axioms

IMPACT FACTOR 1.9

Article

# Quantum Private Set Intersection Scheme Based on Bell States

Min Hou, Yue Wu and Shibin Zhang

Special Issue
Recent Advances in Quantum Mechanics and Mathematical Physics

Edited by
Prof. Dr. Espen Gaarder Haug

MDPI

https://doi.org/10.3390/axioms14020120

*axioms*

MDPI

*Article*

# Quantum Private Set Intersection Scheme Based on Bell States

**Min Hou [1,2,3], Yue Wu [1] and Shibin Zhang [4,5,*]**

[1] School of Computer Science, Sichuan University Jinjiang College, Meishan 620860, China; houmin@scujj.edu.cn (M.H.); ywu@uestc.edu.cn (Y.W.)
[2] Network and Data Security Key Laboratory of Sichuan Province, University of Electronic Science and Technology of China, Chengdu 610054, China
[3] State Key Laboratory of Cognitive Intelligence, Hefei 230088, China
[4] College of Artificial Intelligence (CUIT Shuangliu Industrial College), Chengdu University of Information Technology, Chengdu 610225, China
[5] Advanced Cryptography and System Security Key Laboratory of Sichuan Province, Chengdu 610225, China
* Correspondence: cuitzsb@cuit.edu.cn

**Abstract:** In this paper, we introduce a quantum private set intersection (QPSI) scheme that leverages Bell states as quantum information carriers. Our approach involves encoding private sets into Bell states using unitary operations, enabling the computation of the intersection between two private sets from different users while keeping their individual sets undisclosed to anyone except for the intersection result. In our scheme, a semi-honest third party (TP) distributes the first and second qubits of the Bell states to the two users. Each user encodes their private sets by applying unitary operations on the received qubits according to predefined encoding rules. The modified sequence is encrypted and then sent back to TP, who can compute the set intersection without learning any information about the users' private inputs. The simulation outcomes on the IBM quantum platform substantiate the viability of our scheme. We analyze the security and privacy aspects of the sets, showing that both external attacks and internal threats do not compromise the security of the private inputs. Furthermore, our scheme exhibits better practicality by utilizing easily implementable Bell states and unitary operations, rather than relying on multiple encoded states for set intersection calculations.

**Keywords:** quantum private set intersection (QPSI); Bell states; unitary operation; semi-honest third party; quantum secure multiparty computation

**MSC:** 81P94; 81P65



Academic Editor: Espen Gaarder Haug

Received: 8 January 2025
Revised: 25 January 2025
Accepted: 4 February 2025
Published: 7 February 2025

**Citation:** Hou, M.; Wu, Y.; Zhang, S. Quantum Private Set Intersection Scheme Based on Bell States. *Axioms* **2025**, *14*, 120. https://doi.org/10.3390/axioms14020120



## 1. Introduction

Secure Multiparty Computation (MPC) allows multiple participants to collaboratively compute specific outputs while preserving the confidentiality of their original inputs. First proposed by Yao in 1982 to address the millionaire's problem [1], MPC has undergone significant development, with numerous researchers contributing to a variety of solutions that enhance its diverse functionalities. MPC encompasses several branches tailored to specific applications, including secret sharing [2–4], private query [5–7], and private comparison [8–15].

Among these branches, private set intersection (PSI) plays a critical role by allowing multiple parties to compute the intersection of their private sets without revealing any additional information [16]. The increasing interest in PSI is driven by its practical applications in fields such as privacy-preserving contact tracing [17], vertical federated learning [18], privacy-preserving condition queries [19], and privacy-preserving authorization [20].

PSI schemes primarily depend on classical cryptographic techniques, including confused circuits [21], oblivious transfer [22], and homomorphic encryption [23]. The security of these schemes often rests on unproven mathematical assumptions, rendering them increasingly at risk from quantum threats. The Shor algorithm [24] poses a significant challenge by efficiently factoring large integers, thereby compromising widely used RSA encryption, while the Grover algorithm [25] threatens symmetric-key cryptography through its capacity for function inversion. Therefore, there is an urgent imperative for research dedicated to developing PSI schemes that provide resilience against quantum attacks and achieve quantum-proof security.

In light of the vulnerabilities inherent in classical cryptographic schemes, quantum private set intersection (QPSI) has emerged as a promising alternative. Although research on QPSI remains limited, it offers distinct advantages over classical methods by leveraging principles of quantum mechanics, such as the quantum non-cloning theorem [26]. This foundational aspect enables QPSI to attain quantum-proof security, making it an increasingly compelling area of investigation. Consequently, researchers are intensifying their efforts to develop quantum schemes for PSI, aiming to bolster security against the potential threats posed by quantum computing.

The first QPSI scheme [27] was proposed by Shi in 2016, where $n$ encoded states and quantum operator $G$, and von Neumann measurements to achieve the calculation of set intersection. Cheng et al. [28] highlighted a significant fairness issue in the protocol outlined in Ref. [27], where the server possessed the ability to unilaterally manipulate the outcomes experienced by the client. To counteract this vulnerability, Cheng et al. [28] proposed an improved scheme that introduces a passive third party (TP) to monitor and detect any dishonest behavior by the server. While these schemes are theoretically feasible, they necessitate the preparation of "multi-particle entangled states" as carriers of quantum information, along with the implementation of intricate quantum oracle operators. Achieving these requirements poses significant challenges with current quantum technologies. To improve the scheme's feasibility, Liu et al. [29] proposed a PSI scheme that utilizes the quantum Fourier transform (QFT) and OAM basis measurement, incorporating a semi-honest third party in the process. However, Liu et al. [30] pointed out that there remained vulnerabilities that could lead to the compromise of participants' privacy after the entire operation was concluded, and proposed an improved scheme based on the Hadamard gate. Nevertheless, this enhancement requires fractional times of the Hadamard gate, which remains challenging to implement with current quantum technology.

Although the aforementioned QPSI schemes employ quantum methods to address the challenges of private set intersection, they encounter significant practical difficulties due to the reliance on complex quantum resources and operations. To tackle this issue, we propose a QPSI scheme that utilizes Bell states, unitary operations, and Bell-basis measurement as fundamental components for determining the set intersection without disclosing the private sets, thereby enhancing its practicality. Simulation results conducted on the IBM quantum platform demonstrate the feasibility of our scheme. The privacy of the private sets is effectively safeguarded, even against attempts by external eavesdroppers and participants to execute various attacks aimed at compromising the private data.

