mathematics

IMPACT FACTOR 2.2

CITESCORE 4.6

Article

Authenticated Multi-Party Quantum Private Set Intersection with Single Particles

Gong-De Guo, Li-Qin Zheng, Kai Yu and Song Lin

Special Issue

Quantum Cryptography and Applications

Edited by

Dr. Chun-Wei Yang, Dr. Chia-Wei Tsai and Dr. Jason Lin

MDPI

https://doi.org/10.3390/math13122019

mathematics

MDPI

Article

Authenticated Multi-Party Quantum Private Set Intersection with Single Particles

Gong-De Guo [1,2], Li-Qin Zheng [3], Kai Yu [4,*] and Song Lin [5,*]

[1] School of Artificial Intelligence, Xiamen Institute of Technology, Xiamen 361021, China; ggd@fjnu.edu.cn
[2] Artificial Intelligence Research Institute, Xiamen Institute of Technology, Xiamen 361021, China
[3] Science Research and Training Department, Fujian Institute of Education, Fuzhou 350001, China; zlq124033@163.com
[4] Digital Fujian Internet-of-Things Laboratory of Environmental Monitoring, Fujian Normal University, Fuzhou 350007, China
[5] College of Computer and Cyber Security, Fujian Normal University, Fuzhou 350007, China
* Correspondence: ykai95@163.com (K.Y.); lins95@fjnu.edu.cn (S.L.)

Abstract: As an important branch of secure multi-party computation, privacy set intersection enables multiple parties to input their private sets and jointly compute the intersection of these sets without revealing any information other than the intersection itself. With the increasing demand for privacy protection of user data, privacy set intersection has been widely used in privacy computing and other fields. In this paper, we utilize the properties of mutually unbiased bases to propose a multi-party quantum private set intersection protocol that incorporates identity authentication mechanisms. A semi-honest third party (TP) is introduced to facilitate the secure execution of this task among the multiple participating parties. The TP establishes a shared master key with each party, which serves as the basis for authenticating the identity of each participant throughout the protocol. Single-particle quantum states, prepared by the TP, act as the information carriers and are sequentially transmitted among the participating parties. Each party performs a local unitary operation on the circulating particle, thereby encoding their private data within the quantum state. At the end of the protocol, the TP announces his measurement result, by which all participants can concurrently ascertain the intersection of their private data sets. Notably, the proposed protocol eliminates the need for long-term storage of single-particle quantum states, thereby rendering it feasible with existing quantum technological capabilities. Furthermore, a comprehensive security analysis demonstrates that the protocol effectively resists some common external and internal attacks, thereby ensuring its theoretical security.

Keywords: quantum private set intersection; identity authentication; single particles; mutually unbiased bases

MSC: 81P94

Academic Editors: Chun-Wei Yang, Chia-Wei Tsai and Jason Lin

Received: 16 May 2025
Revised: 30 May 2025
Accepted: 11 June 2025
Published: 18 June 2025

Citation: Guo, G.-D.; Zheng, L.-Q.; Yu, K.; Lin, S. Authenticated Multi-Party Quantum Private Set Intersection with Single Particles. *Mathematics* **2025**, *13*, 2019. https://doi.org/10.3390/math13122019

1. Introduction

Based on the principles of quantum mechanics, particularly the Heisenberg uncertainty principle and the No-Cloning theorem, quantum cryptography transcends the computational limitations of classical encryption by utilizing physical laws to guarantee security. For example, the famous BB84 protocol [1] enables two parties to generate a shared secret key with unconditional security. This security arises from the impossibility of measuring or copying an unknown quantum state chosen from four mutually unbiased base states rather

than unproven mathematical hardness assumptions. Thus, quantum cryptography's security is information-theoretically verifiable, rendering it immune to advances in quantum computing. In the past three decades, researchers have attempted to use quantum cryptography to address other security issues, such as quantum secret sharing [2–5], quantum secure direct communication [6–9], quantum private comparison [10–14], and so on.

The extension of quantum cryptographic principles to multi-party computation introduces quantum private set intersection (QPSI), which is a critical tool for secure collaborative data analysis. In QPSI, multiple parties aim to compute the intersection of their private data sets without revealing any information beyond the intersection itself. Traditional classical private set intersection protocols face vulnerabilities to quantum attacks, as their security often hinges on computational assumptions that quantum computers could invalidate. In contrast, QPSI uses quantum-resistant techniques, such as single-photon manipulation [15–18], rotation operations [19–21], and entanglement-based correlations [22–24], to achieve quantum-proof security. By embedding security into the fabric of quantum physics, QPSI protocols offer a future-proof solution for privacy-preserving applications, such as contact tracking, federated learning, and medical data sharing, where the integrity of sensitive information must be preserved against both classical and quantum threats.

As demonstrated in Ref. [25], some theoretically secure quantum cryptography protocols remain susceptible to man-in-the-middle attacks, due to the lack of identity verification. This is especially true for QPSI. In a two-party QPSI protocol, if an adversary successfully impersonates a legitimate participant, he can easily steal the private data set of the other participant. Here, he does not need to perform any attack operation, but only needs to enter his secret data set as the full set when executing the protocol and then obtain the other private data set based on the final intersection result. Therefore, identity authentication should be considered when designing a practical QPSI protocol. In Ref. [25], Wu et al. delved into the issue and proposed a quantum protocol theoretically to achieve the computation of private sets with identity authentication. The protocol hinges on the quantum entanglement properties of Greenberger–Horne–Zeilinger (GHZ) states, ensuring that only two authenticated users can compute the private set intersection/union cardinality. Stimulated by this work, an authenticated multi-party quantum private set intersection protocol with single particles is presented in this paper. In the designed protocol, a third party is incorporated to enable the secure execution of private set intersection involving multiple participating entities. First, the TP shares a master key with each individual party that forms the cornerstone for authenticating the identity of every participant, ensuring a secure and verified environment throughout the protocol's execution. Secondly, single-particle quantum states prepared by the TP, which serve as carriers of sensitive data, are sequentially transmitted among the participating parties. Upon receiving the circulating particle, each party applies two phase operations to it. One operation is employed to encode the party's private data, while the other aims to keep the information confidential. Similarly to the BB84 protocol, mutually unbiased bases are utilized here to ensure the secure transmission of the particles. Finally, based on the public message declared by the TP, all participants can simultaneously determine the intersection of their private data sets. In this way, the goal of the protocol is achieved in a secure and efficient manner. Note that the TP in the proposed protocol here is assumed to be semi-honest [26]. If he were misbehaving, TP could collude with other participants to attack the protocol. In such a case, the protocol could be viewed as secure computation between two parties: one being the honest participants, and the other being the misbehaving TP combined with the remaining dishonest participants. According to the no-go theorem [27,28], such a quantum secure computation protocol would theoretically be unsafe. Therefore, like most quantum secure multi-party computation protocols, the TP

in this protocol is also assumed to be semi-honest. That is, he behaves honestly during the protocol execution and refrains from colluding with other participants, but may attempt to infer more information afterward.

The remainder of this paper is organized as follows. The relevant preliminary knowledge related to this paper is introduced in Section 2. Subsequently, the proposed multi-party quantum private set intersection protocol and a toy example are elaborated in Sections 3 and 4, respectively. The security of the proposed protocol is analyzed in Section 5. In Section 6, the experimental simulation is provided to demonstrate its feasibility. Finally, Section 7 offers a short conclusion.

2. Preliminary

Unlike classical bits, which can only exist in a definite state of 0 or 1, quantum bits (qubits) can exist in any superposition state. Moreover, it is impossible to accurately measure non-orthogonal quantum states simultaneously. This unique quantum property is often utilized in the design of quantum cryptographic protocols, such as the BB84 protocol [1]. In this protocol, four non-orthogonal quantum states, $|0\rangle, |1\rangle, |0'\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and $|1'\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, are used as signal particles for transmission, thereby ensuring the unconditional security of the protocol in theory. These four quantum states in a two-dimensional Hilbert space are composed of two sets of mutually unbiased bases (MUBs), $\{|0\rangle, |1\rangle\}$ and $\{|0'\rangle, |1'\rangle\}$, making the protocol more sensitive to eavesdropping.

For a d-dimensional Hilbert space H_d, there are at most $d+1$ mutually unbiased bases [29]. Suppose that the computational basis of H_d is denoted by $\Pi_d = \{|0\rangle, |1\rangle, \cdots, |d-1\rangle\}$. When d is an odd prime, the other d bases are given as $\Pi_0, \Pi_1, \cdots, \Pi_{d-1}$, where $\Pi_y = \{|\epsilon^d_{x,y}\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{k(x+yk)} |k\rangle \mid x, y \in Z_d, \omega = e^{2\pi \mathrm{i}/d}, \mathrm{i} = \sqrt{-1}\}$ and $Z_d = \{0, 1, \cdots, d-1\}$. Through simple calculations, it can be shown that for any $x, y, x', y', z \in Z_d$, $\langle z|\epsilon^d_{x,y}\rangle = \frac{1}{\sqrt{d}}$ and

$$\langle \epsilon^d_{x,y} | \epsilon^d_{x',y'} \rangle = \begin{cases} \frac{1}{\sqrt{d}} & \text{if } y \neq y' \\ 0 & \text{if } y = y' \end{cases}. \tag{1}$$

Thus, these $d+1$ sets of bases are mutually unbiased, and will be utilized in the protocol presented in this paper.

