_{00} and G_{01} is

$$P_e^{\{G_{00},G_{01}\}} = \frac{1}{2}(1 - \sqrt{1 - |\langle\psi|G_{01}^{+}G_{00}|\psi\rangle|^2}). \tag{9}$$

Here, we minimize the overlap of $|\langle\psi|G_{01}^{+}G_{00}|\psi\rangle|$ by choosing an appropriate $|\psi\rangle$. $|\psi\rangle$ can be represented by using the eigenvector $|j\rangle$ of $G_{01}^{+}G_{00}$ as the basis [50], that is, $|\psi\rangle = \sum_j \psi_j|j\rangle$. Then, we define

$$z_\psi = \langle\psi|G_{01}^{+}G_{00}|\psi\rangle = \sum_j |\psi_j|^2 e^{i\mu_j}, \tag{10}$$

where, $e^{i\mu_j}$ are the eigenvalues of $G_{01}^{+}G_{00}$. The normalization condition for $|\psi\rangle$ is $\sum_j |\psi_j|^2 = 1$, and thus the subset $M(G_{01}^{+}G_{00}) \subset \mathbb{C}$ ($\mathbb{C}$ is a plural) described by z_ψ under varying $|\psi\rangle$ is a convex polygon with points $e^{i\mu_j}$ as its vertices. The minimum overlap

$$r(G_{01}^{+}G_{00}) = \min_{||\psi||=1} |\langle\psi|G_{01}^{+}G_{00}|\psi\rangle| \tag{11}$$

is the distance of $M(G_{01}^{+}G_{00})$from $z = 0$, as shown in Figure 1. Figure 1 illustrates in a simple way the best that can be done in distinguishing between G_{00} and G_{01}: if M contains the origin, then the two operations can be completely distinguished, otherwise the point in M closest to the origin must be found, and the minimum error probability is related to

its distance from the origin. Once the best point in M is found, the best state $|\psi\rangle$ are those corresponding that point by Equation (10).

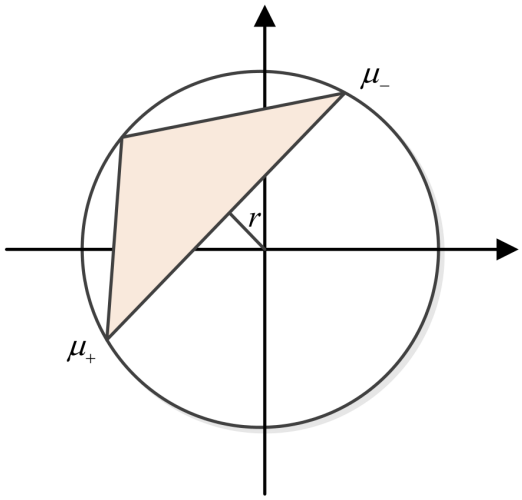

Figure 1. r is the minimum distance between the origin and the polygon M.

If $\phi(G_{01}^{+}G_{00})$ is the angular distribution of the eigenvalues of $G_{01}^{+}G_{00}$ (see Figure 1, it is $\phi = \mu_+ - \mu$), from Equation (9), for $\phi < \pi$, we have

$$P_e = \frac{1}{2}(1 - \sqrt{1 - \cos^4\frac{\phi}{2}}). \tag{12}$$

While for $\phi \geq \pi$, we have $P_e = 0$ and the discrimination is exact.

In order to acquire the minimum overlap $r(G_{01}^{+}G_{00})$, we first compute the eigenvalues of $G_{01}^{+}G_{00}$ and get

$$\begin{cases} b_1 = \frac{\sqrt{2}}{2}(1+i) = e^{\frac{i\pi}{4}} \\ b_2 = \frac{\sqrt{2}}{2}(1-i) = e^{\frac{-i\pi}{4}} \end{cases}. \tag{13}$$

Then, the following equation can be derived,

$$\begin{aligned} r(G_{01}^{+}G_{00}) &= \min|\sum_j |\psi_j|^2 e^{i\mu_j}| \\ &= \min||\psi_1|^2 e^{\frac{i\pi}{4}} + |\psi_2|^2 e^{\frac{-i\pi}{4}}| \\ &= \min|\frac{\sqrt{2}}{2}(1 + i(|\psi_1|^2 - |\psi_2|^2))| \\ &= \frac{\sqrt{2}}{2} \end{aligned}. \tag{14}$$

When $|\psi_1|^2 = |\psi_2|^2 = \frac{1}{2}$, Equation (14) holds. Consequently, the minimum error probability of distinguishing between G_{00} and G_{01} is $P_e^{\{G_{00},G_{01}\}} = \frac{1}{2} - \frac{\sqrt{2}}{4}$. In the same way, we can gain $P_e^{\{G_{00},G_{11}\}} = P_e^{\{G_{10},G_{01}\}} = P_e^{\{G_{10},G_{11}\}} = \frac{1}{2} - \frac{\sqrt{2}}{4}$. Therefore, each set of rotation operations $\{G_{00}, G_{01}\}$, $\{G_{00}, G_{11}\}$, $\{G_{10}, G_{01}\}$, $\{G_{10}, G_{11}\}$ cannot be completely distinguished from each other, and this property between them provides a safeguard against the leakage of secret information during the transmission of particles.

3. Quantum Secure Multi-Party Summation Protocol

In the protocol, there is a third party TP and N mutually distrustful participants P_j ($j = 1, 2, \cdots, N$). TP is semi-trusted [53], which means that they may misbehave alone, but will not collude with anyone. P_j is dishonest [53] who tries to steal secret information from other honest participants. Each participant P_j has a personal identification ID_j and a secret

integer $S_j = (s_j^1, s_j^2, \cdots, s_j^L)$ of length L. Here, ID_j is randomly generated and disclosed by each participant, and $s_j^l \in \{0,1\}$, $l = 1,2,\cdots,L$. In order to ensure the legitimacy of the participants identity, it is necessary for P_j to complete the authentication with the help of TP, who shares a private key $\bar{k}_j$ with P_j. Then, through performing the protocol, all participants are able to calculate the summation of their secret integers as shown Equation (15), without revealing their secret integers. The flowchart of the protocol is shown in Figure 2.

$$S = \oplus_{j=1}^{N} S_j = (\oplus_{j=1}^{N} s_j^1, \oplus_{j=1}^{N} s_j^2, \cdots, \oplus_{j=1}^{N} s_j^L). \tag{15}$$

In the proposed protocol, photons are used as quantum bits to transmit information, and there are some quantum channels and classical channels that are used to transmitted particles and classical messages among the participants. Here, all quantum channels are public, and classical channels are almost public. In other words, the classical messages transmitted in the classical channels cannot be tampered, but the attacker is allowed to eavesdrop on the messages and to send fake messages by impersonating other participants. The specific steps of the protocol are described as follows.

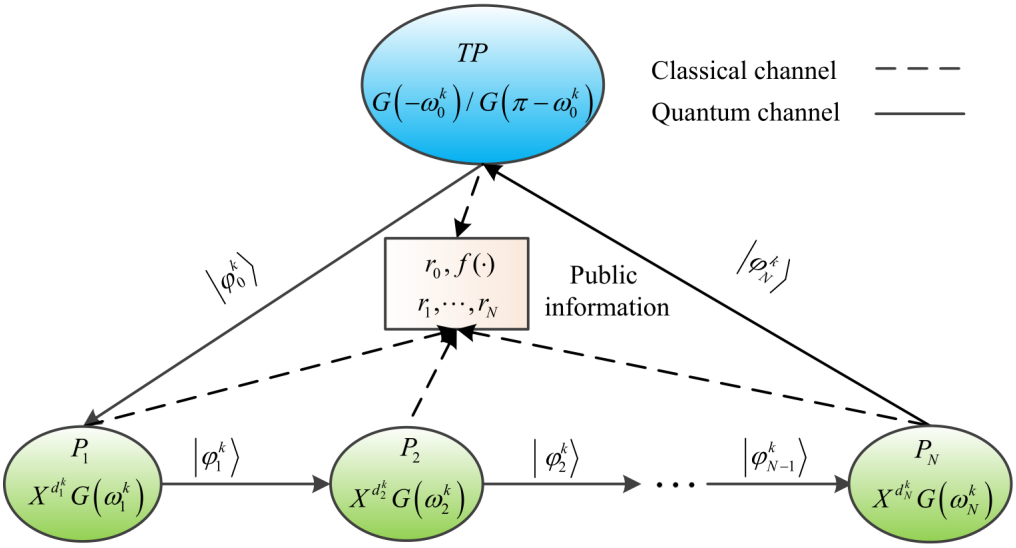

Figure 2. The process of quantum secure multi-party summation protocol. First, TP performs authentication operation on quantum state $|\varphi^k\rangle$ ($k = 1,2,\cdots,L+N\delta$) to get $|\varphi_0^k\rangle$. Second, N participants can alternately complete encoding operation and authentication operation on the encrypted sequence while obtaining the operated encrypted sequence. Third, the last participant sends the operated encrypted sequence to TP. Finally, after the N participants have completed identity authentication, TP can calculate the secret summation result of the N participants. Here, $X^{d_j^k}$ ($j = 1,2,\cdots,N$) is the encoding operation, $G(\omega_j^k)$ and $G(-\omega_0^k)$ ($G(\pi-\omega_0^k)$) are authentication operations.

