entropy

IMPACT FACTOR 2.7

Indexed in: PubMed

CITESCORE 4.7

Article

A Semi-Quantum Private Comparison Base on W-States

Jian Li, Zhuo Wang, Jun Yang, Chongqiang Ye and Fanting Che

Special Issue
Quantum and Classical Physical Cryptography

Edited by
Dr. Hua-Lei Yin, Dr. Kaizhi Huang and Dr. Guan-Jie Fan-Yuan

MDPI

https://doi.org/10.3390/e25091269

entropy

MDPI

Article

A Semi-Quantum Private Comparison Base on W-States

Jian Li [1,2], Zhuo Wang [3,*], Jun Yang [1], Chongqiang Ye [3] and Fanting Che [3]

[1] School of Information Engineering, Ningxia University, Yinchuan 750021, China; lijian@bupt.edu.cn (J.L.); dragon@nxu.edu.cn (J.Y.)
[2] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876, China
[3] School of Artificial Intelligence, Beijing University of Posts and Telecommunications, Beijing 100876, China; chongqiangye@bupt.edu.cn (C.Y.); qingxi1999@outlook.com (F.C.)
* Correspondence: zhuowang@bupt.edu.cn

Abstract: Privacy comparison is an important research topic in secure multi-party computing, widely used in e-commerce, secret ballots, and other fields. However, the development of quantum computing power poses a growing potential security threat to secure multi-party algorithms based on mathematically tricky problems, and most of the proposed quantum privacy comparison schemes could be more efficient. Therefore, based on the W-state, we offer a more efficient semi-quantum privacy comparison method. The security analysis shows that the scheme can resist third-party, measurement, and entanglement attacks. Compared with the previous work, the scheme significantly improves communication efficiency and has stronger practicability.

Keywords: quantum private comparison; quantum cryptography; quantum communication

check for updates

Citation: Li, J.; Wang, Z.; Yang, J.; Ye, C.; Che, F. A Semi-Quantum Private Comparison Base on W-States. *Entropy* **2023**, *25*, 1269. https://doi.org/10.3390/e25091269

Academic Editors: Hua-Lei Yin, Kaizhi Huang, Guan-Jie Fan-Yuan and Osamu Hirota

Received: 27 June 2023
Revised: 21 August 2023
Accepted: 23 August 2023
Published: 29 August 2023

1. Introduction

Secure multiparty computing (secure multiparty computation, SMC) was proposed by Yao to prevent multiple participants' privacy leakage and let them work together to solve the computing problem [1]. SMC is widely used in e-commerce, data compression, and secret ballots. Secure multiparty computing (SMC) is an essential topic in distributed computing. It allows a group of users who do not trust each other to perform distributed computing with the participation of a semi-trusted third party to obtain the comparison results of private information without revealing their input.

However, the quantum computer threatens the security of classical SMC. With the improvement of computing power and the emergence of quantum algorithms [2,3], the SMC cryptographic protocol based on classical NP problems is repeatedly broken. As an indivisible smallest unit, quantum has its unique properties. The principle of quantum uncertainty makes it impossible for eavesdroppers to measure the state of transmitted quantum states accurately, and the principle of quantum non-cloning ensures that eavesdroppers cannot accurately copy transmitted quantum states and obtain adequate information [4–6]. Therefore, quantum privacy comparison is applied to resist quantum attacks as a branch of quantum cryptography.

Compared with quantum communication, semi-quantum communication has unique advantages, which are easier to realize while ensuring security. Users can use only straightforward quantum devices, saving the high cost of buying or preparing quantum states. In particular, if the device fails during quantum communication, it can switch from quantum communication to semi-quantum communication to complete the whole process. Therefore, the research on semi-quantum cryptographic communication is significant in quantum communication. Compared with quantum privacy comparison, semi-quantum privacy comparison has the advantages of lower requirements on hardware devices, easier realization, and more common application scenarios.