Moreover, the transformation between these states can be achieved using two unitary phase operators. One is $E^d_{x'}$, which is defined by

$$E^d_{x'} = \sum_{k=0}^{d-1} \omega^{kx'} |k\rangle\langle k|. \tag{2}$$

For any state $|\epsilon^d_{x,y}\rangle$, we have

$$E^d_{x'} |\epsilon^d_{x,y}\rangle = |\epsilon^d_{x+x',y}\rangle. \tag{3}$$

The other is $S^d_{y'}$,

$$S^d_{y'} = \sum_{k=0}^{d-1} \omega^{k^2 y'} |k\rangle\langle k|, \tag{4}$$

which can convert the state $|\epsilon^d_{x,y}\rangle$ to $|\epsilon^d_{x,y+y'}\rangle$, i.e.,

$$S^d_{y'} |\epsilon^d_{x,y}\rangle = |\epsilon^d_{x,y+y'}\rangle. \tag{5}$$

From Equations (3) and (5), we can derive

$$S_{y'}^{d} E_{x'}^{d} |\epsilon_{x,y}^{d}\rangle = |\epsilon_{x+x',y+y'}^{d}\rangle. \tag{6}$$

That is, any $|\epsilon_{x,y}^{d}\rangle$ can be transformed into $|\epsilon_{x+x',y+y'}^{d}\rangle$ by performing the unitary operator $S_{y'}^{d} E_{x'}^{d}$. Thus, these two operators will serve as the encoding and encrypting operations, respectively, in the presented protocol.

3. Proposed Protocol

In this section, we propose a multi-party QPSI protocol with identity authentication. For generality, we consider a system model consisting of m participants, Bob_i ($i = 1, 2, \cdots, m$) and a third party, Trent. Each participant Bob_i holds a private data set $B_i = \{b_i^1, b_i^2, \cdots, b_i^{n_i}\} \subseteq Z_n = \{0, 1, \cdots, n-1\}$, and has a secure key k_i with Trent. With the help of Trent, the m participants aim to securely compute the intersection of their private sets, denoted as $B_1 \cap B_2 \cap \cdots \cap B_m$. Meanwhile, the identity of each Bob_i is authenticated by Trent. The entire communication process is shown in Figure 1. The proposed protocol consists of four phases, which are detailed as follows.

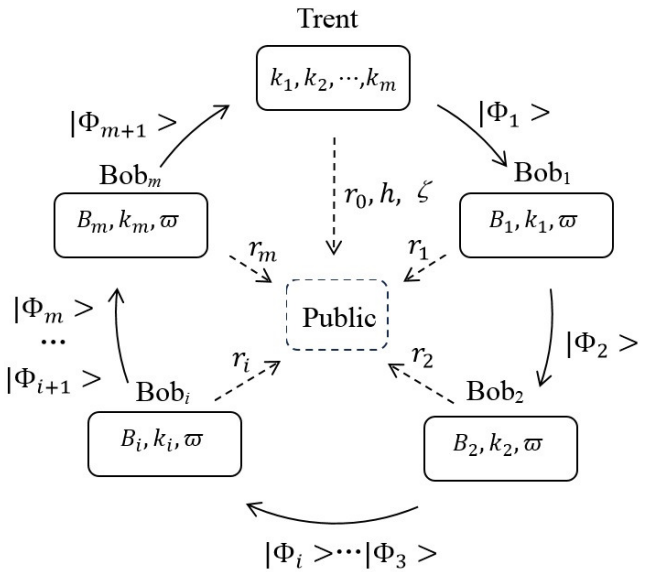

Figure 1. Communications in the proposed protocol. The solid line represents the transmission of a quantum message between two participants, and a dashed line represents a classical authenticated message.

I. Initializing phase

I.1. m participants Bob_i request a PSI from Trent. They each generate a random bit string r_i and send it to Trent. Meanwhile, according to the following rule,

$$c_i^j = \begin{cases} 1 & \text{if } j \in B_i \\ 0 & \text{otherwise} \end{cases}, \tag{7}$$

each participant Bob_i converts his secret private set B_i into an n-bit string $C_i = (c_i^1, c_i^2, \cdots, c_i^n)$.

I.2. Based on the actual environment and security requirements, Trent sets a security parameter ξ, which is the number of particles detected. Then, he chooses a hash function from a class of universal one-way hash function, $h : \{0,1\}^* \to \{0, 1, \cdots, d-1\}^{n'}$, where $n' = n + \xi$ and $d > m$. He generates a random bit string r_0, and calculates m private

strings, $Y_1, Y_2, \cdots, Y_m$, where $Y_i = (y_i^1, y_i^2, \cdots, y_i^{n'}) = h(r_0||r_1||\cdots||r_m||k_i)$. At last, Trent announces ξ, h, and r_0 to all participants.

I.3. After receiving the messages announced by Trent, each participant Bob_i obtains his authenticated message by calculating $Y_i = (y_i^1, y_i^2, \cdots, y_i^{n'}) = h(r_0||r_1||\cdots||r_m||k_i)$. After that, these m participants agree on a permutation function ϖ, which transforms each element of the set $Z_{n'}$ into a unique element within the same set, with no repetitions or omissions. Finally, each participant Bob_i generates a private ξ-bit string, $A_i = (a_i^1, a_i^2, \cdots, a_i^{\xi})$, which is used as the check samples. Bob_i utilizes the function ϖ to permute the bit string $C_i||A_i$ and obtain a new bit string $X_i = (x_i^1, x_i^2, \cdots, x_i^{n'})$.

II. Quantum phase

II.1. Trent prepares n' particles, each initially in the state $|\epsilon_{0,0}^d\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} |k\rangle$. For the j-th particle ($j = 1, 2, \cdots, n'$), Trent generates two random numbers $x_0^j, y_0^j \in Z_d$. According to these two values, he performs the operation $S_{y_0^j}^d E_{x_0^j}^d$ on the particle, and obtains the state, $|\phi_1^j\rangle = S_{y_0^j}^d E_{x_0^j}^d |\epsilon_{0,0}^d\rangle = |\epsilon_{x_0^j, y_0^j}^d\rangle$. Finally, Trent sends these n' particles in the state $|\Phi_1\rangle = \otimes_{j=1}^{n'} |\phi_1^j\rangle$ to the first participant Bob_1.

II.2. Upon receiving the quantum state $|\phi_1^j\rangle$ ($j = 1, 2, \cdots, n'$), Bob_1 performs his encoding operation $E_{x_1^j}^d$ on the signal particle, and executes the encrypting operation, $S_{y_1^j}^d$. In this way, Bob_1 obtains the state $|\Phi_2\rangle = \otimes_{j=1}^{n'} |\phi_2^j\rangle$, where $|\phi_2^j\rangle = S_{y_1^j}^d E_{x_1^j}^d |\phi_1^j\rangle = |\epsilon_{x_0^j + x_1^j, y_0^j + y_1^j}^d\rangle$ and sends it to the next participant, Bob_2.

II.3. Bob_i ($i = 2, 3, \cdots, m$) conducts a process analogous to that in II.2. Specifically, when Bob_i receives the j-th signal particle, he performs his operation $S_{y_i^j}^d E_{x_i^j}^d$ on it. Then, he sends the quantum state $|\phi_{i+1}^j\rangle = S_{y_i^j}^d E_{x_i^j}^d |\phi_i^j\rangle = |\epsilon_{x_0^j + x_1^j + \cdots + x_i^j, y_0^j + y_1^j + \cdots + y_i^j}^d\rangle$ to the subsequent participant. Notably, the last participant, Bob_m, returns these n' signal particles to Trent.

II.4. When receiving the quantum state $|\phi_{m+1}^j\rangle$, Trent performs the corresponding decrypting operation, $S_{-y_0^j - y_1^j - \cdots - y_m^j}^d$, on the state $|\phi_{m+1}^j\rangle$. Then, he measures these signal particles in the bases $\Pi_0 = \{|\epsilon_{0,0}^d\rangle, |\epsilon_{1,0}^d\rangle, \cdots, |\epsilon_{d-1,0}^d\rangle\}$, and obtains the result, o^j. According to o^j and x_0^j, Trent calculates $z^j = o^j - x_0^j$, and obtains $Z = (z^1, z^2, \cdots, z^{n'})$.

III. Eavesdropping check phase

The m participants tell Trent the positions of the test samples, i.e., $\{\varpi(n+1), \varpi(n+2), \cdots, \varpi(n')\}$, and tell Trent their A_is, respectively. In terms of these public messages, Trent uses these ξ samples to execute the eavesdropping detection process. Concretely, for the j-th sample ($j = 1, 2, \cdots, \xi$), Trent judges whether $o^{\varpi(j+n)}$ is equal to $x_0^{\varpi(j+n)} + a_1^j + a_2^j + \cdots + a_m^j$ or not. If they are not equal, the number of errors is increased by 1. Finally, if the error rate exceeds a predefined threshold, Trent believes that the protocol is eavesdropping, abandons and restarts the protocol. Otherwise, he proceeds to the next step.

IV. Result announcement phase

After abandoning these test samples, Trent obtains the remaining n results to get $T = (t^1, t^2, \cdots, t^n)$. When $t^j = m$, he announces the value of j. In accordance with this message, all participants infer that the $\varpi^{-1}(j)$-th element is present in the intersection of their private data sets. In this way, the m participants simultaneously acquire the intersection of their private data sets, $B_1 \cap B_2 \cap \cdots \cap B_m$.