Step 1: TP and P_j ($j = 1,2,\cdots,N$) generate a random bit string r_0 and r_j, respectively, while making these bit strings public. Then, TP selects a hash function $f: 2^* \to 2^{2(L+N\delta)}$ from hash clusters and declares it. f is a one-way hash function that works in one direction. It is easy to compute its hash value $f(x_1)$ from the pre-mapped value x_1, but it is hard to generate a pre-mapped value x_2 such that its hash value $f(x_2) = y$ (y is a fixed value). A good hash function is conflict-free, that is, it is hard to generate two different pre-mapped values x_1 and x_2 such that their hash values $f(x_1) = f(x_2)$. In general, in order to ensure that a hash function does not collide, it is required to output a minimum length of 80 bits [18]. Here, some common hash functions (e.g., SHA-1 or MD5) are used to generate the identity information of TP and each participant P_j. Subsequently, TP and P_j compute

their hash value $h_j = f_{\overline{k}_j}(ID_j \parallel r_j \parallel r_0)$. For binary bit string $h_{j,t}$ $(t = 1, 2, \cdots, 2(L + N\delta))$, which is encoded as follows.

$$\begin{aligned} &h_{j,2k-1}h_{j,2k} = 00 : \omega_j^k = 0, \quad h_{j,2k-1}h_{j,2k} = 01 : \omega_j^k = \frac{\pi}{2}, \\ &h_{j,2k-1}h_{j,2k} = 10 : \omega_j^k = \pi, \quad h_{j,2k-1}h_{j,2k} = 11 : \omega_j^k = \frac{3\pi}{2}, \end{aligned} \tag{16}$$

where, $k = 1, 2, \cdots, L + N\delta$.

Step 2: TP and P_j $(j = 1, 2, \cdots, N)$, respectively, produces a random number $D_0 = (d_0^1, d_0^2, \cdots, d_0^{L+N\delta})$ and $D_j = (d_j^1, d_j^2, \cdots, d_j^{L+N\delta})$ of length $L + N\delta$, with d_0^k, $d_j^k \in \{0, 1\}$, $k = 1, 2, \cdots, L + N\delta$. According to the bit string D_0, TP prepares a sequence of quantum states $Q = \{|\varphi^k\rangle,\ k = 1, 2, \cdots, L + N\delta\}$. Concretely, if $d_0^k = 0$, then $|\varphi^k\rangle = |0\rangle$; otherwise $|\varphi^k\rangle = |1\rangle$.

Step 3: TP calculates $h_0 = \boxplus_{j=1}^N h_j$, where $\boxplus$ denotes *mod* 4 operation. Then, TP performs authentication encoding operation on the k-th photon $|\varphi^k\rangle$ in the sequence Q based on $h_{0,2k-1}h_{0,2k}$. Specifically, if N is odd, TP executes operation $G(-\omega_0^k)$ on the photon $|\varphi^k\rangle$; if N is even, TP carries out operation $G(\pi - \omega_0^k)$ on $|\varphi^k\rangle$. The sequence of quantum states after authentication encoding operation is labelled Q_0. After that, TP sends it to P_1.

Step 4: Upon receiving the sequence Q_0, P_1 performs an encryption operation on the quantum state sequence based on D_1. Concretely, if $d_1^k = 0$, he implements I operation on the k-th photon, otherwise, he performs X operation on the k-th photon. Then, in accordance with $h_{1,2k-1}h_{1,2k}$, P_1 executes identity authentication operation $G(\omega_1^k)$ on the k-th quantum state in the sequence Q_0. The encrypted new quantum state sequence is marked as Q_1, which is sent to P_2 by P_1.

Step 5: After receiving the sequence Q_{j-1} from P_{j-1}, P_j $(j = 2, 3, \cdots, N)$ repeats the same procedure as P_1 does in step 4. That is, he encrypts the random number D_j into the sequence Q_{j-1}, and then performs the identity encoding operation $G(\omega_j^k)$ on the k-th photon in Q_{j-1} according to $h_{j,2k-1}h_{j,2k}$, obtaining a new sequence Q_j. Afterward, P_j sends the sequence Q_j to P_{j+1}. If $j = N$, the last participant, P_N, sends the sequence Q_N to TP.

Step 6: Once receiving the photon sequence Q_N, TP measures it using a set of base $\{|0\rangle, |1\rangle\}$ and gains the measurement $M = (m^1, m^2, \cdots, m^{L+N\delta})$. By computing

$$u^k = m^k \oplus d_0^k,\ k = 1, 2, \cdots, L + N\delta, \tag{17}$$

TP obtains the calculation results $U = (u^1, u^2, \cdots, u^{L+N\delta})$.

Step 7: P_j $(j = 1, 2, \cdots, N)$ authenticates the identification of the other $N - 1$ participants P_i $(i = 1, 2, \cdots, N, i \neq j)$, detects whether there is impersonal behaviour during the execution of the protocol. Specifically, P_j randomly selects δ photons from $L + N\delta$ photons as detection photons and announces their positions. Then, he asks TP to publish u^k corresponding to the positions of the δ detection photons in U, while asking the $N - 1$ participants P_i to announce d_i^k corresponding to the positions of the δ detected photons in D_i. The order of publication of the $N - 1$ participants is decided by P_j at random. P_j determines whether the equation $d_j^k = u^k \oplus \oplus_{i=1, i\neq j}^N d_i^k$ holds, and calculates the error rate. If the error rate is lower than the pre-set threshold, P_j considers that participants executing the protocol with them are indeed the $N - 1$ participants P_i; otherwise, he considers that there is impersonal behaviour among the $N - 1$ participants, and terminates the protocol.

Step 8: P_j $(j = 1, 2, \cdots, N)$ removes d_j^k corresponding to the $N\delta$ detected photons in D_j. The bits at the remaining positions are noted as $\overline{D_j} = (d_j^1, d_j^2, \cdots, d_j^L)$. Subsequently, P_j calculates and publishes $V_j = (v_j^1, v_j^2, \cdots, v_j^L)$, with $v_j^l = s_j^l \oplus d_j^l$, $l = 1, 2, \cdots, L$.

Step 9: TP discards the declared u_k and records the remaining calculation as $\overline{U} = (u^1, u^2, \cdots, u^L)$. Then, he calculates the summation

$$s^l = u^l \oplus \oplus_{j=1}^N v_j^l. \tag{18}$$

Finally, TP announces the summation result $S = (s^1, s^2, \cdots, s^L)$.

Through the above steps 1 to 9, all participants can obtain the sum of their secret integer. In order to better understand the process of the proposed protocol, we design its quantum circuit, as shown in Figure 3. Simultaneously, an example containing three participants (i.e., $N = 3$) is given. For the sake of convenience, the detection particles in the protocol are ignored. In this example, there are three participants P_1, P_2 and P_3, who, respectively, have secret integer $S_1 = 1110$, $S_2 = 0011$, $S_3 = 1100$ of length 4 (i.e., $L = 4$) and identification $ID_1 = 01101011$, $ID_2 = 10101101$, $ID_3 = 11010010$ with length 8. Through conducting the above protocol, they evaluate the sum $S = S_1 \oplus S_2 \oplus S_3$ of the secret integers. The relevant information involved in the example of the three participants is shown in Table 1.

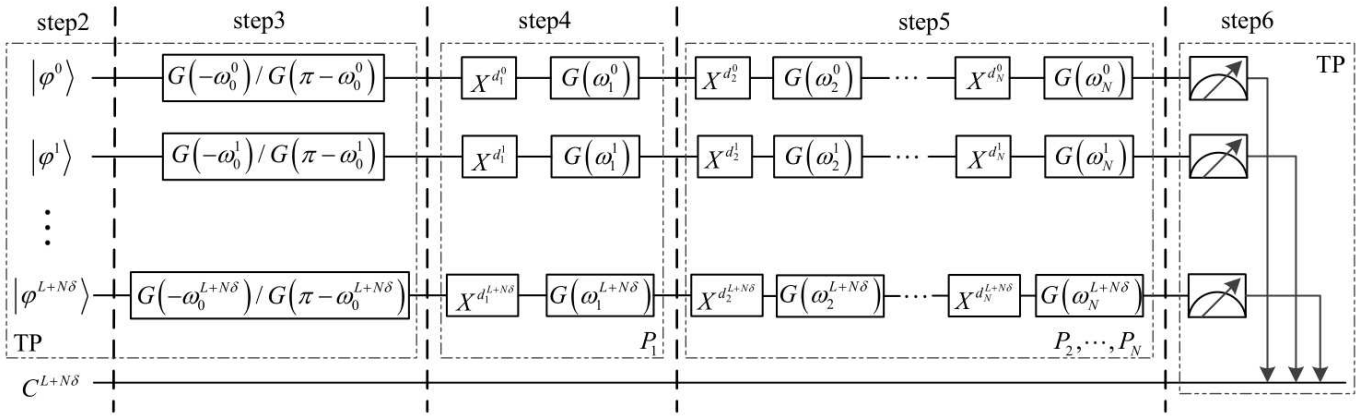

Figure 3. The quantum circuit of the proposed protocol. First, TP performs authentication operations on the quantum sequence $Q = \{|\varphi^0\rangle, |\varphi^1\rangle, \cdots, |\varphi^{L+N\delta}\rangle\}$. Then, each participant encodes D_j into the quantum sequence by performing the encoding operation, and applies the authentication operation to encrypt the sequence which is subsequently sent to the next participant. Finally, TP measures each qubit in the computational basis.

Table 1. The relevant information involved in the examples of the three participants (- indicates no.).