The remainder of the paper is organized as follows: Section 2 introduces the unitary operations and Bell states used, while Section 3 provides a detailed description of the proposed scheme. Section 4 presents the simulation conducted, and Sections 5 and 6 discuss security and comparisons, respectively. Finally, Section 7 concludes the paper.

## 2. Preliminaries

In quantum communication, the bit flip and phase shift operators are fundamental concepts that manipulate quantum bits (qubits) and play crucial roles in information encoding, error correction, and quantum operations. The bit flip and phase shift operators [31] can be given by

$$X = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, Z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \tag{1}$$

The bit flip operator is a quantum gate that changes a qubit from $|0\rangle$ to $|1\rangle$ (or vice versa) and the phase shift operator flips the phase of the $|1\rangle$ state while leaving the $|0\rangle$ state unchanged.

Applying the above two operators to an orthonormal basis $\{|0\rangle, |1\rangle\}$, we obtain

$$\begin{cases} X|0\rangle = |1\rangle, X|1\rangle = |0\rangle \\ Z|0\rangle = |0\rangle, Z|1\rangle = -|1\rangle \end{cases} \tag{2}$$

The rotational encryption operator [32] can be written as

$$R_y(\theta) = \begin{pmatrix} \cos\frac{\theta}{2} & -\sin\frac{\theta}{2} \\ \sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix} \tag{3}$$

where $\theta$ serves as the encryption key. When we use the rotational encryption operator $R_y(\theta)$ to encrypt the quantum states, we only need to apply the operation $R_y(-\theta)$ on the encrypted quantum states to recover the original quantum states.

Four Bell states [33] can be written as

$$|\varphi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \tag{4}$$

$$|\varphi_{01}\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \tag{5}$$

$$|\varphi_{10}\rangle = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \tag{6}$$

$$|\varphi_{11}\rangle = \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \tag{7}$$

To simplify the expression of Equations (4)–(7), four Bell states can be given by

$$|\varphi_{ab}\rangle = \sum_{i=0}^{1} |i + a\rangle|i\rangle, a, b \in \{0, 1\} \tag{8}$$

According to Equation (8), we can obtain $|\varphi_{00}\rangle = \sum_{i=0}^{1} |i\rangle|i\rangle$ and $|\varphi_{ab}\rangle = X(a)Z(b)|\varphi_{00}\rangle$.

Consider a scenario involving three participants: Charlie, Tom, and John. Tom holds an input $a \in F_2$, while John holds an input $b \in F_2$. The objective is for Charlie to learn the product $ab$ without acquiring any information about the individual inputs $a$ and $b$.

Assume that Charlie prepares a Bell state $|\varphi_{00}\rangle$, and distributes the first qubit to Tom and second qubit to John. If $a = 0$, Tom applies the phase shift operator $Z$ (which adds a phase of $\pi$ to the $|1\rangle$ state) to her qubit. If $a = 1$, Tom applies the bit flip operator X to her qubit. If $b = 0$, John applies the phase shift operator Z to his qubit. If $b = 1$, John applies the bit flip operator $X$ to his qubit. After Tom and John perform their respective operations, they return their individual qubits to Charlie, who then performs a Bell basis measurement on the combined state of the two qubits. The outcomes of the Bell basis measurement are $|\varphi_{00}\rangle$ and $|\varphi_{11}\rangle$, respectively. In this situation, Charlie knows $a$ and $b$

due to the measurement result $|\varphi_{ab}\rangle$ is produced by performing the operators X and Z corresponding to $a = 1$ and $b = 1$ on the first and second qubit.

To keep the inputs undisclosed, Tom and John randomly select three different encodings [34] to encode $a = 1$ and $b = 1$ to the same quantum state $|\varphi_{11}\rangle$. Note that in each row, the same operator is consistently applied to the first qubit, regardless of the column index. Likewise, in each column, the same operator is applied to the second qubit. Three different encodings can be seen in Table 1. When these encodings are applied to $|\varphi_{00}\rangle$, the resultant states are shown in Table 2. It can be observed that if and only if $a = 1$ and $b = 1$, Charlie receives the state $|\varphi_{11}\rangle$; otherwise, Charlie receives one of the other three Bell states. Thus, the specific encodings ensure that Charlie reveals nothing about their inputs. This mechanism is fundamental for designing the subsequent QPSI scheme.

**Table 1.** Three different encodings.

| | $b=0$ | $b=1$ | | $b=0$ | $b=1$ | | $b=0$ | $b=1$ |
|---|---|---|---|---|---|---|---|---|
| $a=0$ | $I\otimes I$ | $I\otimes Z$ | $a=0$ | $I\otimes Z$ | $I\otimes X$ | $a=0$ | $X\otimes I$ | $X\otimes X$ |
| $a=1$ | $X\otimes I$ | $X\otimes Z$ | $a=1$ | $Z\otimes Z$ | $Z\otimes X$ | $a=1$ | $Z\otimes I$ | $Z\otimes X$ |
| | (1) | | | (2) | | | (3) | |

**Table 2.** The resultant states.

| | $b=0$ | $b=1$ | | $b=0$ | $b=1$ | | $b=0$ | $b=1$ |
|---|---|---|---|---|---|---|---|---|
| $a=0$ | $\|\varphi_{00}\rangle$ | $\|\varphi_{01}\rangle$ | $a=0$ | $\|\varphi_{01}\rangle$ | $\|\varphi_{10}\rangle$ | $a=0$ | $\|\varphi_{10}\rangle$ | $\|\varphi_{00}\rangle$ |
| $a=1$ | $\|\varphi_{10}\rangle$ | $\|\varphi_{11}\rangle$ | $a=1$ | $\|\varphi_{00}\rangle$ | $\|\varphi_{11}\rangle$ | $a=1$ | $\|\varphi_{01}\rangle$ | $\|\varphi_{11}\rangle$ |
| | (1) | | | (2) | | | (3) | |

## 3. The Proposed QPSI Scheme

This scheme involves three entities: The semi-honest third party (TP), Alice, and Bob.

*Semi-honest TP*: This entity possesses quantum capabilities, including preparing quantum states and performing quantum measurements. In the scheme, TP strictly follows the outlined steps and assists Alice and Bob in obtaining their set intersection. However, it cannot collude with or favor either Alice or Bob.