4. Toy Example

In this section, we will take a toy example (depicted in Table 1) to better understand the presented protocol and show that it is correct. Suppose Bob_1, Bob_2, Bob_3, and Bob_4 are four parties ($m = 4$, $d = 5$), and $B_1, B_2, B_3, B_4 \in Z_6$ ($n = 6$) are their private sets, respectively,

where $B_1 = \{1,4\}, B_2 = \{2,3,4\}, B_3 = \{0,3,4\}$, and $B_4 = \{4,5\}$. In accordance with Equation (7), the four participants each calculate their private six-bit strings, C_1 = '010010', C_2 = '001110', C_3 = '100110', and C_4 = '000011'. Additionally, they each share four master keys, k_1 = '0010111111', k_2 = '1100011010', k_3 = '0100000110', and k_4 = '0011001111', with Trent.

Table 1. The quantum and classical sequences in this toy example.

	Trent	**Bob$_1$**	**Bob$_2$**	**Bob$_3$**	**Bob$_4$**
Input	k_1, k_2, k_3, k_4	$B_1 = \{1,4\}$ k_1 = '0010111111'	$B_2 = \{2,3,4\}$ k_2 = '1100011010'	$B_3 = \{0,3,4\}$ k_3 = '0100000110'	$B_4 = \{4,5\}$ k_4 = '0011001111'
Phase I	r_0 = '0100000110' Y_1, Y_2, Y_3, Y_4	C_1 = '010010' r_1 = '0011010001' Y_1 = '0000011100' A_1 = '1101' X_1 = '1100011001'	C_2 = '001110' r_2 = '1101000010' Y_2 = '1110111001' A_2 = '1000' X_2 = '1000101100'	C_3 = '100110' r_3 = '0111111101' Y_3 = '0110100101' A_3 = '0101' X_3 = '1000010111'	C_4 = '000011' r_4 = '1111001011' Y_4 = '0001101100' A_4 = '0100' X_4 = '1001000001'
Phase II	X_0 = '1000010101' Y_0 = '1011011000' $\|\Phi_1\rangle = \|\epsilon^5_{1,1}\rangle\|\epsilon^5_{0,0}\rangle$ $\|\epsilon^5_{0,1}\rangle\|\epsilon^5_{0,1}\rangle\|\epsilon^5_{0,0}\rangle\|\epsilon^5_{1,1}\rangle$ $\|\epsilon^5_{0,1}\rangle\|\epsilon^5_{1,0}\rangle\|\epsilon^5_{0,0}\rangle\|\epsilon^5_{1,0}\rangle$ Z = '4101122213'	$\|\Phi_2\rangle = \|\epsilon^5_{2,1}\rangle\|\epsilon^5_{1,0}\rangle$ $\|\epsilon^5_{0,1}\rangle\|\epsilon^5_{0,1}\rangle\|\epsilon^5_{0,0}\rangle\|\epsilon^5_{2,2}\rangle$ $\|\epsilon^5_{1,2}\rangle\|\epsilon^5_{1,1}\rangle\|\epsilon^5_{0,0}\rangle\|\epsilon^5_{2,0}\rangle$	$\|\Phi_3\rangle = \|\epsilon^5_{3,2}\rangle\|\epsilon^5_{1,1}\rangle$ $\|\epsilon^5_{0,2}\rangle\|\epsilon^5_{0,1}\rangle\|\epsilon^5_{1,1}\rangle\|\epsilon^5_{2,3}\rangle$ $\|\epsilon^5_{2,3}\rangle\|\epsilon^5_{2,1}\rangle\|\epsilon^5_{0,0}\rangle\|\epsilon^5_{2,1}\rangle$	$\|\Phi_4\rangle = \|\epsilon^5_{4,2}\rangle\|\epsilon^5_{1,2}\rangle$ $\|\epsilon^5_{0,3}\rangle\|\epsilon^5_{0,1}\rangle\|\epsilon^5_{1,2}\rangle\|\epsilon^5_{3,3}\rangle$ $\|\epsilon^5_{2,3}\rangle\|\epsilon^5_{3,2}\rangle\|\epsilon^5_{1,0}\rangle\|\epsilon^5_{3,2}\rangle$	$\|\Phi_5\rangle = \|\epsilon^5_{5,2}\rangle\|\epsilon^5_{1,2}\rangle$ $\|\epsilon^5_{0,3}\rangle\|\epsilon^5_{1,2}\rangle\|\epsilon^5_{1,3}\rangle\|\epsilon^5_{3,3}\rangle$ $\|\epsilon^5_{2,4}\rangle\|\epsilon^5_{3,3}\rangle\|\epsilon^5_{1,0}\rangle\|\epsilon^5_{4,2}\rangle$
Phase III	'0223'	'0111'	'0010'	'0101'	'0001'
Phase IV	$j = 0$				

In Step I.1, these participants respectively generate four random bit strings, r_1 = '0011010001', r_2 = '1101000010', r_3 = '0111111101', and r_4 = '1111001011', and send them to Trent. Then, Trent sets $\xi = 4$ ($n' = n + \xi = 10$), r_0 = '0100000110', and the hash function h. Here, for simplicity, the hash function is set as $h(r_0||r_1||r_2||r_3||r_4||k_i) = r_0 \oplus r_1 \oplus r_2 \oplus r_3 \oplus r_4 \oplus k_i$, where $\oplus$ denotes a bitwise exclusive-OR (XOR) operation. Based on this function and k_i, Bob$_i$ (i = 1, 2, 3, 4) and Trent obtain Y_i, depicted in Table 1, and keep it secret. In Step I.3, four participants respectively generate four 4-bit strings, A_1 = '1101', A_2 = '1000', A_3 = '0101', and A_4 = '0100', and agree on a permutation function $\varpi(j) = (3j + 8) \bmod 10$ that is only known to them. Based on this function, the corresponding permutation table (Table 2) is derived. Then, Bob$_i$ can calculate $X_i = \varpi(C_i||A_i)$ as specified in Table 1.

Table 2. The permutation table.

0	1	2	3	4	5	6	7	8	9
8	1	4	7	0	3	6	9	2	5

In Step II, Trent generates two random bit strings X_0 = '1000010101', and Y_0 = '1011011000', and prepares 10 particles that are in the state $|\Phi_1\rangle = \otimes_{j=1}^{10}|\phi_1^j\rangle = |\epsilon_{0,0}^5\rangle$. After that, these ten signal particles are transmitted among the four participants. Each participant Bob_i performs his encoding operation and encrypting operation on these particles, and obtains the state $|\Phi_{i+1}\rangle$ as outlined in Table 1. In Step II.4, Trent applies the corresponding decrypting operation to these particles, and measures them in the basis Π_0. For example, the first qudit is in the state $|\epsilon_{1,1}^5\rangle$, after Trent applies the operation $S_{y_0^j}^d E_{x_0^j}^d$ on state $|\epsilon_{0,0}^5\rangle$. Subsequently, four participants, respectively, execute operations $S_0^d E_1^d$, $S_1^d E_1^d$, $S_0^d E_1^d$, and $S_0^d E_1^d$, when they receive this qudit. In this case, the state is transformed to $|\epsilon_{5,2}^5\rangle$ and returned to Trent. After that, Trent executes the decrypting operation S_{-2}^d, and obtains the measurement result '5'. From this result and the first bit of X_0, he deduces that the first bit of Z is '4'.

In the eavesdropping check phase, the four participants tell Trent the positions of four samples, i.e., 2, 5, 6, and 9, and their A_is. Based on these messages and Z, Trent determines whether the particles have been transmitted securely. After discarding the four samples, Trent obtains $t^0 = 4 = m$, and announces it in Step IV. From this public message and the permutation function ϖ, the four participants can concurrently ascertain the intersection of their private data sets, i.e., $B_1 \cap B_2 \cap B_3 \cap B_4 = \{\varpi^{-1}(0) = 4\}$.

From the above example, it can be seen that the proposed protocol requires that the dimension $d = 5$ of the signal particles be a prime number greater than the number of participants, $m = 4$. When the number of participants is large, this prime number becomes very large, which greatly limits the practicality of the proposed protocol. To solve this problem, we can group the users. Concretely, all participants are randomly divided into g disjoint groups, and then each group of participants performs the proposed protocol with Trent. In this way, Trent can obtain the intersection of private data sets of participants in each of the g groups, and further intersecting these intersections can yield the intersection of all private data sets. This solution effectively addresses the issue of the number of participants in the proposed protocol, but may lead to the leakage of some information to Trent, thereby reducing the security level of the protocol.

To further address this issue, the Chinese Remainder Theorem can be applied, which is similar to that in Ref. [30]. Given the number of participants m, a series of small primes $d_1, d_2, \cdots, d_r$ can be obtained such that $D = d_1, d_2, \cdots, d_r > m$. By executing the proposed protocol for r rounds, a series of values $t_{d_1}^j, t_{d_2}^j, \cdots, t_{d_r}^j$ can be obtained and satisfy the following equation:

$$\begin{cases} t_{d_1}^j = t^j \bmod d_1 \\ t_{d_2}^j = t^j \bmod d_2 \\ \quad \cdots \\ t_{d_r}^j = t^j \bmod d_r \end{cases} \tag{8}$$

Then, according to the Chinese Remainder Theorem, t^j can be calculated,

$$t^j = \sum_{i=1}^{r} D_i \times e_i \times t_{d_i}^j \bmod D, \tag{9}$$

where $D = \prod_{i=1}^{r} d_i$, $D_i = \frac{D}{d_i}$, and $1 = e_i \times D_i \bmod d_i$. Next, let us consider the same scenario as in the above example. Here, the four master keys, four private data sets, and two functions (h, ϖ) are identical to those in the previous example and are denoted using the same notation. Additionally, Trent and four participants agree on two primes $d_1 = 2$ and $d_2 = 3$, and execute the proposed protocol in two rounds.