	TP	P_1	P_2	P_3
ID_j	-	01101011	10101101	11010010
r_j	0101	1100	1111	0010
h_j	01000110	10010010	11011110	00101010
D_j	0110	0010	1001	1110
V_j	-	1100	1010	0010
S_j	-	1110	0011	1100

In the protocol, TP prepares a quantum sequence $Q = |0\rangle|1\rangle|1\rangle|0\rangle$ based on D_0. In step 3, TP calculates $h_0 = 01000110$. Then, according to it, he executes the authentication operation $G(-\frac{\pi}{2}) \otimes G(0) \otimes G(-\frac{\pi}{2}) \otimes G(-\pi)$ on the sequence Q to yield the sequence Q_0. After that, TP sends Q_0 to P_1. In step 4, when P_1 receives the sequence Q_0 from TP, he performs the corresponding encoding operations based on D_1 and h_1. Similarly, P_2 and P_3 perform the corresponding encrypted operations. The encoding operations on the quantum sequence and the change of the quantum states are shown in Table 2.

At the end of the protocol, TP obtains the particle sequence $Q_3 = |0\rangle|0\rangle|1\rangle|1\rangle$. TP then measures it with the base $\{|0\rangle, |1\rangle\}$ and gets the measurement result $M = 0011$. According to Equations (17) and (18), TP calculates $S = M \oplus D_0 \oplus_{i=1}^{3} V_i = 0001$. Apparently, $S = S_1 \oplus S_2 \oplus S_3$. Therefore, P_1, P_2 and P_3 gain the sum of their secret integers.

Table 2. Encoding operations on the quantum sequence.

Q_0	Q_1	Q_2	Q_3
$\|0\rangle \xrightarrow{01:G(-\frac{\pi}{2})} \frac{\sqrt{2}}{2}(i\|1\rangle - \|0\rangle)$	$\xrightarrow{X^0G_{10}} \frac{\sqrt{2}}{2}(i\|1\rangle - \|0\rangle)$	$\xrightarrow{X^1G_{11}} i\|0\rangle$	$\xrightarrow{X^1G_{00}} -\|0\rangle$
$\|1\rangle \xrightarrow{00:G(0)} i\|0\rangle$	$\xrightarrow{X^0G_{01}} \frac{\sqrt{2}}{2}(i\|0\rangle - \|1\rangle)$	$\xrightarrow{X^0G_{01}} -\|1\rangle$	$\xrightarrow{X^1G_{10}} -\|0\rangle$
$\|1\rangle \xrightarrow{01:G(-\frac{\pi}{2})} \frac{\sqrt{2}}{2}(i\|0\rangle - \|1\rangle)$	$\xrightarrow{X^1G_{00}} -\frac{\sqrt{2}}{2}(i\|1\rangle + \|0\rangle)$	$\xrightarrow{X^0G_{11}} -\|0\rangle$	$\xrightarrow{X^1G_{10}} -\|1\rangle$
$\|0\rangle \xrightarrow{10:G(-\pi)} -\|0\rangle$	$\xrightarrow{X^0G_{10}} -\|0\rangle$	$\xrightarrow{X^1G_{10}} -\|1\rangle$	$\xrightarrow{X^0G_{10}} -\|1\rangle$

4. Protocol Analysis

In this section, the correctness and security of the proposed protocol are firstly analyzed. Then, we compare the proposed protocol with the previous protocols.

4.1. Correctness

For a QSMS protocol, its correctness implies that all participants honestly execute the protocol and obtain the sum of their secret integer without revealing any secrets. Suppose the initial signal photon prepared by TP is $|\varphi^l\rangle$, $l = 1, 2, \cdots, L$. In step 3, TP computes $h_0 = \boxplus_{j=1}^{N} h_j$, and performs the identity encoding operation on the signal photon $|\varphi^l\rangle$ based on $h_{0,2l-1}h_{0,2l}$ to obtain $|\varphi_0^l\rangle$. In steps 4 and 5, when the N participants have completed encryption operation $X^{d_j^l}$ and the identity authentication operation $G(\omega_j^l)$ on $|\varphi_0^l\rangle$ in turn according to d_j^l and $h_{j,2l-1}h_{j,2l}$, the final signal photon is in state $|\varphi_N^l\rangle$. Since TP needs to perform different identity authentication operations on the signal photon $|\varphi^l\rangle$ depending on the parity of N, we discuss the final quantum state in the following two cases.

(1) When N is an odd number, the identity authentication operation performed by TP on the signal photon $|\varphi^l\rangle$ is $G(-\omega_0^l)$. Depending on Equation (6), it is known that the final quantum state evolves as

$$\begin{aligned} |\varphi_N^l\rangle &= \prod_{j=1}^{N}[G(\omega_j^l)X^{d_j^l}]G(-\omega_0^l)|\varphi^l\rangle \\ &= \prod_{j=1}^{N} G(\omega_j^l)G(-\omega_0^l)|\varphi^l \oplus \oplus_{j=1}^{N} d_j^l\rangle \\ &= \begin{pmatrix} -\cos\frac{\sum_{j=1}^{N}\omega_j^l-\omega_0^l}{2} & i\sin\frac{\sum_{j=1}^{N}\omega_j^l-\omega_0^l}{2} \\ i\sin\frac{\sum_{j=1}^{N}\omega_j^l-\omega_0^l}{2} & -\cos\frac{\sum_{j=1}^{N}\omega_j^l-\omega_0^l}{2} \end{pmatrix}|\varphi^l \oplus \oplus_{j=1}^{N} d_j^l\rangle \\ &= -|\varphi^l \oplus \oplus_{j=1}^{N} d_j^l\rangle \end{aligned} . \tag{19}$$

(2) When N is an even number, The identity authentication operation executed by TP on the signal photon $|\varphi^l\rangle$ is $G(\pi - \omega_0^l)$. Similarly, according to Equation (6), we can get the final quantum state as shown below.

$$\begin{aligned} |\varphi_N^l\rangle &= \prod_{j=1}^{N}[G(\omega_j^l)X^{d_j^l}]G(\pi-\omega_0^l)|\varphi^l\rangle \\ &= \prod_{j=1}^{N} G(\omega_j^l)G(\pi-\omega_0^l)|\varphi^l \oplus \oplus_{j=1}^{N} d_j^l\rangle \\ &= \begin{pmatrix} \sin\frac{\sum_{j=1}^{N}\omega_j^l-\omega_0^l+\pi}{2} & i\cos\frac{\sum_{j=1}^{N}\omega_j^l-\omega_0^l+\pi}{2} \\ i\cos\frac{\sum_{j=1}^{N}\omega_j^l-\omega_0^l+\pi}{2} & \sin\frac{\sum_{j=1}^{N}\omega_j^l-\omega_0^l+\pi}{2} \end{pmatrix}|\varphi^l \oplus \oplus_{j=1}^{N} d_j^l\rangle \\ &= |\varphi^l \oplus \oplus_{j=1}^{N} d_j^l\rangle \end{aligned} . \tag{20}$$

It can be seen from the above analysis that without considering the global phase, no matter whether N is odd or even, TP can eventually gain the quantum state $|\varphi_N^l\rangle = |\varphi^l \oplus \oplus_{j=1}^N d_j^l\rangle$. Then, he measures it with the base $\{|0\rangle, |1\rangle\}$ and gets the measurement result $m^l = d_0^l \oplus \oplus_{j=1}^N d_j^l$. On the basis of Equations (17) and (18) and v_j^l $(j = 1, 2, \cdots, N)$ published by all participants, we can gain the summation result $s^l = m^l \oplus d_0^l \oplus \oplus_{j=1}^N v_j^l$, $l = 1, 2, \cdots, L$. In summary, the proposed protocol is correct.

4.2. Security

In this section, we first prove that the encoded quantum states in our protocol cannot be unambiguous discriminated (i.e., Theorem 1). Then, on that basis, the proposed protocol is shown to be secure under common external and internal attacks. Furthermore, it is demonstrated that our proposed protocol is resistant to Trojan horse attacks and impersonation attacks.

Theorem 1. *In this protocol, when four different authentication operations $G(0)$, $G(\frac{\pi}{2})$, $G(\pi)$, $G(\frac{3\pi}{2})$ are, respectively, applied to a certain quantum state of the transmission, the resulting quantum states cannot be unambiguous discriminated. That is, there is a linear correlation between the encrypted quantum states.*

Proof of Theorem 1. Since the initial quantum states change continuously and are in one of the four quantum states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ during the execution of the protocol, where $|\pm\rangle = \frac{\sqrt{2}}{2}(|0\rangle \pm i|1\rangle)$. Without loss of generality, we assume that the k-th $(k = 1, 2, \cdots, L + N\delta)$ particle in the hands of P_j $(j = 1, 2, \cdots, N)$ is in state

$$|\varphi_j^k\rangle = \alpha|0\rangle + \beta|1\rangle. \tag{21}$$

Then, P_j encodes the random number d_j^k into the photon $|\varphi_j^k\rangle$. After that, he executes the identity authentication operation $G(\omega_j^k)$ on the photon depending on $h_{j,2k-1}h_{j,2k}$, and gets a new quantum state $|\varphi_j^k\rangle_{h_{j,2k-1}h_{j,2k}}$. Based on Equation (16), the new quantum state $|\varphi_j^k\rangle_{h_{j,2k-1}h_{j,2k}}$ is in one of the following four quantum states.