*Alice*: She holds her private set $A$ and wishes to know the intersection of $A$ with Bob's private set $B$.

*Bob*: He possesses his private set $B$ and seeks to determine the intersection of his set $B$ with Alice's private set $A$.

The proposed scheme must satisfy the following requirements:

Correctness: If Alice and Bob provide their respective sets $A$ and $B$ honestly, the semi-honest TP will announce the correct set intersection.

Security: Outside attackers cannot access the private sets of Alice and Bob. Additionally, the semi-honest TP and any dishonest participant cannot obtain any information about the honest participant's private set, except for the set intersection.

Thus, the goal of the proposed QPSI scheme is for Alice and Bob to learn the intersection (which may be empty) of their respective sets with the assistance of a semi-honest TP, without disclosing their individual private sets.

We assume a universal set denoted as $U = \{0, 1, 2, \cdots, n-1\}$, where the sets of Alice and Bob belong to this universal set, such that $A \subset U$ and $B \subset U$. According to

the encoding rules outlined in Equation (9), Alice and Bob generate $n$-bit strings $S_A$ and $S_B$, respectively.

$$S_A^j = \begin{cases} 1, j \in A \\ 0, j \notin A \end{cases}, S_B^j = \begin{cases} 1, j \in B \\ 0, j \notin B \end{cases} \text{ for } j \in \{0, 1, 2, \cdots, n-1\} \tag{9}$$

Additionally, we assume that the protocol operates over a noise-free and lossless quantum channel. in practical scenarios, noise and errors can be effectively immune by the application of quantum error correction [35–39] and decoherence-free subspaces [40–43].

Before the scheme begins, we suppose that Alice and Bob share a secret key $K_{AB} = \left\{k_{AB}^0, k_{AB}^1, \cdots, k_{AB}^{n-1}\right\}$ via a QKD protocol [44], where $k_{AB}^j \in \{00, 01, 10, 11\}$ for $j \in \{0, 1, 2, \cdots, n-1\}$.

The steps of the scheme are as follows, and its diagram is depicted in Figure 1.

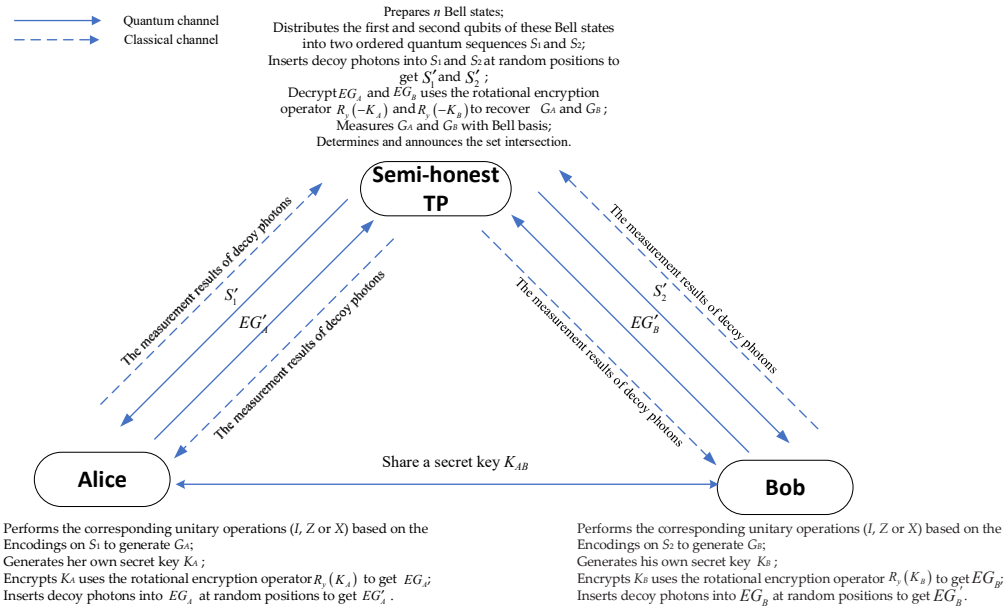


**Figure 1.** The diagram of the proposed QPSI scheme.

**Step 1**. TP prepares $n$ Bell states all in the form of $|\varphi_{00}\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ that are entangled pairs of two qubits, and distributes the first and second qubits of these Bell states into two ordered quantum sequences $S_1$ and $S_2$, respectively. After this, TP prepares two decoy-photon sequences $D_A$ and $D_B$, where each decoy-photon sequence contains $d$ decoy particles randomly chosen from $\left\{|0\rangle, |1\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$, and inserts $D_A$ into $S_1$ and $D_B$ into $S_2$ at random positions, and records these inserted positions. The new generated sequences are denoted as $S_1'$ and $S_2'$. Eventually, TP sends $S_1'$ to Alice and $S_2'$ to Bob, respectively. It is important to note that the use of decoy photons helps detect eavesdropping, as any interception would alter the statistics of the received photons.

**Step 2**. After receiving $S_1'$ ($S_2'$), Alice (Bob) consults with TP aiming at performing the eavesdropping detection. TP tells Alice (Bob) the positions and measurement bases of each decoy photon in $D_A$ ($D_B$) via a classical channel. Alice (Bob) performs the corresponding quantum measurements on $D_A$ ($D_B$) and returns the measurement outcome to TP who then compares these results of $D_A$ ($D_B$) with the initially prepared decoy particles in $D_A$ ($D_B$) and calculate the error rate. TP instructs Alice (Bob) to restart the protocol if the error rate exceeds the predetermined threshold. Otherwise, the scheme proceeds to the next step. This step highlights the interplay of quantum communication, where classical channels are

used for the verification process, while quantum channels are used for the transmission of qubits.

**Step 3**. Alice (Bob) discards all decoy particles in $S_1'$ ($S_2'$) to recover $S_1$ ($S_2$). After this, Alice (Bob) performs the operations as follows.

For Alice:

(1) She selects the encoding rule from Table 1 based on the secret key $K_{AB}$ to encode her own set elements in $S_A$.

- If $k_{AB}^j \in \{00, 11\}$, she chooses the first encoding.
- If $k_{AB}^j \in 01$, she chooses the second encoding.
- If $k_{AB}^j \in 10$, she chooses the third encoding.