In the first round, Trent and four participants respectively generate five new random bit strings, r_0 = '1101000010', r_1 = '0111111101', r_2 = '1111001011', r_3 = '0100000110', and r_4 = '1111101100'. Based on two new random bit strings X_0' = '0000000110' and Y_0' = '0001001111', Trent prepares ten qubits in the state $|\Phi_1'\rangle = |\epsilon_{0,0}^2\rangle|\epsilon_{0,0}^2\rangle|\epsilon_{0,0}^2\rangle|\epsilon_{0,1}^2\rangle|\epsilon_{0,0}^2\rangle$ $|\epsilon_{0,0}^2\rangle|\epsilon_{0,1}^2\rangle|\epsilon_{1,1}^2\rangle|\epsilon_{1,1}^2\rangle|\epsilon_{0,1}^2\rangle$ and transmits them to Bob_1. After four participants respectively perform their operation on these qubits and send them back to Trent, he measures these qubits and obtains t_2 = '011101'. Similarly, in the second round, ten qutrits are used as signal particles and transmitted among Trent and four participants. After that, Trent obtains t_3 = '011101'. The corresponding quantum and classical sequences of these two rounds are presented in Tables 3 and 4 , respectively. In terms of t_2 and t_3, Trent calculates t = '411121' using Equation (8), and then declares $t^0 = 4 = m$ to four participants.

Table 3. The quantum and classical sequences of the first round.

	Trent	**Bob_1**	**Bob_2**	**Bob_3**	**Bob_4**
Input	k_1, k_2, k_3, k_4	$B_1 = \{1, 4\}$ k_1 = '0010111111'	$B_2 = \{2, 3, 4\}$ k_2 = '1100011010'	$B_3 = \{0, 3, 4\}$ k_3 = '0100000110'	$B_4 = \{4, 5\}$ k_4 = '0011001111'
Phase I	r_0' = '1101000010' Y_1', Y_2', Y_3', Y_4'	C_1 = '010010' r_1' = '0111111101' Y_1' = '1100100001' A_1' = '0111' X_1' = '1110010001'	C_2 = '001110' r_2' = '1111001011' Y_2' = '0010000100' A_2' = '0101' X_2' = '1000110101'	C_3 = '100110' r_3' = '0100000110' Y_3' = '1010011000' A_3' = '1100' X_3' = '1000001111'	C_4 = '000011' r_4' = '1111101100' Y_4' = '1101010001' A_4' = '1111' X_4' = '1011011001'
Phase II	X_0' = '0000000110' Y_0' = '0001001111' $\|\Phi_1'\rangle = \|\epsilon_{0,0}^2\rangle\|\epsilon_{0,0}^2\rangle$ $\|\epsilon_{0,0}^2\rangle\|\epsilon_{0,1}^2\rangle\|\epsilon_{0,0}^2\rangle\|\epsilon_{0,0}^2\rangle$ $\|\epsilon_{0,1}^2\rangle\|\epsilon_{1,1}^2\rangle\|\epsilon_{1,1}^2\rangle\|\epsilon_{0,1}^2\rangle$ Z = '0101110010'	$\|\Phi_2'\rangle = \|\epsilon_{1,1}^2\rangle\|\epsilon_{1,1}^2\rangle$ $\|\epsilon_{1,0}^2\rangle\|\epsilon_{0,1}^2\rangle\|\epsilon_{0,1}^2\rangle\|\epsilon_{1,0}^2\rangle$ $\|\epsilon_{0,1}^2\rangle\|\epsilon_{1,1}^2\rangle\|\epsilon_{1,1}^2\rangle\|\epsilon_{1,0}^2\rangle$	$\|\Phi_3'\rangle = \|\epsilon_{0,1}^2\rangle\|\epsilon_{1,1}^2\rangle$ $\|\epsilon_{1,1}^2\rangle\|\epsilon_{0,1}^2\rangle\|\epsilon_{1,1}^2\rangle\|\epsilon_{0,0}^2\rangle$ $\|\epsilon_{0,1}^2\rangle\|\epsilon_{0,0}^2\rangle\|\epsilon_{1,1}^2\rangle\|\epsilon_{0,0}^2\rangle$	$\|\Phi_4'\rangle = \|\epsilon_{1,0}^2\rangle\|\epsilon_{1,1}^2\rangle$ $\|\epsilon_{1,0}^2\rangle\|\epsilon_{0,1}^2\rangle\|\epsilon_{1,1}^2\rangle\|\epsilon_{0,1}^2\rangle$ $\|\epsilon_{1,0}^2\rangle\|\epsilon_{1,0}^2\rangle\|\epsilon_{0,1}^2\rangle\|\epsilon_{1,0}^2\rangle$	$\|\Phi_5'\rangle = \|\epsilon_{0,1}^2\rangle\|\epsilon_{1,0}^2\rangle$ $\|\epsilon_{0,0}^2\rangle\|\epsilon_{1,0}^2\rangle\|\epsilon_{1,1}^2\rangle\|\epsilon_{1,0}^2\rangle$ $\|\epsilon_{0,0}^2\rangle\|\epsilon_{1,0}^2\rangle\|\epsilon_{0,1}^2\rangle\|\epsilon_{0,1}^2\rangle$
Phase III	'0100'	'1101'	'0101'	'0011'	'1111'
Phase IV	$t_2 = 011101$				

Table 4. The quantum and classical sequences of the second round.

	Trent	**Bob$_1$**	**Bob$_2$**	**Bob$_3$**	**Bob$_4$**
Input	k_1, k_2, k_3, k_4	$B_1 = \{1,4\}$ k_1 = '0010111111'	$B_2 = \{2,3,4\}$ k_2 = '1100011010'	$B_3 = \{0,3,4\}$ k_3 = '0100000110'	$B_4 = \{4,5\}$ k_4 = '0011001111'
Phase I	r_0'' = '0010011111' $Y_1'', Y_2'', Y_3'', Y_4''$	C_1 = '010010' r_1'' = '1000010101' Y_1'' = '1000010110' A_1'' = '0010' X_1'' = '1110000000'	C_2 = '001110' r_2'' = '1011011000' Y_2'' = '0110110011' A_2'' = '1111' X_2'' = '1010111101'	C_3 = '100110' r_3'' = '1111110011' Y_3'' = '1110101111' A_3'' = '1001' X_3'' = '1000011110'	C_4 = '000011' r_4'' = '0100001000' Y_4'' = '1001100110' A_4'' = '0101' X_4'' = '1001010001'
Phase II	X_0'' = '1011101000' Y_0'' = '0101001011' $\|\Phi_1''\rangle = \|\epsilon^3_{1,0}\rangle\|\epsilon^3_{0,1}\rangle$ $\|\epsilon^3_{1,0}\rangle\|\epsilon^3_{1,1}\rangle\|\epsilon^3_{1,0}\rangle\|\epsilon^3_{0,0}\rangle$ $\|\epsilon^3_{1,1}\rangle\|\epsilon^3_{0,0}\rangle\|\epsilon^3_{0,1}\rangle\|\epsilon^3_{0,1}\rangle$ Z = '1121102212'	$\|\Phi_2''\rangle = \|\epsilon^3_{2,1}\rangle\|\epsilon^3_{1,1}\rangle$ $\|\epsilon^3_{2,0}\rangle\|\epsilon^3_{1,1}\rangle\|\epsilon^3_{1,0}\rangle\|\epsilon^3_{0,1}\rangle$ $\|\epsilon^3_{1,1}\rangle\|\epsilon^3_{0,1}\rangle\|\epsilon^3_{0,2}\rangle\|\epsilon^3_{0,1}\rangle$	$\|\Phi_3''\rangle = \|\epsilon^3_{0,1}\rangle\|\epsilon^3_{1,2}\rangle$ $\|\epsilon^3_{0,1}\rangle\|\epsilon^3_{1,1}\rangle\|\epsilon^3_{2,1}\rangle\|\epsilon^3_{1,2}\rangle$ $\|\epsilon^3_{2,1}\rangle\|\epsilon^3_{1,1}\rangle\|\epsilon^3_{0,0}\rangle\|\epsilon^3_{1,2}\rangle$	$\|\Phi_4''\rangle = \|\epsilon^3_{1,2}\rangle\|\epsilon^3_{1,0}\rangle$ $\|\epsilon^3_{0,2}\rangle\|\epsilon^3_{1,1}\rangle\|\epsilon^3_{2,2}\rangle\|\epsilon^3_{2,2}\rangle$ $\|\epsilon^3_{0,2}\rangle\|\epsilon^3_{2,2}\rangle\|\epsilon^3_{1,1}\rangle\|\epsilon^3_{1,0}\rangle$	$\|\Phi_5''\rangle = \|\epsilon^3_{2,0}\rangle\|\epsilon^3_{1,0}\rangle$ $\|\epsilon^3_{0,2}\rangle\|\epsilon^3_{2,2}\rangle\|\epsilon^3_{2,0}\rangle\|\epsilon^3_{0,2}\rangle$ $\|\epsilon^3_{0,2}\rangle\|\epsilon^3_{2,0}\rangle\|\epsilon^3_{1,2}\rangle\|\epsilon^3_{2,0}\rangle$
Phase III	'0022'	'1000'	'1111'	'0110'	'0101'
Phase IV	$t_3 = 111121$				

5. Security Analysis

The proposed protocol adopts a collaborative eavesdropping detection method, which can effectively enhance the detection efficiency and reduce the quantum capabilities required of participants, but it also leads to higher security risks for the protocol. In this section, a detailed security analysis of the protocol is provided. Based on the different roles of attackers in the protocol, three scenarios are considered, in which an external eavesdropper, some dishonest internal participants, and the semi-honest TP attack the proposed protocol, respectively.