$$\begin{aligned}
|\varphi_j^k\rangle_{00} &= G(0)X^{d_j^k}|\varphi_j^k\rangle = i(\alpha|1 \oplus d_j^k\rangle + \beta|d_j^k\rangle),\\
|\varphi_j^k\rangle_{01} &= G(\frac{\pi}{2})X^{d_j^k}|\varphi_j^k\rangle\\
&= \frac{\sqrt{2}}{2}[i(\alpha|1 \oplus d_j^k\rangle + \beta|d_j^k\rangle) + (\alpha|d_j^k\rangle + \beta|1 \oplus d_j^k\rangle)],\\
|\varphi_j^k\rangle_{10} &= G(\pi)X^{d_j^k}|\varphi_j^k\rangle = \alpha|d_j^k\rangle + \beta|1 \oplus d_j^k\rangle),\\
|\varphi_j^k\rangle_{11} &= G(\frac{3\pi}{2})X^{d_j^k}|\varphi_j^k\rangle\\
&= \frac{\sqrt{2}}{2}[-i(\alpha|1 \oplus d_j^k\rangle + \beta|d_j^k\rangle) + (\alpha|d_j^k\rangle + \beta|1 \oplus d_j^l\rangle)].
\end{aligned} \tag{22}$$

By simple calculation, we gather that there are linear correlations between the above four encrypted quantum states:

$$\begin{aligned}
|\varphi_j^k\rangle_{01} &= \frac{\sqrt{2}}{2}(|\varphi_j^k\rangle_{10} + |\varphi_j^k\rangle_{00}),\\
|\varphi_j^k\rangle_{01} &= \frac{\sqrt{2}}{2}(|\varphi_j^k\rangle_{10} - |\varphi_j^k\rangle_{00}).
\end{aligned} \tag{23}$$

As Chefles et al. [54] said, the necessary and sufficient condition for distinguishing the quantum states is that they are linearly independent. Therefore, these linearly correlated quantum states cannot be unambiguous discriminated. □

4.2.1. External Attack

Suppose Eve is an external attacker, and she wants to eavesdrop on the secret integer S_j and the private key $\overline{k}_j$ without being detected. In the proposed protocol, the private key $\overline{k}_j$ is shared between TP and P_j, and it is used to compute the hash value h_j. Then, P_j performs the identity encoding on the sequence Q_{j-1} based on h_j. In the presented protocol, the hash function $f(.)$, the identification ID_j, the random bit strings r_j and r_0 are publicly. Since P_j does not disclose their hash value h_j, Eve cannot infer any information about $\overline{k}_j$ from these publicly available information. The secret integer $S_j = \overline{D_j} \oplus V_j$, V_j is exposed by P_j in step 8, so Eve can only obtain information about $\overline{D_j}$ that he first needs to obtain in order to obtain S_j. Since $\overline{D_j}$ is encoded in the traveling photon, Eve has to attack the travelling photon sequence to obtain $\overline{k}_j$ and $\overline{D_j}$ of P_j. Next, we consider some common external attacks as well as Trojan Horse attacks.

(1) Intercept resend attack

In this attack, suppose that Eve intercepts a sequence F of photons sent by P_{j-1} and resends a sequence $\widetilde{\mathrm{F}}$ of pseudo photons to P_j. Since the detection photons are included in the sequence of travelling photons, these detection photons are randomly in one of the four states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ after the encoding operation. Eve does not know the position and state of these detection photons, thus her attack would inevitably introduce some errors and will be detected with a probability of $1 - (\frac{3}{4})^{\delta}$ in step 7. When δ is large enough, the probability converges to 1. Despite this, Eve still hopes to infer the secret key $\overline{k}_j$ and $\overline{D_j}$ of P_j. However, this is unsuccessful. In the following, we analyse the case where Eve has access to $\overline{k}_j$ and $\overline{D_j}$ while avoiding detection.

Since $\overline{D_j}$ is encoded in the signal photons of the sequence Q_{j-1}, Eve can only obtain information about $\overline{D_j}$ by attacking the signal photons of P_{j-1}. Suppose that the k-th photon $|\varphi_j^k\rangle$ intercepted by Eve is the signal photon of P_{j-1}, and resent a fake quantum state $|\widetilde{\varphi}\rangle = \alpha|0\rangle + \beta|1\rangle$ to P_j. According to the random number d_j^k and the hash value $h_{j,2k-1}h_{j,2k}$, P_j executes the encryption operation $X^{d_j^k}$ and the identity authentication operation $G(\omega_j^k)$ on the fake quantum state $|\widetilde{\varphi}\rangle$ in turn. He gets a new quantum state $|\widetilde{\varphi}\rangle_{h_{j,2k-1}h_{j,2k}}$, as shown in Table 3. Afterwards, Eve intercepts $|\widetilde{\varphi}\rangle_{h_{j,2k-1}h_{j,2k}}$ and measures it to distinguish which operation is performed by P_j. The process of Eve performing intercept resend attack is shown in Figure 4.

In order to distinguish the operation of P_j, Eve first requires to distinguish the above four encrypted quantum states. From Theorem 1, the above four quantum states cannot be unambiguous discriminated. That is, Eve cannot distinguish between the encoded operation and the identity authentication operation performed by P_j. Therefore, she cannot infer h_j and d_j^k, nor can she infer $\overline{k}_j$ from the public information. In a word, the proposed protocol can resist intercept resend attack.

Table 3. Quantum states after different encoding operations on pseudo quantum state.

Secret Data	$h_{j,2k-1}h_{j,2k}$	Encoded Quantum State
d_j^k	00	$\widetilde{\varphi}_{00} = i(\alpha\|1 \oplus d_j^k\rangle + \beta\|d_j^k\rangle)$
	01	$\widetilde{\varphi}_{01} = \frac{\sqrt{2}}{2}[i(\alpha\|1 \oplus d_j^k\rangle + \beta\|d_j^k\rangle) + (\alpha\|d_j^k\rangle + \beta\|1 \oplus d_j^k\rangle)]$
	10	$\widetilde{\varphi}_{10} = \alpha\|d_j^k\rangle + \beta\|1 \oplus d_j^k\rangle)$
	11	$\widetilde{\varphi}_{11} = \frac{\sqrt{2}}{2}[-i(\alpha\|1 \oplus d_j^k\rangle + \beta\|d_j^k\rangle) + (\alpha\|d_j^k\rangle + \beta\|1 \oplus d_j^k\rangle)]$

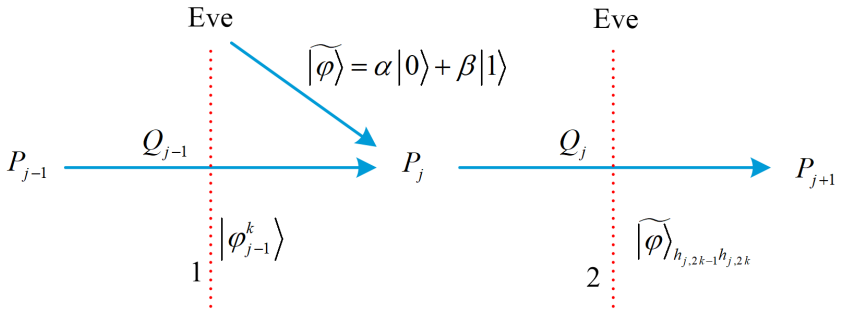

Figure 4. The running process of Eve performing intercept resend attack. The red dashed lines 1 and 2 indicates that Eve intercepts photons $|\varphi_j^k\rangle$ and $|\widetilde{\varphi}\rangle_{h_{j,2k-1}h_{j,2k}}$, respectively, the blue solid line indicates transmitting photons.

(2) Entangle measure attack

In this attack, assume that Eve intercepts a signal photon $|\varphi_j^k\rangle$ sent by P_j and prepares an additional photon $|E\rangle$. She then performs an entanglement operation U_E on the signal photon $|\varphi_j^k\rangle$ and the additional photon $|E\rangle$, and sends the intercepted signal photon to P_{j+1}. Subsequently, P_{j+1} encodes their secret data d_{j+1}^k into the signal photon, and performs an identity authentication operation $G(\omega_{j+1}^k)$ on it based on $h_{j+1,2k-1}h_{j+1,2k}$. Finally, Eve deduces the private key $\bar{k}_{j+1}$ and the secret message d_{j+1}^k by measuring the additional photon. The process of entangle measure attack performed by Eve is shown in Figure 5. However, this attack is not possible, the detailed analysis is as follows.

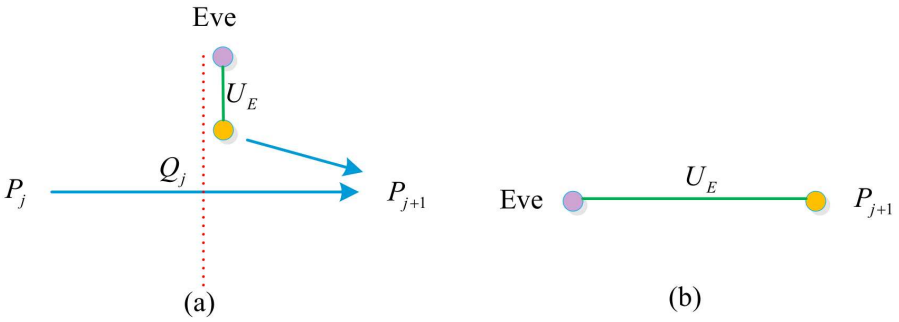

Figure 5. The running process of Eve performing entangle measure attack. (**a**) Eve entangles an additional photon. (**b**) Eve and P_{j+1} share an entangled state. The red dashed line indicates that Eve intercepts a photon $|\varphi_j^k\rangle$, which is indicated by an orange dot. The purple dot indicates Eve's additional particle $|E\rangle$. The blue solid line indicates the transmitting particle.