(2) She performs the corresponding unitary operations ($I$, $Z$ or $X$) based on the encodings on $S_1$ to generate a new sequence $G_A$.

(3) She generates her own secret key $K_A = \left\{\theta_A^0, \theta_A^1, \theta_A^2, \cdots, \theta_A^{n-1}\right\}$, where $\theta_A^j \in [0, 2\pi)$ for $j \in \{0, 1, 2, \cdots, n-1\}$.

(4) She uses the rotational encryption operator $R_y(K_A)$ to encrypt $G_A$ to obtain a new sequence $EG_A$.

(5) She prepares $d$ decoy particles randomly chosen from $\left\{|0\rangle, |1\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$.

(6) She inserts these decoy photons into $EG_A$ to obtain a new sequence $EG_A'$.

(7) She records the inserted positions of the decoy particles.

(8) She sends $EG_A'$ to TP.

For Bob:

(1) He selects the encoding rule from Table 1 based on the secret key $K_{AB}$ to encode his own set elements in $S_B$.

- If $k_{AB}^j \in \{00,\ 11\}$, he chooses the first encoding.
- If $k_{AB}^j \in 01$, he chooses the second encoding.
- If $k_{AB}^j \in 10$, he chooses the third encoding.

(2) He performs the corresponding unitary operations ($I$, $Z$ or $X$) based on the encodings on $S_2$ to generate a new sequence $G_B$.

(3) He generates her own secret key $K_B = \left\{\theta_B^0, \theta_B^1, \theta_B^2, \cdots, \theta_B^{n-1}\right\}$, where $\theta_B^j \in [0, 2\pi)$ for $j \in \{0, 1, 2, \cdots, n-1\}$.

(4) He uses the rotational encryption operator $R_y(K_B)$ to encrypt $G_B$ to obtain a new sequence $EG_B$.

(5) He prepares $d$ decoy particles randomly chosen from $\left\{|0\rangle, |1\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}}\right\}$.

(6) He inserts these decoy photons into $EG_B$ to obtain a new sequence $EG_B'$.

(7) He records the inserted positions of the decoy particles.

(8) He sends $EG_B'$ to TP.

**Step 4.** When TP has received $EG_A'$ ($EG_B'$) from Alice (Bob), TP consults with Alice (Bob) to perform the eavesdropping detection in the same way as discussed above. If no eavesdropper exists in this communication, TP instructs Alice (Bob) to restart the protocol. Otherwise, Alice (Bob) tells the secret key $K_A$ ($K_B$) to TP and the scheme proceeds the next steps for calculating the set intersection. This step is crucial for validating that the communication between Alice (Bob) and TP has not been compromised.

**Step 5.** TP discards all decoy particles in $EG_A'$ ($EG_B'$) to recover $EG_A$ ($EG_B$). Then, TP performs the following operations:

(1) TP uses the rotational encryption operator $R_y(-K_A)$ to decrypt $EG_A$ and $R_y(-K_B)$ to decrypt $EG_B$, thereby recovering the original sequence $G_A$ and $G_B$.
(2) TP performs Bell measurements on $G_A$ and $G_B$ to obain $n$ Bell states. If the $j$-th Bell states is $|\varphi_{11}\rangle$, then the set intersection includes $j$. If none of the Bell states are $|\varphi_{11}\rangle$, the set intersection is empty.
(3) TP announces the set intersection to Alice and Bob.

## 4. Simulation

We consider the case that Alice holds her private set $A = \{1, 2\}$ and Bob possesses his private set $B = \{0, 1, 2\}$. Alice and Bob desire to know the intersection of $A$ and $B$.

According to the encoding rules outlined in Equation (9), Alice and Bob generate 6-bit strings $S_A = (011)$ and $S_B = (111)$, respectively. We suppose that Alice and Bob share a secret key $K_{AB} = (011011)$ via a QKD protocol in advance. According to the encoding rule from Table 1 based on the secret key $K_{AB}$, we can know that the corresponding unitary operations ($I$, $Z$ or $X$) performed on $S_1$ and $S_2$ are $\{I, Z, X\}$ and $\{X, X, Z\}$, respectively. We assume that Alice's secret key $K_A = (\frac{2\pi}{3}, \frac{\pi}{2}, \frac{5\pi}{6})$ and Bob's secret key $K_B = (\frac{\pi}{3}, \frac{5\pi}{6}, \frac{9\pi}{7})$. The Bell measurement can be implemented by applying the CNOT gate and Hadamard gate on the quantum states. The measurement results 00,01,10 and 11 correspond to four Bell states $|\varphi_{00}\rangle, |\varphi_{01}\rangle, |\varphi_{10}\rangle$ and $|\varphi_{11}\rangle$.

We simulate the proposed scheme on the IBM quantum platform, focusing solely on the quantum operations without incorporating eavesdropping detection. The quantum circuit implementation for determining the intersection of $A$ and $B$ is shown in Figure 2, and the measurement results are presented in Figure 3.