5.1. External Attack

Suppose that an external attacker, Eve, aims to obtain information about the private data sets (e.g., B_i) of m participants (e.g., Bob$_i$). Obviously, she can only achieve her goal by obtaining X_i. In the protocol, the operations and measurements performed by Trent and m participants are completed locally, which means that this process is secure. Therefore, to eavesdrop on X_i, Eve must attack the transmission of particles between Trent and m participants. In addition, Eve may also impersonate a participant and use the participant's identity to execute the protocol. In this way, she tries to attain the intersection result of the private data sets, from which some information about the private data sets may be derived. In the following, we will analyze several common attack scenarios, including the

intercept–measure–resend attack, entanglement–measure attack, and impersonation attack, to demonstrate the protocol's resistance to external attack.

5.1.1. Intercept–Measure–Resend Attack

In this attack, Eve intercepts the quantum state $|\phi_i^j\rangle$ sent by Bob_{i-1} and performs a certain measurement on this signal particle. Based on the measurement result, she forges a new quantum state and sends it to Bob_i. In the proposed protocol, the signal particle is in one of $d \times d$ states from d MUBs. Since Eve doesn't know each participant's key K_i, she can't determine the correct y_i^j. In this case, she has to randomly choose one basis from the d bases to measure this particle.

When Eve selects the correct basis with a probability of $\frac{1}{d}$, her measurement result is accurate. The fabricated particle prepared based on this will successfully pass the eavesdropping detection in Step **III**. When she selects the incorrect basis, which occurs with a probability of $\frac{d-1}{d}$, her measurement result will be random. The corresponding fabricated particle will be detected in the eavesdropping detection phase with a probability of $\frac{d-1}{d}$ as well. In summary, the total error probability is $(\frac{d-1}{d})^2$, which is higher than the $\frac{1}{4}$ error probability in the BB84 protocol. Therefore, when the number of the test samples, ξ, is sufficiently large, the probability of detecting Eve's attack, $1-[1-(\frac{d-1}{d})^2]^{\xi}$, approaches 1.

5.1.2. Entanglement–Measure Attack

In this attack scenario, to eavesdrop on Bob_i's secret input x_i^j, Eve intercepts the quantum state $|\phi_i^j\rangle = |\epsilon_{\dot{x},\dot{y}}\rangle$ ($\dot{x} = x_0^j + x_1^j + \cdots + x_{i-1}^j$, $\dot{y} = y_0^j + y_1^j + \cdots + y_{i-1}^j$) sent by Bob_{i-1} and prepares an auxiliary particle $|0\rangle$. Subsequently, she entangles the signal particle with the auxiliary particle using a unitary operator Ξ. We write the most general operation Eve can do as

$$\Xi|k\rangle|0\rangle = \sum_{l=1}^{d-1} |l\rangle|\eta_{k,l}\rangle, \tag{10}$$

where $k \in Z_d$ and $|\eta_{k,l}\rangle$ are pure ancilla states uniquely determined by Ξ. The following conditions can be derived from the unitary feature of Ξ:

$$\sum_{l=1}^{d-1} \langle\eta_{k,l}|\eta_{k',l}\rangle = \delta_{k,k'} = \begin{cases} 1 & k = k' \\ 0 & k \neq k' \end{cases}, \tag{11}$$

After this unitary interaction, the signal particle and the auxiliary particle are in the state

$$|\varphi_1\rangle = \Xi|\phi_i^j\rangle|0\rangle = \Xi|\epsilon_{\dot{x},\dot{y}}\rangle|0\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{k(\dot{x}+\dot{y}k)} \sum_{l=0}^{d-1} |l\rangle|\eta_{k,l}\rangle. \tag{12}$$

Then, Eve sends the signal particle to Bob_i, and keeps the auxiliary particle in her possession. In Step II.3, Bob_i performs his operation $S_{y_i^j}^d E_{x_i^j}^d$ on the signal particle. The whole system is in the state

$$|\varphi_2\rangle = S_{y_i^j}^d E_{x_i^j}^d |\varphi_1\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{k(\dot{x}+\dot{y}k)} \sum_{l=0}^{d-1} \omega^{l(x_i^j+y_i^j l)} |l\rangle|\eta_{k,l}\rangle. \tag{13}$$

Similarly, after the remaining participants execute their operations, the state is converted to

$$|\varphi_3\rangle = S_{y_m^j}^d E_{x_m^j}^d \cdots S_{y_{i+1}^j}^d E_{x_{i+1}^j}^d |\varphi_2\rangle = \frac{1}{\sqrt{d}} \sum_{k=0}^{d-1} \omega^{k(\dot{x}+\dot{y}k)} \sum_{l=0}^{d-1} \omega^{l(x_i^j+\ddot{x}+y_i^j l+\ddot{y}l)} |l\rangle|\eta_{k,l}\rangle, \tag{14}$$

where $\ddot{x} = x_{i+1}^j + \cdots + x_m^j$ and $\ddot{y} = y_{i+1}^j + \cdots + y_m^j$. At the end of the protocol, Eve utilizes the auxiliary particle to eavesdrop on some information about x_i^j. However, it is impossible.

In the following, we will show that Eve cannot obtain any information about x_i^j under the condition that no errors are to occur.

In the eavesdropping detection phase, Trent applies the decrypting operation $S^d_{-y_0^j-y_1^j-\cdots-y_m^j}$ on the signal particle, and obtains the following state:

$$|\varphi_4\rangle = S^d_{-y_0^j-y_1^j-\cdots-y_m^j}|\varphi_3\rangle = \frac{1}{\sqrt{d}}\sum_{k=0}^{d-1}\omega^{k(\dot{x}+\dot{y}k)}\sum_{l=0}^{d-1}\omega^{l(x_i^j+\ddot{x}-\dot{y}l)}|l\rangle|\eta_{k,l}\rangle. \tag{15}$$

In order for there to be no errors, the projective measurement Π_0 executed by Trent should satisfy the following conditions:

$$(|\varphi_4\rangle, |\epsilon_{k,0}\rangle) = \begin{cases} 1 & k = \dot{x} + x_i^j + \ddot{x} \\ 0 & k \neq \dot{x} + x_i^j + \ddot{x} \end{cases}, \tag{16}$$

According to Equations (9) and (14), the following equations can be deduced:

$$\begin{cases} |\eta_{0,0}\rangle = |\eta_{1,1}\rangle = \cdots = |\eta_{d-1,d-1}\rangle, \\ |\eta_{k,l}\rangle = \mathbf{0} \text{ if } k \neq l \end{cases}, \tag{17}$$

where $\mathbf{0}$ denotes the null vector. As a result, it is evident that $|\varphi_1\rangle$ is a product of $|\phi_i^j\rangle$ and the ancilla. This implies that Eve cannot obtain more information about Bob_i's secret input x_i^j from observing the ancilla. Consequently, the proposed protocol is immune to the entanglement–measure attacks.

5.1.3. Impersonation Attack

Let us start by considering a simple scenario in which Eve impersonates a participant named Bob_i^*, together with other participants, makes a computation request to Trent. According to the protocol, she generates a random number $\tilde{r}_i$ and announces it publicly. However, since she does not know k_i, Eve cannot compute the correct $Y_i = h(r_0||\cdots\tilde{r}_i||\cdots||r_m||k_i)$. In Step II.3, she has to randomly select a $\tilde{y}_i^j$ and perform the operation $S^d_{\tilde{y}_i^j}$ on the j-th particle. Evidently, the probability of choosing incorrectly, that is, $\tilde{y}_i^j \neq y_i^j$, is $\frac{d-1}{d}$. In Step II.4, based on y_i^j, Trent performs his decrypting operation on this particle. When $\tilde{y}_i^j \neq y_i^j$, Trent's measurement basis does not match, causing the measurement result to be random. Therefore, the total probability of error is $(\frac{d-1}{d})^2$, which will inevitably be detected by Trent. Furthermore, since the protocol requires each participant to generate a random number r_i, this ensures that each Y_i remains fresh. In other words, even if Eve knows some old $\dot{Y}_i$s that Bob_i has used before, she cannot leverage this advantage for her impersonation attack. This is because the other random numbers $r_0, \cdots, r_{i-1}, r_{i+1}, \cdots, r_m$ are determined by Trent and other participants, and obviously Y_i generated based on these are not correlated with previous $\dot{Y}_i$ s.

Next, we discuss the worst-case scenario in which Eve impersonates $m-1$ participants. Without loss of generality, assume that Bob_1 is the honest participant, while the remaining $m-1$ participants, $\text{Bob}_2^*, \cdots$, and Bob_m^* are impersonated by Eve who intends to eavesdrop on Bob_1's secret input x_1^j. As shown in the above section, if they entangle an auxiliary particle with the signal particle, Eve cannot obtain x_1^j, because y_1^j is unknown to them. Therefore, they may utilize their advantage to perform a more practical attack that poses a viable threat to QPSI protocols without identity authentication.