The effect of Eve's unitary operation U_E on the signal photons and additional photons as shown below.

$$\begin{aligned} U_E|0\rangle|E\rangle &= a_1|0\rangle|e_{00}\rangle + a_2|1\rangle|e_{01}\rangle, \\ U_E|1\rangle|E\rangle &= a_3|0\rangle|e_{10}\rangle + a_4|1\rangle|e_{11}\rangle. \end{aligned} \tag{24}$$

Here, $|e_{00}\rangle$, $|e_{01}\rangle$, $|e_{10}\rangle$, $|e_{11}\rangle$ are the four states uniquely determined by unitary operation U_E, and the four coefficients a_1, a_2, a_3, a_4 satisfy $|a_1|^2 + |a_2|^2 = |a_3|^2 + |a_4|^2 = 1$. If Eve does not introduce errors, then U_E needs to satisfy the following conditions.

$$\begin{aligned} U_E|0\rangle|E\rangle &= a_1|0\rangle|e_{00}\rangle, \\ U_E|1\rangle|E\rangle &= a_4|1\rangle|e_{11}\rangle. \end{aligned} \tag{25}$$

From the Equations (24) and (25), we can obtain that $a_1 = a_4 = 1$, $a_2 = a_3 = 0$.

Without loss of generality, suppose the signal photon is $|\varphi_j^k\rangle$ shown in Equation (21). After U_E acts on the signal photon $|\varphi_j^k\rangle$ and the additional photon $|E\rangle$, the resulting state of the whole system is

$$|\Psi\rangle = U_E|\varphi_j^k\rangle|E\rangle = \alpha|0\rangle|e_{00}\rangle + \beta|1\rangle|e_{11}\rangle. \tag{26}$$

In step 5, when P_{j+1} has completed the encryption operation $X^{d_{j+1}^k}$ and the identity authentication operation $G(\omega_{j+1}^k)$ on the signal photon based on d_{j+1}^k and $h_{j+1,2k-1}h_{j+1,2k}$, the whole quantum system is in one of the four states:

$$|\Psi\rangle_{h_{j+1,2k-1}h_{j+1,2k}} = G(\omega_{j+1}^k)X^{d_{j+1}^k} \otimes I|\Psi\rangle. \tag{27}$$

After a simple calculation, we can rewrite four states of Equation (27) as

$$\begin{aligned}
|\Psi\rangle_{00} &= i(\alpha|d_{j+1}^k \oplus 1\rangle|e_{00}\rangle + \beta|d_{j+1}^k\rangle|e_{11}\rangle),\\
|\Psi\rangle_{01} &= \frac{\sqrt{2}}{2}[(\alpha|d_{j+1}^k\rangle|e_{00}\rangle + \beta|d_{j+1}^k \oplus 1\rangle|e_{11}\rangle)\\
&\quad + i(\alpha|d_{j+1}^k \oplus 1\rangle|e_{00}\rangle + \beta|d_{j+1}^k\rangle|e_{11}\rangle)],\\
|\Psi\rangle_{10} &= \alpha|d_{j+1}^k\rangle|e_{00}\rangle + \beta|d_{j+1}^k \oplus 1\rangle|e_{11}\rangle,\\
|\Psi\rangle_{11} &= \frac{\sqrt{2}}{2}[(\alpha|d_{j+1}^k\rangle|e_{00}\rangle + \beta|d_{j+1}^k \oplus 1\rangle|e_{11}\rangle)\\
&\quad - i(\alpha|d_{j+1}^k \oplus 1\rangle|e_{00}\rangle + \beta|d_{j+1}^k\rangle|e_{11}\rangle)].
\end{aligned} \tag{28}$$

We find that there are linear correlations between the four quantum states:

$$\begin{aligned}
|\Psi\rangle_{10} &= \frac{\sqrt{2}}{2}(|\Psi\rangle_{11} + |\Psi\rangle_{00}),\\
|\Psi\rangle_{10} &= \frac{\sqrt{2}}{2}(|\Psi\rangle_{11} - |\Psi\rangle_{00}).
\end{aligned} \tag{29}$$

According to Theorem 1, these encrypted quantum states cannot be unambiguously distinguished. Therefore, Eve cannot obtain any information about the secret information d_{j+1}^k and the private key $\bar{k}_{j+1}$ through the entanglement measurement attack. In summary, the entangle measure attack is invalid for our protocol.

(3) Trojan Horse attacks

Since the proposed protocol transports photons over more than once, it may be insecure against two types of Trojan horse attacks, namely, delayed photon attacks [55] and invisible photon attacks [56]. To prevent these two types of attacks, the participants can install some special quantum optical devices such as wavelength quantum filters and photon number splitters during the execution of the protocol. For invisible photons that appear during transmission, they can be filtered out using a wavelength quantum filter. Meanwhile, for the delayed photons that appear in it, the photon number splitters can be used to split each legitimate photon to discover it. In short, with the addition of the two devices, both the invisible photon attack and the delayed photon attack appearing in the presented protocol will fail.

4.2.2. Internal Attack

Compared to external attackers, internal participants are more destructive because they have greater privileges than external attackers to gain access to the secret information of other participants. In addition to analysing some common internal attacks, we also analyse impersonation attacks.

(1) A dishonest participant's attack

Since all participants play the same role in our protocol, we can assume that P_1 is dishonest, noted as P_1^*. He tries to steal secret input from P_j and sends a pseudophoton sequence F to P_j. Then, P_j performs the encoding and identity authentication operation on the sequence F and gets the photon sequence $\widetilde{F}$, then he sends it to P_{j+1}. At this point, P_1^* attacks the photon sequence $\widetilde{F}$ to distinguish the operations. Since P_1 does not know the positions and states of the decoy photons in the sequence Q_{j-1}, their attack will be detected in step 7 just like the external attacker, Eve. Therefore, such an attack would be ineffective against our protocol.

(2) Dishonest participants' collusion attack

In this attack, there may be two or more dishonest participants who want to collectively steal the secret input of other honest participants. Without loss of generality, suppose P_{j-1} and P_{j+1} are dishonest participants, who are denoted as P_{j-1}^* and P_{j+1}^*. Obviously, it is easier for them to conspire to steal the secret integer of P_j than that of other participants. In collusion attack, both P_{j-1}^* and P_{j+1}^* need to intercept the photons in the transmission sequence and retransmit a fake sequence to P_j and P_{j+2}, respectively. Since P_{j-1}^* and P_{j+1}^* do not know the positions and states of the decoy photons, their attack will be detected in the eavesdropping detection. Nevertheless, P_{j-1}^* and P_{j+1}^* still want to obtain the secret data of the other honest participants. However, they are unlikely to succeed. The situation where P_{j-1}^* and P_{j+1}^* conspire to attack P_j is discussed as follows.

Here, we consider a more general attack strategy. Suppose the k-th photon in the sequence Q_{j-1} intercepted by is a signal photon, he keeps it in their hands. Then, he sends a pseudophoton $|\widehat{\varphi}\rangle = \alpha|0\rangle + \beta|1\rangle$ to P_j. P_j encodes the secret data d_j^k into $|\widehat{\varphi}\rangle$, and performs the authentication operation $G(\omega_j^k)$ on it according to $h_{j,2k-1}h_{j,2k}$. Subsequently, he sends the resulting new quantum state $|\widehat{\varphi}\rangle_{h_{j,2k-1}h_{j,2k}}$ (as shown in Table 4) to P_{j+1}^*. Since P_{j-1}^* and P_{j+1}^* do not know $h_{j,2k-1}h_{j,2k}$, they cannot determine which identity authentication operation P_j executes. Therefore, P_{j+1}^* can only distinguish which operation P_j performs by measuring $|\widehat{\varphi}\rangle_{h_{j,2k-1}h_{j,2k}}$. Because there is a linear relationship similar to Equation (20) for the four quantum states in Table 4, so that P_{j+1}^* cannot distinguish between these four quantum states. Therefore, even if P_{j-1}^* and P_{j+1}^* collude to attack P_j, they cannot infer any information about P_j's secret information d_j^k and private key $\overline{k}_j$. To sum up, our protocol is immune to this attack.

Table 4. Quantum states after different encoding operations on pseudo photons.

Secret Data	$h_{j,2k-1}h_{j,2k}$	Encoded Quantum State
d_j^k	00	$\widehat{\varphi\rangle}_{00} = i(\alpha\|1 \oplus d_j^k\rangle + \beta\|d_j^k\rangle)$
	01	$\widehat{\varphi\rangle}_{01} = \frac{\sqrt{2}}{2}[i(\alpha\|1 \oplus d_j^K\rangle + \beta\|d_j^k\rangle) + (\alpha\|d_j^k\rangle + \beta\|1 \oplus d_j^k\rangle)]$
	10	$\widehat{\varphi\rangle}_{10} = \alpha\|d_j^k\rangle + \beta\|1 \oplus d_j^k\rangle)$
	11	$\widehat{\varphi\rangle}_{11} = \frac{\sqrt{2}}{2}[-i(\alpha\|1 \oplus d_j^k\rangle + \beta\|d_j^k\rangle) + (\alpha\|d_j^k\rangle + \beta\|1 \oplus d_j^k\rangle)]$

(3) A semi-trusted third party's attack

In the proposed protocol, TP is semi-trusted, which implies that he cannot conspire with the other participants to carry out bad activities, but he can misbehave himself. For convenience, the semi-trusted third party is denoted as TP*, who hopes to gain P_j's secret integer S_j. In order to achieve this goal, TP* can intercept the photons sent by P_{j-1} and resend a fake photon sequence to P_j. In this case, although TP* can infer the identity encoding operation acting on the pseudo photon based on h_j, he does not know the position of the detection photons in the travelling photon sequence. Therefore, their behaviour

introduces errors as Eve does and is detected in step 7. As a conclusion, the proposed protocol is resistant to attacks by semi-trusted third party.