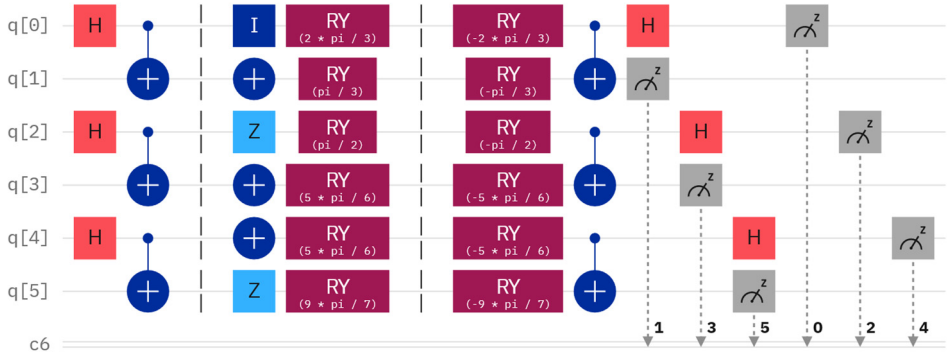


**Figure 2.** The quantum circuit implementation for determining the intersection of $A$ and $B$.

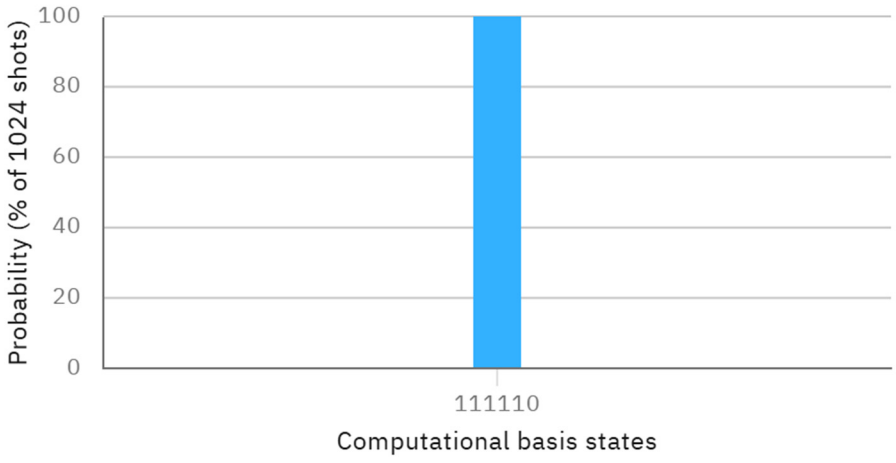


**Figure 3.** The measurement results.

Based on the measurement result depicted in Figure 3, the final results are 10, 11 and 11 from right to left. According to the rules of Bell measurement, these results correspond to $|\varphi_{10}\rangle$, $|\varphi_{11}\rangle$ and $|\varphi_{11}\rangle$. Thus, we can know that the first and second Bell states are $|\varphi_{11}\rangle$, and then the set intersection is one and two.

## 5. Security Analysis

In this protocol, both the outsider eavesdropper and the insider participants (TP, Alice, and Bob) may attempt to obtain the honest participant's private set. Therefore, the proposed protocol must satisfy the following security properties:

(1) The outsider eavesdropper cannot access to the private sets of Alice and Bob, even if they employ various quantum attack strategies.
(2) TP does not gain any information about the private sets, apart from the set intersection.
(3) Alice is unable to obtain Bob's private set.
(4) Bob cannot access to Alice's private set.

**Theorem 1.** *The outsider eavesdropper cannot access to the private sets of Alice and Bob, even if they employ various quantum attack strategies.*

**Proof.** The outsider eavesdropper, often referred to as Eve, may employ various quantum attack strategies, such as intercept–resend, entangle-measurement attack and Trojan horse attacks to obtain the private sets of Alice and Bob. However, the decoy-state method is employed for eavesdropping detection, which can make intercept–resend and the entangle-measurement attack invalid.

Eve may perform the intercept–resend attack [45] to intercept the sequence during the transmission process, measure the intercepted particles and resend a fake sequence whose states are the same as the measurement result to the original receiver. In this scheme, decoy photons are additional, randomly chosen photons sent along with the actual quantum states. If Eve measures the decoy photon in the Z basis ($|0\rangle, |1\rangle$), there is no error. However, if she measures the decoy photon in the X basis (($|+\rangle, |-\rangle$), there is a 50% chance of introducing an error because $|0\rangle$ and $|1\rangle$ are equal superpositions of $|+\rangle$ and $|-\rangle$. Since there is a 50% chance that Eve chooses the Z basis or the X basis, the overall probability of choosing the X basis and introducing an error is $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$. Therefore, when Eve intercepts a decoy photon and chooses a measurement basis that does not match the original state's basis, the measurement results will introduce an error rate of $1/4$. For $d$ decoy photons, the probability that Eve's attack will be detected can be calculated as [46]:

$$p(\text{detected}) = 1 - \left(\frac{3}{4}\right)^d \tag{10}$$

This formula represents the likelihood that $d$ decoy photons will yield errors due to Eve's incorrect measurement basis. As $d$ becomes large, the probability of detection approaches 1. This means that with enough decoy photons, the likelihood of detecting an eavesdropping attempt becomes nearly certain. Therefore, Eve cannot reliably obtain the information from the private sets of Alice and Bob.

The entangle-measure attack [47] is another sophisticated strategy that an eavesdropper, Eve, might employ in a quantum cryptographic protocol. Eve firstly intercepts the quantum sequence during its transmission, and entangles her prepared auxiliary particle

sequence $E = \{|E_0\rangle, |E_1\rangle, \cdots, |E_{n-1}\rangle\}$ on the intercepted sequence through some unitary operations. This process can be given by

$$U|0\rangle|E_i\rangle = \alpha|0\rangle|e_{00}\rangle + \beta|1\rangle|e_{01}\rangle \tag{11}$$

$$U|1\rangle|E_i\rangle = \lambda|0\rangle|e_{10}\rangle + \gamma|1\rangle|e_{11}\rangle \tag{12}$$

$$\begin{aligned} U|+\rangle|E_i\rangle \quad &= \tfrac{1}{2}|+\rangle(\alpha|e_{00}\rangle + \beta|e_{01}\rangle + \lambda|e_{10}\rangle + \gamma|e_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \lambda|e_{10}\rangle - \gamma|e_{11}\rangle) \end{aligned} \tag{13}$$

$$\begin{aligned} U|-\rangle|E_i\rangle \quad &= \tfrac{1}{2}|+\rangle(\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \lambda|e_{10}\rangle - \gamma|e_{11}\rangle) \\ &+\tfrac{1}{2}|-\rangle(\alpha|e_{00}\rangle - \beta|e_{01}\rangle - \lambda|e_{10}\rangle + \gamma|e_{11}\rangle) \end{aligned} \tag{14}$$

where $|\varepsilon_{00}\rangle, |\varepsilon_{01}\rangle, |\varepsilon_{10}\rangle, |\varepsilon_{11}\rangle$ are four pure quantum states determined by the unitary operations and the parameters should satisfy: $|\alpha|^2 + |\beta|^2 = 1$ and $|\lambda|^2 + |\gamma|^2 = 1$.