After receiving the signal particle transmitted by Bob_1 in Step II.2, which is in the state $|\phi_2^j\rangle$, Eve carries out the encoding operation E_1^d on this particle $m-1$ times, i.e., $x_2^j = x_3^j = \cdots = x_m^j = 1$ and sends it back to Trent. The particle is in the state

$|\phi^j_{m+1}\rangle = |\epsilon_{x^j_0+x^j_1+m-1, y^j_0+y^j_1+\tilde{y}^j_2+\cdots+\tilde{y}^j_m}\rangle$. Here, the corresponding $\tilde{y}^j_i$ $(i = 2, 3, \cdots, m)$ is random, because Eve doesn't know k_i and cannot calculate the right $Y_i = (y^1_i, y^2_i, \cdots, y^{n'}_i) = h(r_0||r_1||\cdots||r_m||k_i)$. Thus, the probability that $\sum_{i=2}^m \tilde{y}^j_i$ is equal to $\sum_{i=2}^m y^j_i$ is $\frac{1}{d}$. After performing his decrypting operation on this particle, the state is not in one of the sets Π_0 if $\sum_{i=2}^m \tilde{y}^j_i \neq \sum_{i=2}^m y^j_i$, which occurs with a probability of $\frac{1}{d}$. In this case, Trent's measurement result is random, with a probability of $\frac{d-1}{d}$. No matter what fake messages in which Eve impersonates Bob^*_i $(i = 2, 3, \cdots, m)$ to announce in Phase III, this attack will also introduce a $(\frac{d-1}{d})^2$ error rate, which will be detected by Trent. Therefore, the result announcement phase is canceled, Eve cannot deduce any information about Bob_1's private set according to Trent's declared message in this phase. Moreover, since Y_1 remains confidential throughout the entire protocol execution, Eve is unable to infer Bob_1's master secret key k_1 based on the hash function h and the values of $r_0, r_1, \cdots, r_m$.

5.2. Internal Attack

In the PSI protocol, not all participants are honest. There may be one or more dishonest participants attempting to eavesdrop on secret information from other honest participants. Moreover, due to the involvement of internal participants in the protocol execution process, they may possess greater advantages than external attackers in eavesdropping on secret information. Generally speaking, internal participants pose a more significant threat compared to external attackers [31,32] and cannot be ignored. On the other hand, for the proposed protocol, it is evident that the attack launched by one dishonest participant is similar to that of an external attacker like Eve, which has been shown to be ineffective in the previous section. Therefore, in the following, we will focus on a more powerful internal attack, a collusion attack by two specific dishonest participants.

In this attack, two adjacent participants of an honest participant are dishonest, and they collaborate to steal the honest participant's secret information. Assume Bob_{i-1} and Bob_{i+1} are dishonest, denoted as Bob^*_{i-1} and Bob^*_{i+1}. They try to eavesdrop on Bob_i's private data set by performing the following attack action.

First, instead of applying the encoding operation on the signal state $|\phi^j_{i-1}\rangle$, Bob^*_{i-1} prepares two fake particles in $|\varphi_0\rangle = \sum_{k=0}^{d-1} |k\rangle|k\rangle$. Then, he replaces the signal particle with the first fake particle and sends it to Bob_i. In Step II.3, Bob_i applies his operation $S^d_{y^j_i} E^d_{x^j_i}$ to this fake particle and sends it to Bob^*_{i+1}. In this case, these two fake particles are in the state $|\varphi_0\rangle = \sum_{k=0}^{d-1} \omega^{k(x^j_i+y^j_i k)}|k\rangle|k\rangle$. Bob^*_{i-1} and Bob^*_{i+1} wish to exploit this state to obtain Bob_i's secret input x^j_i. y^j_i is known only to Bob_i and Trent, and has not been disclosed throughout the protocol. Thus, to obtain x^j_i, two dishonest participants must distinguish the following sets: $(\Omega_0, \Omega_1, \cdots, \Omega_{d-1})$, where $\Omega_u = \{\sum_{k=0}^{d-1} \omega^{ku}|k\rangle|k\rangle, \sum_{k=0}^{d-1} \omega^{k(u+k)}|k\rangle|k\rangle, \cdots, \sum_{k=0}^{d-1} \omega^{k(u+(d-1)k)}|k\rangle|k\rangle\}$. However, these states are non-orthogonal and cannot be distinguished by any projective measurement. Furthermore, these states are linearly dependent and cannot be deterministically distinguished [33]. This implies that their attack actions will inevitably introduce errors during the eavesdropping detection process. Therefore, the proposed protocol is secure against this attack.

5.3. Semi-Honest Third Party's Attack

In the protocol, Trent is semi-honest, which means that she cannot collude with other participants to engage in malicious activities. However, she may attempt to exploit her involvement in the protocol to eavesdrop on the secret information x^j_i of participant Bob_i. To achieve this, Trent can intercept the particles transmitted by Bob_{i-1} and forward a fake particle to Bob_i. Similarly to the external attacker Eve, Trent's attack fails to obtain Bob_i's secret input. Thus, the proposed protocol is resistant to attacks from a semi-honest third party.

As shown in the above analysis, the proposed protocol can defend against some common internal and external attacks, making it theoretically secure. Notably, despite using classical hash functions, the security of this protocol isn't compromised since their output isn't publicly disclosed. To obtain the hash value $h(x)$, the signal particles that contain $h(x)$ information should be attacked, which inevitably introduces errors and is detected by the participants. This means that even if advanced quantum algorithms could break the hash function, the lack of $h(x)$ prevents computing x. Thus, the protocol can use common classical hash functions, e.g., SHA-1 and MD5, and the master keys held by the participants can be reused. However, these analyses are idealized, and practical applications may face some physical attacks, such as side-channel [34,35], photon number splitting [36], and Trojan horse attacks [37]. Fortunately, technologies like quantum teleportation, measurement-device-independent, the decoy method, and wavelength quantum filters can counteract these threats [38–41]. In practical protocol applications, integrating these technologies can ensure their security.

6. Simulation Experiment

In this section, the feasibility of the multi-party QPSI protocol is verified through an example simulation. The experimental circuit was constructed based on the proposed protocol described in Section 3 and simulated on IBM quantum experience.

For convenience, the experimental data are taken from Tables 3 and 4. Two rounds of the protocol, based on the primes $d_1 = 2$ and $d_2 = 3$, were executed to obtain the private set intersection of four participants. Since external attacks and eavesdropping are considered independent processes in quantum protocol design, the quantum circuit in this simulation excludes identity authentication and eavesdropping detection. Therefore, the quantum simulation here focuses solely on implementing Phase II of the protocol. In the first round, the system is initialized as a quantum system with $\lceil \log d_1 \rceil = 1$ qubit. Based on this quantum system, the operations in the protocol can be simplified. Specifically, the Fourier transform corresponds to the Hadamard gate (H), the operations E_0 and S_0 correspond to the identity gate I, whereas E_1, S_1 and S_{-1} correspond to the Pauli-Z gate Z. According to Table 3, Trent prepares ten particles in the protocol, and each participant applies different operations to each particle. To maintain clarity, the circuit diagram depicting the evolution of the first particle is provided in Figure 2. The measurement results, including those of the first particle and the others, are given as '0101110100', as illustrated in Figure 3. Then, we can obtain Z = '0101110010' using $z^j = (o^j - X_0^j) \mod d_1$.

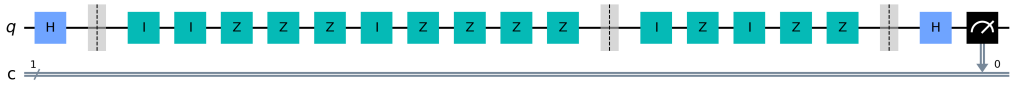

Figure 2. Quantum circuit for the first particle in Round 1 with $d_1 = 2$.

In the second round, the system is initialized as a quantum system consisting of $\lceil \log d_2 \rceil = 2$ qubits. According to the protocol, a three-dimensional Fourier transform

$$FT_3 = \frac{1}{\sqrt{3}} \begin{bmatrix} 1 & 1 & 1 \\ 1 & \omega & \omega^2 \\ 1 & \omega^2 & \omega \end{bmatrix}, \tag{18}$$

is required to prepare the initial state, where $\omega = e^{2\pi \mathrm{i}/3}$. Since Qiskit supports quantum gates only in dimensions that are powers of two, the transform matrix FT_3 is embedded into a four-dimensional space, denoted as matrix $QFT = \begin{bmatrix} FT_3 & 0 \\ 0 & 1 \end{bmatrix}$. The corresponding circuit implementation is shown in Figure 4a. Furthermore, the circuits for the operations E_1, S_1,

and S_{-1} are shown in Figures 4b, 4c, and 4d, respectively. Figure 4e illustrates the circuit for the operations performed on the first particle. The measurement outcomes of this particle and the others are '2102200212', as displayed in Figure 5. Based on these measurement results, the value Z = '1121102212' can be obtained by calculating $z^j = (o^j - X_0^j) \mod d_2$.