(4) Impersonation attack

In addition to the above attacks, impersonation attack from an adversary should be considered. Depending on the function of the role in the protocol, we can analyze impersonation attack from two aspects.

Case 1: Impersonating the third party

In this attack, an adversary can impersonate a semi-trusted third-party TP to execute the protocol, in which he attempts to attack the participants and obtain their secret integers S_j. For simplicity, the adversary is recorded as $\widehat{TP}$. In the semi-honest third-party attack, it has been shown that a genuine third-party TP cannot even gain access to the secret information S_j of the participants, and hence it can be deduced that the impersonated $\widehat{TP}$ cannot successfully eavesdrop as well. In a word, the proposed protocol is resistant to the attack of impersonating a semi-trusted third party.

Case 2: Impersonating a participant

Here, an adversary can impersonate a participant P_j and executes the protocol with the other participants. The adversary is indicated by $\widehat{P}_j$. His aim is to eavesdrop the private key $\overline{k}_j$, and compute the summation result S while successfully tricking the other participants. However, this is not possible. Because $\widehat{P}_j$ has no knowledge of P_j's hash value h_j, thus he cannot deduce the private key $\overline{k}_j$ from the public information, nor can he perform the correct identity authentication operation. It will result in a change in the final particles obtained by TP, and the results obtained with the base $\{|0\rangle, |1\rangle\}$ measuring will also be random. Such the behaviour of $\widehat{P}_j$ will be detected in the eavesdropping detection in step 7. Consequently, this attack is ineffective against our protocol.

To sum up, the proposed protocol is resistant to impersonation attacks from the adversary.

4.3. Comparison

We compare the performance of the proposed protocol and the existing QSMS protocols [33,36–38,45] in terms of quantum resource, model, function and quantum efficiency, which is shown in Table 5.

Table 5. Comparison with previous protocols.

Protocols	Quantum Resource	TP	Authentication	Quantum Efficiency
Zhang et al. [33]	Single-particle state	Yes	No	$\frac{L}{2N\delta+L}$
Zhang et al. [36]	Single-particle state	No	No	$\frac{L}{N(2\delta+L)-\delta}$
Liu et al. [37]	2-particle Bell state	Yes	No	$\frac{L}{N(2\delta+L)-2\delta}$
Liu et al. [38]	single-particle state	Yes	No	$\frac{L}{N\delta+L}$
Zhang et al. [45]	2-particle entangled state	Yes	No	$\frac{2L}{N(2\delta+L)+2\delta+2L}$
Our protocol	Single-particle state	Yes	Yes	$\frac{L}{N\delta+L}$

As a convenience, we assume that the number of participants in all protocols is N, the semi-trusted third parties involved is TP, and the length of a secret integer is L. When eavesdropping detection is required between two parties, the number of decoy particles they make use of is δ. The quantum efficiency can be defined as

$$\eta = \frac{c}{q+b}. \tag{30}$$

Here, c denotes the total number of bits in the classical plaintext message, q represents the total number of quantum bits used in the quantum protocol, and b indicates the number of exchanged classical bits used to decode the message.

Although the protocols of Zhang et al. [36] and Zhang et al. [45] initially prepare single-particle and two-particle states, respectively, they both require to generate multi-

particle entangled states with unitary operations during the execution of the protocol. However, our protocol adopts quantum resources that exist as single particles throughout the execution of the protocol. In protocols [36,37,45], one of the particles of the entangled state needs to be kept in the hands of the preparer, and the other particles is transmitted as a travelling particle. It has the potential to become unentangled during transmission, which does not guarantee that the secret data of each participant acts on the quantum state to participate in the summation. Furthermore, it is easier to prepare a single-particle state than a multi-particle entangled state on the basis of current technology. Therefore, the proposed protocol has the advantage of quantum resources.

As with the protocols [33,37,38,45], our protocol also requires the help of a semi-trusted third party to implement the sum. However, our protocol has identity authentication function, which can resist impersonation attacks. Compared with Zhang et al.'s protocol [36], the proposed protocol still possesses that advantage. As can be seen from Table 5, even though the quantum efficiency of the proposed protocol is the same as that of the protocol [38], the proposed protocol implements the identity authentication function. The quantum efficiency of the proposed protocol is better with respect to the protocols [33,36,37,45].

To sum up, the proposed protocol has significant advantages in terms of both quantum resource, function and quantum efficiency.

5. Experiments on the IBM Q Experience

In order to confirm the correctness of the proposed protocol, we run the example of the three-party quantum secure summation protocol given in Section 3 on the cloud quantum computing platform provided by IBM Q Experience [57]. In the example, TP prepares a quantum sequence $Q = |0\rangle_1|1\rangle_2|1\rangle_3|0\rangle_4$ based on the bit string $D_0 = 0110$. Then, TP and three participants perform the operations shown in Table 2.

In order to better conduct the experiment, we first need to design the corresponding quantum circuits for the four quantum states of the quantum sequence Q according to Figure 3, which are illustrated in Figure 6.

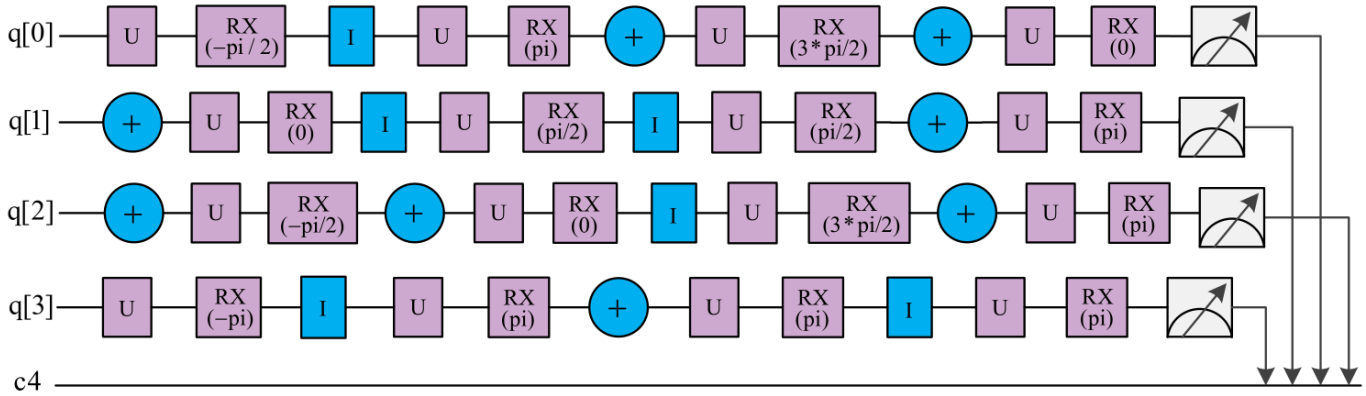

Figure 6. Quantum circuits corresponding to the quantum sequence $Q = |0\rangle_1|1\rangle_2|1\rangle_3|0\rangle_4$. The circuits of the quantum states q[0], q[1], q[2] and q[3] correspond to the initial states $|0\rangle_1$, $|1\rangle_2$, $|1\rangle_3$ and $|0\rangle_4$ in turn.

Here, + and I denote the Pauli operator X and I gates, respectively, and the operations U and RX are defined in the following form.

$$U(\omega,\phi,\lambda) = \begin{pmatrix} \cos\frac{\omega}{2} & -e^{i\lambda}\sin\frac{\omega}{2} \\ e^{i\phi}\sin\frac{\omega}{2} & e^{i(\phi+\lambda)}\cos\frac{\omega}{2} \end{pmatrix},$$
$$RX = \begin{pmatrix} \cos\frac{\omega}{2} & -i\sin\frac{\omega}{2} \\ -i\sin\frac{\omega}{2} & \cos\frac{\omega}{2} \end{pmatrix}. \quad (31)$$

Therefore, based on Equation (31), the rotation operation $G(\omega)$ used in the proposed QSMS protocol can be re-expressed as

$$G(\omega) = U(\pi, \frac{\pi}{2}, \frac{3\pi}{2})RX. \tag{32}$$

For the sake of improving the accuracy of the experiments, we, respectively, run five rounds for each quantum circuit in Figure 6, each round containing 8192 shots. The corresponding simulation statistics for each circuit are shown in Figure 7.

As can be seen from Figure 7, the measured probabilities of obtaining the four final quantum states $|0\rangle_1|0\rangle_2|1\rangle_3|1\rangle_4$ through simulation experiment, which are compared with the theoretically expected probabilities of gaining the final quantum states $Q_3 = |0\rangle_1|0\rangle_2|1\rangle_3|1\rangle_4$ in the example given in Section 3, as shown in Table 6.

Table 6. The comparison between the measured and expected quantum states.