The eavesdropping detection is performed during the transmission of quantum sequences using decoy photons. When a decoy photon is prepared in the states $|0\rangle$ or $|1\rangle$, Eve must set parameters $\beta = \lambda = 0$ to avoid detection. For the states $|+\rangle$ or $|-\rangle$, if Eve tries to pass the detection process, she must manipulate the quantum states such that $\alpha|e_{00}\rangle - \beta|e_{01}\rangle + \lambda|e_{10}\rangle - \gamma|e_{11}\rangle$ and $\alpha|e_{00}\rangle + \beta|e_{01}\rangle - \lambda|e_{10}\rangle - \gamma|e_{11}\rangle$ becomes a zero vector. Therefore, we can deduce that $\alpha|e_{00}\rangle = \gamma|e_{11}\rangle$.

Substituting the above results into Equations (11)–(14), we obtain

$$U|0\rangle|E_i\rangle = \alpha|0\rangle|e_{00}\rangle \tag{15}$$

$$U|1\rangle|E_i\rangle = \gamma|1\rangle|e_{11}\rangle = \alpha|0\rangle|e_{00}\rangle \tag{16}$$

$$U|+\rangle|E_i\rangle = \frac{1}{2}|+\rangle(\alpha|e_{00}\rangle + 0 + 0 + \gamma|e_{11}\rangle) = \alpha|0\rangle|e_{00}\rangle \tag{17}$$

$$U|-\rangle|E_i\rangle = \frac{1}{2}|-\rangle(\alpha|e_{00}\rangle - 0 - 0 + \gamma|e_{11}\rangle) = \alpha|0\rangle|e_{00}\rangle \tag{18}$$

As can be seen from Equations (15)–(18), if Eve can pass the eavesdropping check under the condition that the particles and ancillary states are in a product state, then the entangle-measurement attack does not succeed.

Eve may attempt Trojan horse attacks, such as the delay-photon attack and the invisible photon attack [48], to intercept private inputs. These attacks threaten the security of the two-way quantum protocol by compromising the transmission of quantum sequences from Alice or Bob to TP. To mitigate this risk, it is recommended to implement a wavelength quantum filter and a photon number splitter [49], which would resist such attacks. Once these attacks are detected, the scheme will be restarted.

Therefore, the outsider eavesdropper cannot access the private sets of Alice and Bob, even if they employ various quantum attack strategies. □

**Theorem 2.** *TP does not gain any information about the private sets, apart from the set intersection.*

**Proof.** A dishonest TP may prepare single photons instead of Bell states to gain any information about the private sets $A$ and $B$. Assume that TP prepares $2n$ single photons, and sends $n$ single photons to Alice, while sending another $n$ single photons to Bob. When Alice and Bob perform the corresponding unitary operations based on the secret key $K_{AB}$ to encode Bob's own set elements in $S_A and S_B$, he can learn the final states. However, the different unitary operations performed on the same single photons may produce the same result. Therefore, TP cannot deduce the elements of Alice's and Bob's sets without knowing the secret key $K_{AB}$. In conclusion, the proposed scheme is secure against TP's attack

and TP does not gain any information about the private sets $A$ and $B$, apart from the set intersection. □

**Theorem 3.** *Alice is unable to obtain Bob's private set.*

**Proof.** Since there is no direct communication between Alice and Bob, if Alice wants to obtain Bob's private set $B$, she needs to perform an intercept–resend attack on the quantum channel with the quantum sequence $EG'_B$ transmitted from Bob to TP. Even if Bob receives the fake sequence, he will announce the inserted positions of the decoy particles. Despite the detection of the attack, Alice can obtain the sequence $EG_B$. In fact, if Alice knows $G_B$, she can deduce the private set of Bob based on the relationship between $G_B$ and the secret key $K_{AB}$. However, $EG_B$ is generated using the rotational encryption operator $R_y(K_B)$ to encrypt $G_B$. After passing the eavesdropping detection, Bob will announce the secret key $K_B$ to TP for obtaining $G_B$. If the eavesdropping detection fails due to the presence of an eavesdropper, the scheme will be restarted, and Bob will not announce his secret key $K_B$. Therefore, even if Alice can obtain the sequence $EG_B$, she cannot access to Bob's private set $B$ without knowing the secret key $K_B$. □

**Theorem 4.** *Bob cannot access Alice's private set.*

**Proof.** The roles of Alice and Bob in the proposed scheme are identical. If Bob wants to access Alice's private set $A$, he also needs to perform an intercept–resend attack on the quantum channel with the quantum sequence $EG'_A$ transmitted from Alice to TP. Similar to Alice's attack, Bob has no chance of knowing Alice's secret key $K_A$ due to the failure of passing the eavesdropping detection. Therefore, even if Bob can obtain $EG_A$ by performing the intercept–resend attack, he cannot access Alice's private set $A$ due to him not knowing the secret key $K_A$ for decrypting $EG_A$ to obtain $G_A$. □

## 6. Comparison

To effectively compare our scheme with the existing QPSI scheme, we outline key aspects such as the quantum resources used, quantum operations, and quantum measurements in Table 3.

**Table 3.** Comparison between our scheme with the existing QPSI scheme.

| Protocol | Quantum Source | Quantum Operation | Quantum Measurements | Technical Implementation Difficulty |
|---|---|---|---|---|
| Ref. [27] | n encoded states | $U_0$ and $U_S$ | Von Neumann measurements | Difficult |
| Ref. [28] | n encoded states | $U_0$ and $U_S$ | von Neumann measurements | Difficult |
| Ref. [29] | OAM basis states of single photons | QFT | OAM basis measurement | Difficult |
| Ref. [30] | Single photons | Fractional times of the Hadamard gate | Single-particle projective measurements | Difficult |
| Ours | Bell states | $I$, $X$ and $Z$ | Bell-basis | Easy |

Ref. [27] requires the preparation of $n$ encoded states that are multi-particle entangled states, as well as the quantum operator $G$, and von Neumann measurements to achieve the calculation of set intersection, where $G = -U_0 U_S$. Here, the two unitary operations $U_0$ and $U_S$ are defined as follows:

$$U_0 = \sum_{x \neq 0} |x\rangle\langle x| - |0\rangle\langle 0| \tag{19}$$

$$U_S = \sum_{x \notin S} |x\rangle\langle x| - \sum_{x \in S} |x\rangle\langle x| \tag{20}$$

These two unitary operations are realized by complex oracles.

Ref. [28] proposed an improved scheme to address the fairness issue present in Ref. [27]; thus, the quantum technologies used are the same as those in Ref. [27]. Consequently, both schemes in Refs. [27,28] are difficult to implement under the current quantum technologies, which limits their practicality.