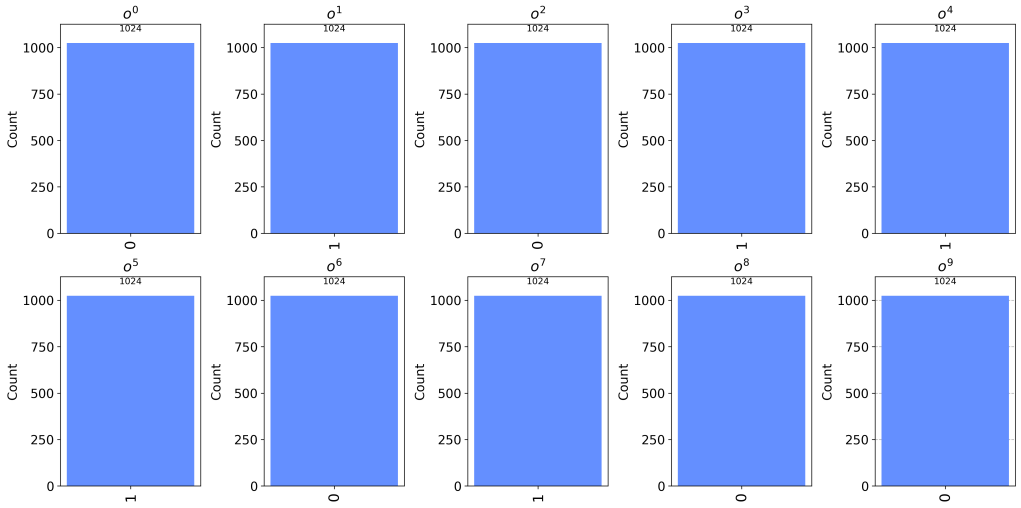

Figure 3. The measurement outcome in Round 1 with $d_1 = 2$.

In summary of the above simulation results, the results are consistent with the theoretical descriptions in Tables 3 and 4. This confirms the feasibility of the proposed protocol through a concrete example.

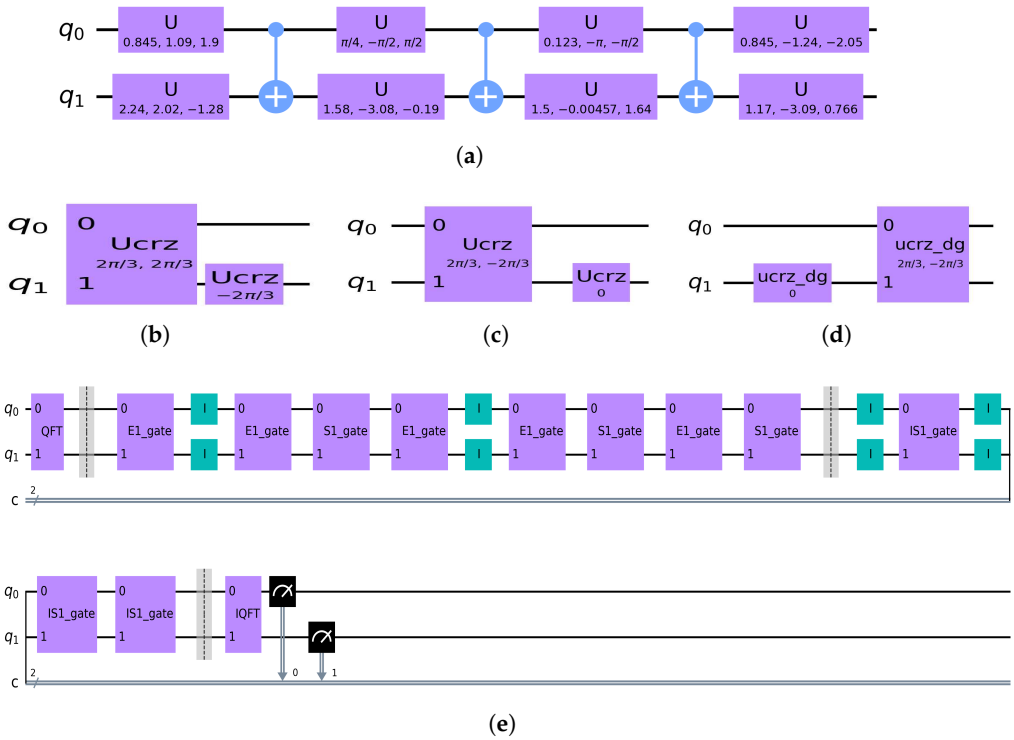

Figure 4. Quantum circuit designs for Round 2 with $d_2 = 3$. (**a**) The quantum circuit for operation QFT. (**b**) The circuit of the operation E_1. (**c**) The construction of S_1. (**d**) The circuit of the operation S_{-1}, which is labeled as $IS1$. (**e**) Quantum circuit for the first particle in Round 2 with $d_2 = 3$.

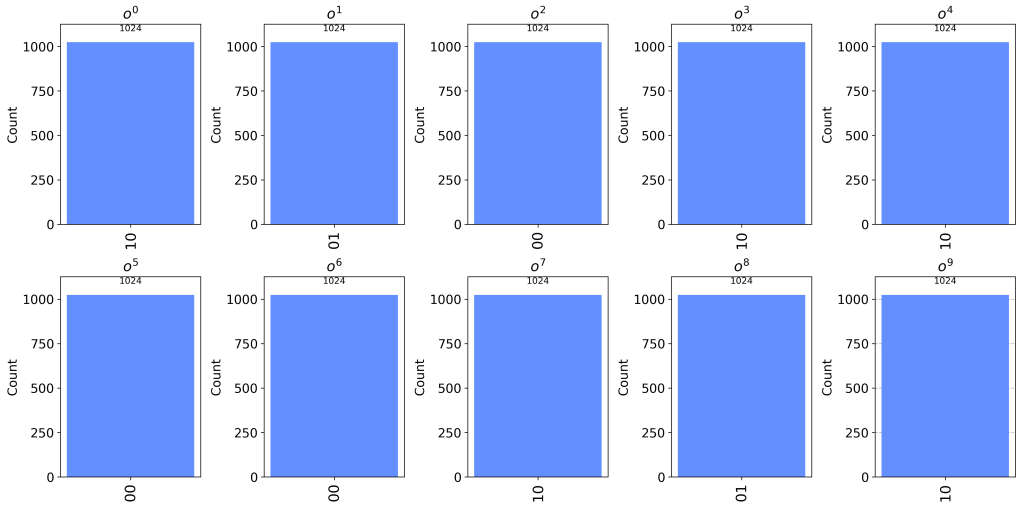

Figure 5. The measurement outcome in Round 2 with $d_2 = 3$.

7. Discussion and Summary

Before drawing a conclusion, it is worthwhile to discuss the performance of the proposed protocol. To better demonstrate the performance of our proposed protocol, we compare it with two existing state-of-the-art QPSI protocols, the HZZ protocol [21] and the WSW protocol [24]. The comparison presented in Table 5 is based on various factors, including communication complexity, quantum resources, quantum operations, etc.

Communication cost is an important indicator when analyzing the efficiency of QPSI protocols. As shown in Figure 1, the protocol involves the transmission of n qudits between Trent and m participants. Additionally, from Table 1, it is deduced that $2mn$ classical bits are required. In total, the communication overhead includes $(m+1)n(\log_2 d)$ qubits and $2mn$ classical bits. Given that $d = m+1$, the overall communication complexity of the proposed protocol is $O(nm \log_2 m)$. Additionally, in the proposed protocol, there are ξ particles used as the test samples. Here, the security parameter ξ is determined by various factors, such as the amount of information, channel noise, and security level. To better compare the eavesdropping detection efficiency of different protocols, we can assume that each detection uses ξ test samples. In addition to these ξ qudits, each participant needs to transmit ξ classical bits to Trent during the eavesdropping detection phase. Thus, the communication cost for the entire eavesdropping detection process is $O(\xi(\log_2 m + m))$. In the HZZ protocol, the TP is required to share m rotation angle information with each participant, and it requires the transmission of λ copies of particle sequences to ensure the correctness of the protocol. Therefore, its communication complexity is $O(\lambda m^2 n)$. In addition, the HZZ protocol does not provide identity authentication, exposing it to impersonation risks. In the WSW protocol, which only considers the case of two parties, n three-particle GHZ states are prepared by the TP who sends each participant n particles. Thus, its quantum communication complexity is $2n$. In order to calculate the result, two participants are required to send the $2n$ classical bits message to the TP, which means that its classical communication complexity is $4n$. Therefore, the overall communication complexity of the WSW protocol is $6n$. Furthermore, to ensure the security of the transmitted particles, both the HZZ protocol and the WSW protocol require the insertion of decoy states in the quantum communication, which mandates quantum storage capabilities for all participants. In the proposed protocol, its implementation does not require quantum memory, and only single particles are employed, which makes it more feasible with current technology.

Table 5. Comparison of the proposed protocol with existing QPSI protocols.

Protocols	WSW Protocol	HZZ Protocol	Our Protocol
Application scenario	Two-party	Multi-party	Multi-party
Communication complexity	$O(6n)$	$O(\lambda m^2 n)$	$O(mn\log_2 m)$
Cost of eavesdropping detection	$O(6\xi)$	$O(3\xi m)$	$O(\xi(\log_2 m + m))$
Quantum resource	GHZ states	Single particles	Single particles
Quantum operation	H operation	Rotation operation	Phase operation
Identity authentication	Yes	No	Yes
Deterministic or probabilistic	Deterministic	Probabilistic	Deterministic
Quantum storage	Yes	Yes	No

m = number of parties, n = cardinality of the data set.