In 2016, the first semi-quantum privacy comparison protocol (SQPC) [7] based on Bell states was proposed by Chou et al., ensuring that two classical users compare their private information without revealing privacy. Subsequently, many improvements and optimizations of SQPC have been proposed [8–18]. In 2018, Ye et al. [11] constructed an SQPC protocol based on the product of two-particle tensors without an entanglement exchange. In 2018, Thapliyal et al. [12] proposed an SQPC protocol based on an orthogonal state in a noisy environment, which adopted the Bell state as a quantum state carrier In the same year, Lang [13] proposed two SQPC protocols with different TP identities and abandoned the quantum entanglement exchange operation. For malicious TP, he cannot know the private information or the results. Lin et al. [14] abandoned the quantum entanglement exchange operation in 2019. They used a single-photon state to build a practical and efficient SQPC protocol, requiring a shared key in advance to achieve. In 2021, Tian et al. [15] proposed a novel semi-quantum private comparison (SQPC) protocol based on W-state, which is more efficient. In 2022, Wang et al. [16] designed an SQPC protocol using the GHZ state with D-dimension. Geng et al. [17] constructed the SQPC protocol for the D-level single-particle state size relationship. In 2023, He et al. [18] proposed an improved SQPC protocol with a higher security level than Tian et al. 's scheme [15]. Based on the decoherence-free states, two multi-party semi-quantum private comparison protocols are proposed to counteract collective noises [19]. And by adopting d-dimensional Bell states, Lian et al. [20] constructed an MQPC protocol that can be used in a strange user environment.

In this work, a semi-quantum privacy comparison (SQPC) protocol is proposed, which has higher efficiency compared with before works; it does not need to share the key in advance and has a higher interception detection rate. Therefore, this scheme is more practical. The structure of this paper is as follows: in Section 2, the work related to semi-quantum privacy comparison and the basis of quantum information are introduced; in Section 3, the steps and contents of the protocol are explained in detail; the security analysis part is shown in the fourth part; finally, the summary of this work is given.

2. Preliminaries

2.1. Entangled States

The two W-states were used to distribute to the three participants, and they are denoted by

$$|W\rangle = \frac{1}{\sqrt{3}}(|011\rangle + |010\rangle + |100\rangle), \tag{1}$$

$$|H\rangle = \frac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle), \tag{2}$$

The $|W\rangle$ state can be described as

$$\begin{aligned} |W\rangle &= \sqrt{\tfrac{2}{3}}\left(\tfrac{|01\rangle+|10\rangle}{\sqrt{2}}_{1,2} \otimes |0\rangle_3\right) + \tfrac{1}{\sqrt{6}}\left(\tfrac{|00\rangle+|11\rangle}{\sqrt{2}} + \tfrac{|00\rangle-|11\rangle}{\sqrt{2}}\right)_{1,2} \otimes |1\rangle_3 \\ &= \sqrt{\tfrac{2}{3}}\left(\tfrac{|01\rangle+|10\rangle}{\sqrt{2}}_{1,3} \otimes |0\rangle_2\right) + \tfrac{1}{\sqrt{6}}\left(\tfrac{|00\rangle+|11\rangle}{\sqrt{2}} + \tfrac{|00\rangle-|11\rangle}{\sqrt{2}}\right)_{1,3} \otimes |1\rangle_2 \\ &= \sqrt{\tfrac{2}{3}}\left(\tfrac{|01\rangle+|10\rangle}{\sqrt{2}}_{2,3} \otimes |0\rangle_1\right) + \tfrac{1}{\sqrt{6}}\left(\tfrac{|00\rangle+|11\rangle}{\sqrt{2}} + \tfrac{|00\rangle-|11\rangle}{\sqrt{2}}\right)_{2,3} \otimes |1\rangle_1 \\ &= \sqrt{\tfrac{2}{3}}(|\psi^+\rangle) \otimes |0\rangle + \tfrac{1}{\sqrt{6}}(|\phi^+\rangle + |\phi^-\rangle) \otimes |1\rangle \end{aligned} , \tag{3}$$

Therein, the subscript marks the particle position.
The $|H\rangle$ state can be described as

$$\begin{aligned} |H\rangle &= \tfrac{1}{\sqrt{2}}\left(\tfrac{|00\rangle+|11\rangle}{\sqrt{2}} \otimes |1\rangle + \tfrac{|01\rangle+|10\rangle}{\sqrt{2}} \otimes |0\rangle\right) \\ &= \tfrac{1}{\sqrt{2}}(|\phi^+\rangle \otimes |1\rangle + |\psi^+\rangle \otimes |0\rangle) \end{aligned} , \tag{4}$$

Accordingly, the following circuit is used to implement $|H\rangle$ in Figure 1.