Ref. [29] requires the preparation of OAM basis states of single photons as quantum resources. OAM basis states refer to a set of quantum states of light that carry orbital angular momentum. Additionally, it requires OAM basis measurement. However, preparing OAM basis states and conducting OAM basis measurements are challenging with the current quantum technologies.

Ref. [30] utilizes single photons as quantum resources, and a Hadamard gate for encoding the private set. The requirement for fractional applications of the Hadamard gate presents significant challenges in current quantum technology.

In contrast, our scheme utilizes Bell states as quantum resources, $I$, $X$ and $Z$ gates for encoding the private sets, and $R_y$ rotation operation for protecting the privacy of the sets. These components are easier to implement with current technologies, making our scheme more practical.

## 7. Conclusions

In this paper, we propose a quantum private set intersection (QPSI) scheme utilizing Bell states, unitary operations, and Bell measurements as its building blocks. We use the $I$, $X$, and $Z$ gates for encoding the private sets, which are applied to the received Bell states to compute the set intersection. The privacy of the sets is ensured by the principles of quantum mechanics, meaning that even an adversary with quantum capabilities cannot compromise the security of the private inputs. The feasibility of this scheme is verified through simulations conducted on a quantum platform. Compared to existing QPSI schemes, our scheme is more feasible to implement with current technologies, utilizing Bell states as quantum resources, $I$, $X$, and $Z$ gates for encoding the private sets, $R_y$ rotation operations for protecting the privacy of the sets, and Bell measurements for obtaining results. It is worth noting that if the participants or the third party are malicious (e.g., if one of the participants utilizes a universal set for calculation), the other participant's set may be exposed. In this regard, we will focus on the verifiability of QPSI schemes in future work.

**Author Contributions:** Conceptualization, M.H. and S.Z.; methodology, M.H. and S.Z.; Writing—original draft, M.H.; writing—review and editing, Y.W. and S.Z.; supervision, S.Z. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research was funded by the Open Fund of Network and Data Security Key Laboratory of Sichuan Province (Grant No. NDS2024-1) and Gongga Plan for the "Double World-class Project".

**Data Availability Statement:** Data are contained within the article.

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

## References


1. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd IEEE Symposium on Foundations of Computer Science (FOCS' 82), Washington, DC, USA, 3–5 November 1982; p. 160.
2. Tian, Y.; Li, J.; Chen, X.-B.; Ye, C.-Q.; Li, H.-J. An efficient semi-quantum secret sharing protocol of specific bits. *Quantum Inf. Process.* **2021**, *20*, 217. [CrossRef]
3. Senthoor, K.; Sarvepalli, P.K. Theory of communication efficient quantum secret sharing. *IEEE Trans. Inf. Theory* **2022**, *68*, 3164–3186. [CrossRef]
4. Qin, Y.; Cheng, J.; Ma, J.; Zhao, D.; Yan, Z.; Jia, X.; Xie, C.; Peng, K. Efficient and secure quantum secret sharing for eight users. *Phys. Rev. Res.* **2024**, *6*, 033036. [CrossRef]
5. Liu, D.M.; Yan, L.L.; Xu, S.H.; Qiu, C.; Huang, X. New flexible quantum private query protocol against rotation noise. *Quantum Inf. Process.* **2021**, *20*, 1–13. [CrossRef]
6. Qin, L.; Liu, B.; Gao, F.; Huang, W.; Xu, B.; Li, Y. Decoy-state quantum private query protocol with two-way communication. *Phys. A Stat. Mech. Its Appl.* **2024**, *633*, 129427. [CrossRef]
7. Liu, B.; Xia, S.; Xiao, D.; Huang, W.; Xu, B.; Li, Y. Decoy-state method for quantum-key-distribution-based quantum private query. *Sci. China Phys. Mech. Astron.* **2022**, *65*, 240312. [CrossRef]
8. Liu, C.; Zhou, S.; Gong, L.-H.; Chen, H.-Y. Quantum private comparison protocol based on 4D GHZ-like states. *Quantum Inf. Process.* **2023**, *22*, 1–16. [CrossRef]
9. Zhou, N.R.; Xu, Q.D.; Du, N.S.; Gong, L.H. Semi-quantum private comparison protocol of size relation with d-dimensional Bell states. *Quantum Inf. Process.* **2021**, *20*, 1–15. [CrossRef]
10. Kou, T.Y.; Che, B.C.; Dou, Z.; Chen, X.B.; Lai, Y.P.; Li, J. Efficient quantum private comparison protocol utilizing single photons and rotational encryption. *Chin. Phys. B* **2022**, *31*, 060307. [CrossRef]
11. Zhang, J.W.; Xu, G.; Chen, X.B.; Chang, Y.; Dong, Z.C. Improved multiparty quantum private comparison based on quantum homomorphic en-cryption. *Phys. A Stat. Mech. Its Appl.* **2023**, *610*, 128397. [CrossRef]
12. Wu, W.Q.; Zhao, Y.X. Quantum private comparison of size using d-level Bell states with a semi-honest third party. *Quantum Inf. Process.* **2021**, *20*, 155. [CrossRef]
13. Chen, F.-L.; Zhang, H.; Chen, S.-G.; Cheng, W.-T. Novel two-party quantum private comparison via quantum walks on circle. *Quantum Inf. Process.* **2021**, *20*, 178. [CrossRef]
14. Huang, X.; Zhang, W.-F.; Zhang, S.-B. Efficient multiparty quantum private comparison protocol based on single photons and rotation encryption. *Quantum Inf. Process.* **2023**, *22*, 272. [CrossRef]
15. Gianni, J.; Qu, Z. New Quantum private comparison using hyperentangled ghz state. *J. Quantum Comput.* **2021**, *3*, 45–54. [CrossRef]
16. Wei, L.; Liu, J.; Zhang, L.; Wang, Q.; Zhang, W.; Qian, X. Efficient multi-party private set intersection protocols for large participants and small sets. *Comput. Stand. Interfaces* **2024**, *87*, 103764. [CrossRef]
17. Wu, M.; Yuen, T.H. Efficient unbalanced private set intersection cardinality and user-friendly privacy-preserving contact tracing. In Proceedings of the 32nd USENIX Security Symposium (USENIX Security 23), Anaheim, CA, USA, 9–11 August 2023; pp. 283–300.
18. Wang, F.; Mi, B.; Zeng, R. Efficient Private Set Intersection for Vertical Federated Learning in IoV. In *International Conference on Frontiers in Cyber Security*; Springer Nature Singapore: Singapore, 2024; pp. 120–130.
19. Shi, R.H.; Li, Y.F. Quantum private set intersection cardinality protocol with application to privacy-preserving condition query. *IEEE Trans. Circuits Syst. I Regul. Pap.* **2022**, *69*, 2399–2411. [CrossRef]
20. Cai, R.; Chen, L.; Zhu, Y. Using private set intersection to achieve privacy-preserving authorization for IoT systems. *J. Inf. Secur. Appl.* **2024**, *83*, 103759. [CrossRef]
21. Pinkas, B.; Schneider, T.; Tkachenko, O.; Yanai, A. Efficient circuit-based PSI with linear communication. In Proceedings of the Advances in Cryptology–EUROCRYPT 2019: 38th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Darmstadt, Germany, 19–23 May 2019; Proceedings, Part III 38; Springer International Publishing: Cham, Switzerland, 2019; pp. 122–153.
22. Dong, C.; Chen, L.; Wen, Z. When private set intersection meets big data: An efficient and scalable protocol. In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4–8 November 2013.
23. Freedman, M.J.; Nissim, K.; Pinkas, B. Efficient private matching and set intersection. In *International Conference on the Theory and Applications of Cryptographic Techniques*; Springer: Berlin/Heidelberg, Germany, 2004; pp. 1–19.
24. Shor, P.W. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. *SIAM Rev.* **1999**, *41*, 303–332. [CrossRef]
25. Grover, L.K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **1997**, *79*, 325–328. [CrossRef]
26. Huang, X.; Zhang, W.; Zhang, S. Quantum multi-party private set intersection using single photons. *Phys. A Stat. Mech. Its Appl.* **2024**, *649*, 129974. [CrossRef]