In summary, we propose a multi-party QPSI protocol with identity authentication, by which multiple participants can concurrently obtain the intersection of their private data sets with the help of a semi-honest third party. In the protocol, the TP shares a master key with each participant beforehand, which is used to authenticate their identity. The single particles randomly located in one of the MUB states are prepared by the TP and transmitted among these participants, who respectively encode their private inputs into them. The security of the proposed protocol against some common attacks has been analyzed, which shows that it is secure in the zero-error case. In the protocol, eavesdropping detection and identity authentication are ingeniously integrated, thereby enhancing the protocol's practical detection efficiency. Moreover, since no explicit identity authentication information is disclosed, the master key can be reused, which improves the applicability of the protocol. Additionally, there is no need for participants to store the traveling particles in the proposed protocol. Thus, the implementation of this protocol does not require quantum memory, which is still difficult to achieve directly at present. Furthermore, the use of only single particles in the proposed protocol makes it more feasible with current technology. Certainly, there are other practical issues during the application of the protocol. For instance, each particle transmission among the participants inevitably incurs optical loss and phase shift. Thus, how to design an effective error recovery strategy in real-world settings will be a focal point of our future work.

Author Contributions: Conceptualization, G.-D.G.; methodology, G.-D.G. and L.-Q.Z.; software, K.Y.; validation, K.Y. and S.L.; formal analysis, G.-D.G.; investigation, S.L.; resources, K.Y.; data curation, S.L.; writing—original draft preparation, G.-D.G. and L.-Q.Z.; writing—review and editing, S.L.; visualization, K.Y.; supervision, K.Y.; project administration, S.L.; funding acquisition, S.L. 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 (Grant No. 62171131), Fujian Province Natural Science Foundation (Grant Nos. 2022J01186 and 2023J01533), and the Innovation Program for Quantum Science and Technology (Grant No. 2021ZD0302901).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding authors.

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

References

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public-key distribution and coin tossing. In Proceedings of the IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India, 10–12 December 1984; IEEE Computer Society Press: Piscataway, NJ, USA, 1984; pp. 175–179.
2. Cleve, R.; Gottesman, D.; Lo, H.K. How to share a quantum secret. *Phys. Rev. Lett.* **1999**, *83*, 648. [CrossRef]
3. Hillery, M.; Bužek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829. [CrossRef]
4. Lin, S.; Guo, G.; Xu, Y.; Sun, Y.; Liu, X. Cryptanalysis of quantum secret sharing with d-level single particles. *Phys. Rev. A* **2016**, *93*, 062343. [CrossRef]
5. Andronikos, T. A distributed and parallel (k, n) QSS scheme with verification capability. *Mathematics* **2024**, *12*, 3782. [CrossRef]
6. Boström, K.; Felbinger, T. Deterministic secure direct communication using entanglement. *Phys. Rev. Lett.* **2002**, *89*, 187902. [CrossRef]
7. Deng, F.G.; Long, G.L.; Liu, X.S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A* **2003**, *68*, 042317. [CrossRef]
8. Lin, S.; Wen, Q.; Gao, F.; Zhu, F. Quantum secure direct communication with χ-type entangled state. *Phys. Rev. A* **2008**, *78*, 064304. [CrossRef]
9. Sheng, Y.B.; Zhou, L.; Long, G.L. One-step quantum secure direct communication. *Sci. Bull.* **2022**, *67*, 367–374. [CrossRef]
10. Yang, Y.G.; Wen, Q.Y. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. *J. Phys. A Math. Theor.* **2009**, *42*, 055305. [CrossRef]
11. Lin, S.; Sun, Y.; Liu, X.; Yao, Z. Quantum private comparison protocol with d-dimensional Bell states. *Quantum Inf. Process.* **2013**, *12*, 559–568. [CrossRef]
12. Chen, X.B.; Su, Y.; Niu, X.X. Efficient and feasible quantum private comparison of equality against the collective amplitude damping noise. *Quantum Inf. Process.* **2014**, *13*, 101–112. [CrossRef]
13. Liu, B.; Xiao, D.; Huang, W. Quantum private comparison employing single-photon interference. *Quantum Inf. Process.* **2017**, *16*, 180. [CrossRef]
14. Hou, M.; Wu, Y. Two-party quantum private comparison protocol for direct secret comparison. *Mathematics* **2025**, *13*, 326. [CrossRef]
15. Shi, R.H.; Mu, Y.; Zhong, H.; Cui, J.; Zhang, S. An efficient quantum scheme for private set intersection. *Quantum Inf. Process.* **2016**, *15*, 363–371. [CrossRef]
16. Debnath, S.K.; Dey, K.; Kundu, N.; Choudhury, T. Feasible private set intersection in quantum domain. *Quantum Inf. Process.* **2021**, *20*, 41. [CrossRef]
17. Chen, Y.M.; Situ, H.; Huang, Q.; Zhang, C. A novel quantum private set intersection scheme with a semi-honest third party. *Quantum Inf. Process.* **2023**, *22*, 429. [CrossRef]
18. Mohanty, T.; Debnath, S.K. An information-theoretically secure quantum multiparty private set intersection. *J. Inf. Secur. Appl.* **2023**, *78*, 103623. [CrossRef]
19. Maitra, A. Quantum secure two-party computation for set intersection with rational players. *Quantum Inf. Process.* **2018**, *17*, 197. [CrossRef]
20. Liu, W.J.; Li, W.B.; Wang, H.B. An improved quantum private set intersection protocol based on Hadamard gates. *Int. J. Theor. Phys.* **2022**, *61*, 53. [CrossRef]
21. Huang, X.; Zhang, W.F.; Zhang, S.B. Quantum multi-party private set intersection using single photons. *Physica A* **2024**, *649*, 129974. [CrossRef]
22. Wang, Y.; Hu, P.; Xu, Q. Quantum protocols for private set intersection cardinality and union cardinality based on entanglement swapping. *Int. J. Theor. Phys.* **2021**, *60*, 3514–3528. [CrossRef]
23. Sarkar, S.; Mohanty, T.; Srivastava, V.; Debnath, S.K.; Das, A.K.; ParkQuantum, Y. Quantum secure disease surveillance through private set intersection. *IEEE Trans. Consum. Electr.* **2024**, *70*, 5585–5596. [CrossRef]
24. Wu, S.Y.; Sun, W.Q.; Wang, Y.; Liu, J.; Wang, Q. A secure quantum private set computation protocol with identity authentication utilizing GHZ states. *Int. J. Theor. Phys.* **2024**, *63*, 135. [CrossRef]
25. Sandor, I. Quantum communications: Explained for communication engineers. *IEEE Trans. Commun. Mag.* **2013**, *51*, 28–35.
26. Yang, Y.G.; Xia, J.; Jia, X.; Zhang, H. Comment on quantum private comparison protocols with a semi-honest third party. *Quantum Inf. Process.* **2013**, *12*, 877–885. [CrossRef]
27. Lo, H.K.; Chau, H.F. Is quantum bit commitment really possible? *Phys. Rev. Lett.* **1997**, *78*, 3410. [CrossRef]
28. Mayers, D. Unconditionally secure quantum bit commitment is impossible. *Phys. Rev. Lett.* **1997**, *78*, 3414. [CrossRef]
29. Wootters, W.K.; Fields, B.D. Optimal state-determination by mutually unbiased measurements. *Ann. Phys.* **1989**, *191*, 363–381. [CrossRef]
30. Lin, S.; Guo, G.; Huang, F.; Liu, X. Quantum anonymous ranking based on the Chinese remainder theorem. *Phys. Rev. A* **2016**, *93*, 012318. [CrossRef]

31. Gao, F.; Qin, S.J.; Wen, Q.Y.; Zhu, F.C. A simple participant attack on the brádler-dušek protocol. *Quantum Inf. Comput.* **2007**, *7*, 329–334. [CrossRef]
32. Lin, S.; Gao, F.; Guo, F.Z.; Wen, Q.Y.; Zhu, F.C. Comment on "Multiparty quantum secret sharing of classical messages based on entanglement swapping". *Phys. Rev. A* **2007**, *76*, 036301. [CrossRef]
33. Zhang, S.Y.; Ying, M.S. Set discrimination of quantum states. *Phys. Rev. A* **2002**, *65*, 062322. [CrossRef]
34. Qi, B.; Lo, H.K.; Chen, C.; Zhao, Y.; Fung, C.-H.F. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **2007**, *75*, 052332.
35. Bozzio, M.; Cavaillès, A.; Diamanti, E.; Kent, A.; Pitalúa-García, D. Multiphoton and side-channel attacks in mistrustful quantum cryptography. *Phys. Rev. X Quantum* **2021**, *2*, 030338. [CrossRef]
36. Brassard, G.; Lutkenhaus, N.; Mor, T.; Sanders, B.C. Limitations on practical quantum cryptography. *Phys. Rev. Lett.* **2000**, *85*, 1330. [CrossRef]
37. Gisin, N.; Fasel, S.; Kraus, B.; Zbinden, H.; Ribordy, G. Trojan horse attacks on quantum key distribution systems. *Phys. Rev. A* **2006**, *73*, 022320. [CrossRef]
38. Wang, X.B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
39. Deng, F.G.; Li, X.H.; Zhou, H.Y.; Zhang, Z.J. Improving the security of multiparty quantum secret sharing against Trojan horse attack. *Phys. Rev. A* **2005**, *72*, 044302. [CrossRef]
40. Zhang, Q.; Xu, F.; Chen, Y.A.; Peng, C.Z.; Pan, J.W. Large scale quantum key distribution: Challenges and solutions. *Opt. Express* **2018**, *26*, 24260. [CrossRef]
41. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]