Final Quantum State	Measurement Probability	Expected Probability	Fidelity
$\|0\rangle$	100%	100%	1.00
$\|1\rangle$	100%	100%	1.00
$\|1\rangle$	100%	100%	1.00
$\|0\rangle$	100%	100%	1.00

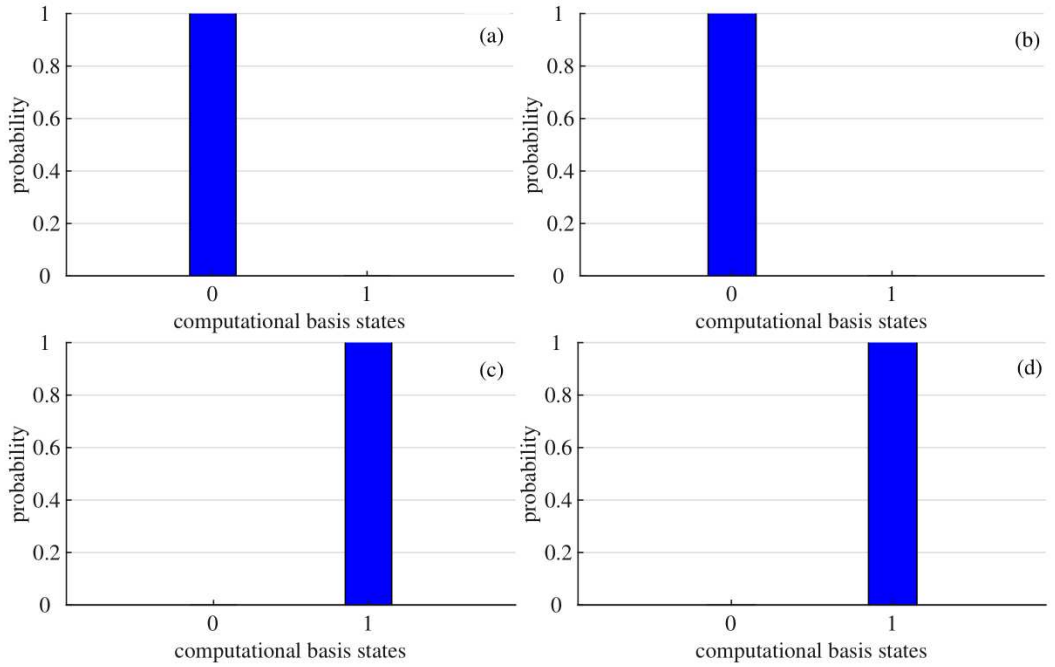

Figure 7. The measurement results of quantum circuits in Figure 6. The horizontal coordinate indicates computational basis states, 1 denotes $|1\rangle$ and 0 represents $|0\rangle$; The vertical coordinate represents the probability of obtaining the computational basis states by measurement. The initial states corresponding to (**a**–**d**) are $|0\rangle$, $|1\rangle$, $|1\rangle$, $|0\rangle$, respectively.

Due to both the expected gained quantum state $|\varphi_3^l\rangle$ and the measured state $|\varphi_3^l\rangle^*$ are pure states, we can calculate the fidelity (F) between them based on the Refs. [58,59]. The fidelity between two pure states is defined as

$$\begin{aligned} F(|\varphi_3^l\rangle\langle\varphi_3^l|, |\varphi_3^l\rangle^{**}\langle\varphi_3^l|) &= tr(\sqrt{|\varphi_3^l\rangle\langle\varphi_3^l||\varphi_3^l\rangle^{**}\langle\varphi_3^l||\varphi_3^l\rangle\langle\varphi_3^l|}) \\ &= |\langle\varphi_3^l|\varphi_3^l\rangle^*| \end{aligned}. \tag{33}$$

The fidelity F takes the value in [0, 1], which represents the mode of overlap between two pure states [58]. The fidelity between the measured four quantum states and the expected quantum states as shown in Table 6.

From Table 6, it can be seen that the measured probabilities and theoretical expected probabilities of obtaining the final quantum states are consistent, and their fidelity values all equal 1.00. In other words, the simulated experimental results for the quantum sequence $Q = |0\rangle_1|1\rangle_2|1\rangle_3|0\rangle_4$ turns out to be 100% correct, and the final quantum states $|0\rangle_1|0\rangle_2|1\rangle_3|1\rangle_4$ obtained by measurement are completely equivalent to the final quantum states $Q_3 = |0\rangle_1|1\rangle_2|1\rangle_3|0\rangle_4$ obtained theoretically in the example given in Section 3. The measurement result for $|0\rangle_1|0\rangle_2|1\rangle_3|1\rangle_4$ is $M = 0011$. Evidently, depending on the data provided in Table 2, we can obtain $S = M \oplus D_0 \oplus_{i=1}^{3} V_i = 0001$. That is, the sum of the secret data of the participants can be correctly obtained by simulation experiments. Therefore, the proposed protocol is feasible.

6. Conclusions

Before deriving our conclusions, we briefly discuss some advantages of the proposed protocol compared with Refs. [33,36–38,45]. Firstly, the impersonation attacks that are inevitable in practical applications are considered. Therefore, we exploit the technique of one-way hash function with key, and combine identity information and random strings to achieve the authentication of participants. Secondly, the theory of quantum state indistinguishability guarantees the security of the protocol. Specifically, the encoded quantum states cannot be unambiguously distinguished, hence, the attacker cannot obtain any information about participants' secret information. Thirdly, our protocol is feasible in technique. The implementation of the protocol only requires preparing single-photon states and performing single-photon measurements. As a result, it is easier to implement with the current technology. Finally, we conduct simulations on the IBM Q Experience cloud platform and confirm that the proposed protocol is effective.

In summary, we propose a QSMS protocol with identity authentication based on commutative encryption. In the protocol, the semi-trusted third party prepares single photons as information carriers, and shares a secret key with each participant. Depending on the calculated hash value, the semi-trusted third party performs the authentication operations on the prepared photons. All the participants then encode their secret integer and perform the authentication operation on the quantum sequence in turn. Finally, all participants calculate the sum of their secret integer with the help of the third party. The analysis of the protocol shows that the proposed protocol is correct, and can resist both common and impersonation attacks. In addition, we verify the proposed protocol on the IBM Q Experience cloud platform. The statistical results and the fidelity of the computed quantum states are 1, which demonstrates the feasibility of the proposed protocol.

Author Contributions: Methodology, N.W.; software, N.W.; validation, N.W.; formal analysis, N.W. and X.Z.; writing—original draft, N.W.; visualization, X.T.; writing—review and editing, S.L.; supervision, S.L.; project administration, S.L.; funding acquisition, S.L. All authors have read and agreed to the published version of the manuscript.

Funding: This work was supported by National Natural Science Foundation of China (Grants No. 61772134, No. 61976053, and No. 62171131), Fujian Province Natural Science Foundation (Grant No. 2022J01186), and Program for New Century Excellent Talents in Fujian Province University.

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.