27. 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]
28. Cheng, X.; Guo, R.; Chen, Y. Cryptanalysis and improvement of a quantum private set intersection protocol. *Quantum Inf. Process.* **2017**, *16*, 1–8. [CrossRef]
29. Liu, W.; Yin, H.W. A novel quantum protocol for private set intersection. *Int. J. Theor. Phys.* **2021**, *60*, 2074–2083. [CrossRef]
30. 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]
31. Hou, M.; Wu, Y. Efficient Quantum Private Comparison with Unitary Operations. *Mathematics* **2024**, *12*, 3541. [CrossRef]
32. Huang, X.; Zhang, W.; Zhang, S. Practical quantum protocols for blind millionaires' problem based on rotation encryption and swap test. *Phys. A Stat. Mech. Its Appl.* **2024**, *637*, 129614. [CrossRef]
33. Hou, M.; Wu, Y. New Quantum Private Comparison Using Bell States. *Entropy* **2024**, *26*, 682. [CrossRef]
34. Christensen, R.B.; Popovski, P. Private product computation using quantum entanglement. *IEEE Trans. Quantum Eng.* **2023**, *4*, 1–9. [CrossRef]
35. Roffe, J. Quantum error correction: An introductory guide. *Contemp. Phys.* **2019**, *60*, 226–245. [CrossRef]
36. Cai, W.; Ma, Y.; Wang, W.; Zou, C.-L.; Sun, L. Bosonic quantum error correction codes in superconducting quantum circuits. *Fundam. Res.* **2021**, *1*, 50–67. [CrossRef]
37. Livingston, W.P.; Blok, M.S.; Flurin, E.; Dressel, J.; Jordan, A.N.; Siddiqi, I. Experimental demonstration of continuous quantum error correction. *Nat. Commun.* **2022**, *13*, 230. [CrossRef] [PubMed]
38. Postler, L.; Butt, F.; Pogorelov, I.; Marciniak, C.D.; Heußen, S.; Blatt, R.; Schindler, P.; Rispler, M.; Müller, M.; Monz, T. Demonstration of fault-tolerant steane quantum error correction. *PRX Quantum* **2024**, *5*, 030326. [CrossRef]
39. Lassen, M.; Berni, A.; Madsen, L.S.; Filip, R.; Andersen, U.L. Gaussian error correction of quantum states in a correlated noisy channel. *Phys. Rev. Lett.* **2013**, *111*, 180502. [CrossRef] [PubMed]
40. Lidar, D.A. Review of Decoherence-Free Subspaces, Noiseless Subsystems, and Dynamical Decoupling. In *Quantum Information and Computation for Chemistry*; John Wiley & Sons, Ltd.: New York, NY, USA, 2014; pp. 295–354.
41. Li, C.K.; Nakahara, M.; Poon, Y.T.; Sze, N.S.; Tomita, H. Recursive encoding and decoding of the noiseless subsystem and decoherence-free sub-space. *Phys. Rev. A At. Mol. Opt. Phys.* **2011**, *84*, 044301. [CrossRef]
42. Hu, X.; Zhang, F.; Li, Y.; Long, G. Optimizing quantum gates within decoherence-free subspaces. *Phys. Rev. A* **2021**, *104*, 062612. [CrossRef]
43. Qin, W.; Wang, C.; Zhang, X. Protected quantum-state transfer in decoherence-free subspaces. *Phys. Rev. A* **2015**, *91*, 042303. [CrossRef]
44. 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; pp. 175–179.
45. Huang, X.; Zhang, S.; Xia, J. Efficient Quantum Private Comparison Using Locally Indistinguishable Orthogonal Product States. In *International Conference on Artificial Intelligence and Security*; Springer International Publishing: Cham, Switzerland, 2022; pp. 260–273.
46. Chen, Y.; 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]
47. Hou, M.; Wu, Y. Quantum Private Comparison Based on Four-Particle Cluster State. *Appl. Sci.* **2024**, *14*, 10759. [CrossRef]
48. Yang, Y.G.; Sun, S.J.; Zhao, Q.Q. Trojan-horse attacks on quantum key distribution with classical Bob. *Quantum Inf. Process.* **2015**, *14*, 681–686. [CrossRef]
49. Jain, N.; Anisimova, E.; Khan, I.; Makarov, V.; Marquardt, C.; Leuchs, G. Trojan-horse attacks threaten the security of practical quantum cryptography. *New J. Phys.* **2014**, *16*, 123030. [CrossRef]