References

1. Paraiso, T.K.; Woodward, R.I.; Marangon, D.G.; Lovic, V.; Yuan, Z.; Shields, A.J. Advanced laser technology for quantum communications (tutorial review). *Adv. Quantum Tech.* **2021**, *4*, 2100062. [CrossRef]
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661. [CrossRef] [PubMed]
3. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Modern Phys.* **2002**, *74*, 145. [CrossRef]
4. Cao, Y.; Zhao, Y.; Wang, Q.; Zhang, J.; Ng, S.X.; Hanzo, L. The evolution of quantum key distribution networks: On the road to the qinternet. *IEEE Comm. Surv. Tutor.* **2022**, *24*, 839–894. [CrossRef]
5. Sidhu, J.S.; Brougham, T.; McArthur, D.; Pousa, R.G.; Oi, D.K.L. Finite key effects in satellite quantum key distribution. *npj Quantum Inf.* **2022**, *8*, 18. [CrossRef]
6. Bloom, Y.; Fields, I.; Maslennikov, A.; Rozenman, G.G. Quantum cryptography—A simplified undergraduate experiment and simulation. *Physics* **2022**, *4*, 104–123. [CrossRef]
7. Liu, R.; Rozenman, G.G.; Kundu, N.K.; Chandra, D.; De, D. Towards the industrialisation of quantum key distribution in communication networks: A short survey. *IET Quantum Comm.* **2022**, *3*, 151–163. [CrossRef]
8. Zhong, Z.Q.; Wang, S.; Zhan, X.H.; Yin, Z.-Q.; Chen, W.; Guo, G.-C.; Han, Z.-F. Realistic and general model for quantum key distribution with entangled-photon sources. *Phys. Rev. A* **2022**, *106*, 052606. [CrossRef]
9. Shirko, O.; Askar, S. A novel security survival model for quantum key distribution networks enabled by software-defined networking. *IEEE Access* **2023**, *11*, 21641–21654. [CrossRef]
10. Li, D.D.; Tang, Y.L.; Zhao, Y.K.; Zhou, L.; Zhao, Y.; Tang, S.-B. Security of optical beam splitter in quantum key distribution. *Photonics* **2022**, *9*, 527. [CrossRef]
11. Mafu, M.; Sekga, C.; Senekane, M. Security of Bennett–Brassard 1984 quantum-key distribution under a collective-rotation noise channel. *Photonics* **2022**, *9*, 941. [CrossRef]
12. Jiang, X.L.; Deng, X.Q.; Wang, Y.; Lu, Y.F.; Li, J.-J.; Zhou, C.; Bao, W.-S. Weak randomness analysis of measurement-device-independent quantum key distribution with finite resources. *Photonics* **2022**, *9*, 356. [CrossRef]
13. Hillery, M.; Bužek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829–1834. [CrossRef]
14. Karlsson, A.; Koashi, M.; Imoto, N. Quantum entanglement for secret sharing and secret splitting. *Phys. Rev. A* **1999**, *59*, 162–168. [CrossRef]
15. Xiao, L.; Long, G.L.; Deng, F.G.; Pan, J.W. Efficient multiparty quantum-secret-sharing schemes. *Phys. Rev. A* **2004**, *69*, 052307. [CrossRef]
16. Liu, B.; Gao, F.; Huang, W.; Wen, Q.Y. Multiparty quantum key agreement with single particles. *Quantum Inf. Process.* **2013**, *12*, 1797–1805. [CrossRef]
17. Sun, Z.W.; Cheng, R.; Wu, C.H.; Zhang, C. New fair multiparty quantum key agreement secure against collusive attacks. *Sci. Rep.* **2019**, *9*, 17177. [CrossRef]
18. Lin, S.; Zhang, X.; Guo, G.D.; Wang, L.L.; Liu, X.F. Multiparty quantum key agreement. *Phys. Rev. A* **2021**, *104*, 042421. [CrossRef]
19. Liu, B.; Gao, Z.F.; Xiao, D.; Huang, W.; Zhang, Z.-Q.; Li, Y.; Xu, B.-J. QKD-based quantum private query protocol in the single-photon interference communication system. *IEEE Access.* **2019**, *7*, 104749–104758. [CrossRef]
20. Liu, B.; Gao, F.; Huang, W.; Wen, Q.Y. QKD-based quantum private query without a failure probability. *Sci. China Phys. Mech. Astr.* **2015**, *58*, 100301. [CrossRef]
21. Gao, F.; Liu, B.; Wen, Q.Y.; Chen, H. Flexible quantum private queries based on quantum key distribution. *Opt. Exp.* **2012**, *20*, 17411–17420. [CrossRef]
22. Lo, H.K. Insecurity of quantum secure computations. *Phys. Rev. A* **1997**, *56*, 1154. [CrossRef] [PubMed]
23. Chau, H.F. Quantum-classical complexity-security trade off in secure multiparty computations. *Phys. Rev. A* **2000**, *61*, 032308. [CrossRef]
24. Ben-Or, M.; Crépeau, C.; Gottesman, D.; Hassidim, A.; Smith, A. Secure multiparty quantum computation with (only) a strict honest majority. In Proceedings of the 2006 47th Annual IEEE Symposium on Foundations of Computer Science (FOCS'06), Berkeley, CA, USA, 21–24 October 2006; IEEE: New York, NY, USA, 2006; pp. 249–260. [CrossRef]
25. Smith, A. Multi-party Quantum Computation. *arXiv* **2010**, arXiv:quant-ph/0111030.
26. Shi, R.H.; Li, Y.F. Quantum protocol for secure multiparty logical AND with application to multiparty private set intersection cardinality. *IEEE Trans. Circuits Syst. I Reg. Pap.* **2022**, *69*, 5206–5218.
27. Goldreich, O.; Micali, S.; Wigderson, A. How to play any mental game. In *Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing*; ACM: New York, NY, USA, 1987; p. 218. [CrossRef]
28. Heinrich, S. Quantum summation with an application to integration. *J. Complex.* **2002**, *18*, 1.
29. Heinrich, S.; Novak, E. On a problem in quantum summation. *J. Complex.* **2003**, *19*, 1. [CrossRef]
30. Heinrich, S.; Kwas, H.; Wozniakowski, M. Quantum Boolean summation with repetitions in the worst-average setting. *arXiv* **2003**, arXiv:quant-ph/0311036. [CrossRef]
31. Hillery, M.; Ziman, M.; Buzěk, V.; Bielikova, M. Towards quantum-based privacy and voting. *Phys. Lett. A* **2006**, *349*, 75.
32. Chen, X.B.; Xu, G.; Yang, Y.X.; Wen, Q.Y. An efficient protocol for the secure multi-party quantum summation. *Int. J. Theor. Phys.* **2010**, *49*, 2793. [CrossRef]
33. Zhang, C.; Sun, Z.; Huang, Y.; Long, D. High-capacity quantum summation with single photons in both polarization and spatial-mode degrees of freedom. *Int. J. Theor. Phys.* **2014**, *53*, 933–941. [CrossRef]

34. Shi, R.H.; Mu, Y.; Zhong, H.; Cui, J.; Zhang, S. Secure multiparty quantum computation for summation and multiplication. *Sci. Rep.* **2016**, *6*, 19655. [CrossRef]
35. Shi, R.H.; Zhang, S. Quantum solution to a class of two-party private summation problems. *Quantum Inf. Process.* **2017**, *16*, 225. [CrossRef] [PubMed]
36. Zhang, C.; Situ, H.; Huang, Q.; Yang, P. Multi-party quantum summation without a trusted third party based on single particles. *Int. J. Quantum Inf.* **2017**, *15*, 1750010. [CrossRef]
37. Liu, W.; Wang, Y.B.; Fan, W.Q. An novel protocol for the quantum secure multi-party summation based on two-particle bell states. *Int. J. Theor. Phys.* **2017**, *56*, 2783. [CrossRef]
38. Liu, W.; Ma, M.Y. An dynamic protocol for the quantum secure multi-party summation based on commutative encryption. In *Proceedings of the International Conference on Artificial Intelligence and Security* ; Springer: Cham, Switzerland, 2019; pp. 537–547. [CrossRef]
39. Yang, H.Y.; Ye, T.Y. Secure multi-party quantum summation based on quantum Fourier transform. *Quantum Inf. Process.* **2018**, *17*, 129.
40. Sutradhar, K.; Om, H. Hybrid quantum protocols for secure multiparty summation and multiplication. *Sci. Rep.* **2020**, *10*, 9097. [CrossRef]
41. Zhang, C.; Razavi, M.; Sun, Z.W.; Situ, H.Z. Improvementn "Secure multi-party quantum summation based on quantum Fourier transform". *Quantum Inf. Process.* **2019**, *18*, 336. [CrossRef]
42. Zhang, C.; Long, Y.X.; Li, Q. Quantum summation using d-level entanglement swapping. *Quantum Inf. Process.* **2021**, *20*, 137. [CrossRef]
43. Wu, W.Q.; Ma, X.X. Multi-party quantum summation without a third party based on d-dimensional bell states. *Quantum Inf. Process.* **2021**, *20*, 200. [CrossRef]
44. Wang, Y.L.; Hu, P.C.; Xu, Q.L. Quantum secure multi-party summation based on entanglement swapping. *Quantum Inf. Process.* **2021**, *20*, 319. [CrossRef]
45. Zhang, X.; Lin, S.; Guo, G.D. Quantum secure multi-party summation based on Grover's search algorithm. *Int. J. Theor. Phys.* **2021**, *60*, 3711–3721. [CrossRef]
46. Sutradhar, K.; Om, H. A generalized quantum protocol for secure multiparty summation. *IEEE Trans. Circuits Syst. II Exp. Briefs.* **2020**, *67*, 2978–2982. [CrossRef]
47. Goldreich, O. Secure multi-party computation. Manuscript. *Prelim. Vers.* **1998**, *78*, 110. [CrossRef]
48. Brandt, N.; Maier, S.; Müller, T.; Müller-Quade, J. Constructing Secure Multi-Party Computation with Identifiable Abort. Cryptology ePrint Archive. 2020. Available online: https://eprint.iacr.org/2020/153 (accessed on 30 April 2023).
49. Kanamori, Y. Quantum Encryption and Authentication Protocols. Ph.D. Thesis, University of Alabama in Huntsville, Huntsville, AL, USA, 2006.
50. Cai, B.B.; Guo, G.D.; Lin, S. Multi-party Quantum Key Agreement without Entanglement. *Int. J. Theor. Phys.* **2017**, *56*, 1039–1051.
51. D'Ariano, G.M.; Presti, P.L.; Paris, M.G.A. Improved discrimination of unitary transformations by entangled probes. *J. Opt. B Quantum Semiclass. Opt.* **2002**, *4*, 273. [CrossRef]
52. Helstrom, C.W. *Quantum Detection and Estimation Theory*; Academic Press: Cambridge, MA, USA, 1976.
53. Huang, S.L.; Hwang, T.; Gope, P. Multi-party quantum private comparison with an almost-dishonest third party. *Quantum Inf. Process* **2015**, *14*, 4225–4235.
54. Chefles, A.; Barnett, S.M. Optimum unambiguous discrimination between linearly independent symmetric states. *Phys. Lett. A* **1998**, *250*, 223–229. [CrossRef]
55. Deng, F.; Li, X.; Zhou, H.; Zhang, Z.-J. Improving the security of multiparty quantum secret sharing against Trojan horse attack. *Phys. Rev. A* **2005**, *72*, 044302. [CrossRef]
56. Li, X.H.; Deng, F.G. Improving the security of secure direct communication based on the secret transmitting order of particles. *Phys. Rev. A* **2006**, *74*, 054302. [CrossRef]
57. Lu, C.B.; Miao, F.Y.; Hou, J.P.; Su, Z.F.; Xiong, Y. Quantum multiparty cryptosystems based on ahomomorphic random basis encryption. *Quantum Inf. Process.* **2020**, *19*, 293. [CrossRef]
58. Raynal, P. Unambiguous State Discrimination of two density matrices in Quantum Information Theory. *arXiv* **2006**, arXiv:quant-ph/0611133. [CrossRef]
59. Zyczkowski, K.; Sommers, H.J. Average fidelity between random quantum states. *Phys. Rev. A* **2005**, *71*, 032313.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.