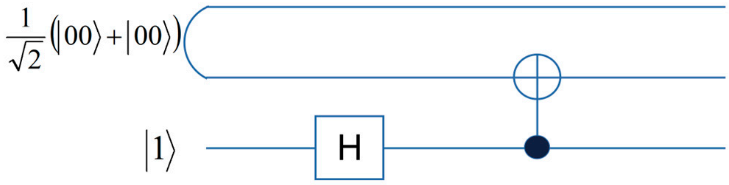

Figure 1. The preparation circuit of $|H\rangle$.

Among them, $|\psi^+\rangle$, $|\phi^+\rangle$, $|\phi^-\rangle$ are kinds of Bell states, which will be used to take the joint measurement and can be expressed a

$$\begin{aligned} |\phi^+\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \\ |\phi^-\rangle &= \tfrac{1}{\sqrt{2}}(|00\rangle - |11\rangle), \\ |\psi^+\rangle &= \tfrac{1}{\sqrt{2}}(|01\rangle + |10\rangle). \end{aligned} \tag{5}$$

2.2. One-Time Pad

The one-time pad (OTP) is a symmetric encryption algorithm, which was first invented by Frank Miller [21]. In OTP, the message sender and the message receiver share a random secret key k, called a one-time pad. In general, it requires that the random pad k and the message m to be sent should have the same size. To encrypt the message, the sender calculates $c = m \oplus k$ and sends OTP ciphertext c to the receiver, where the symbol "$\oplus$" denotes addition under modular two. To decrypt c, the receiver calculates $m = c \oplus k$. It is impossible for an adversary to break m from the ciphertext c due to the unconditional security of OTP [22,23].

3. Semi-Quantum Private Comparison Scheme

By default, the semi-quantum privacy comparison (SQPC) means two participants who do not have complete quantum capabilities are helped by a trusted third party (TP). As a semi-trusted third party, TP will not collude with participants to obtain users' privacy, nor will it disclose any participants' privacy; they have the full quantum capability to prepare, manipulate and measure quantum states. A new semi-quantum privacy comparison protocol based on three-particle entangled states is proposed below, which does not require a pre-shared key and has higher efficiency. The model of SQPC is shown in Figure 2.

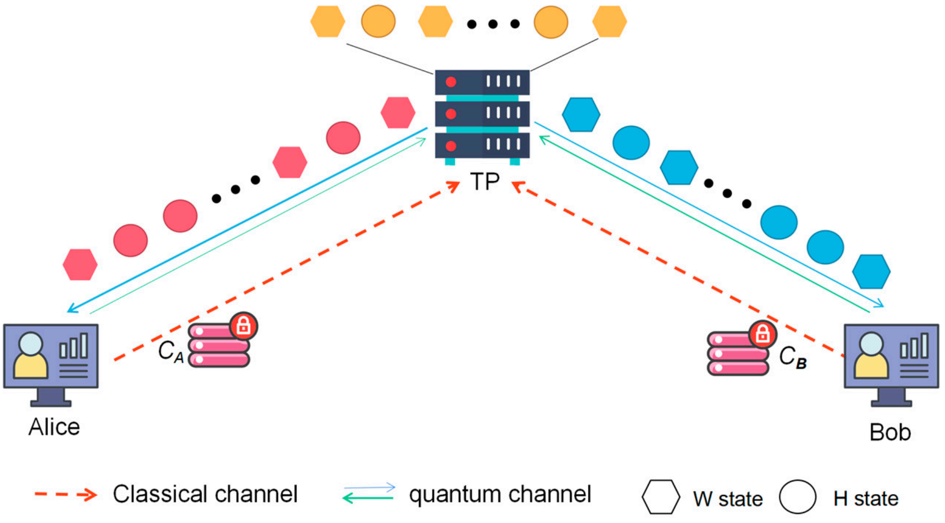

Figure 2. The model of protocol.

Suppose that two copies of private information from Alice and Bob need to be compared. TP must compare whether its private information is consistent without knowing the specific information. Alice and Bob establish a quantum channel and classical channel with TP, respectively, and can only do the following two operations for the received qubit.

(1) MEASURE: Using the Z-basis to measure the qubit, re-prepare the same one with the measurement result and send it back.
(2) REFLECT: Return the qubit without doing anything.

Step 1: TP prepares N (= 4 n) entangled states according to Equations (1) and (2), including 2 n $|W\rangle$ and 2 n $|H\rangle$. TP then divides these entangled states into three single particles. Separately, the particle at the first position forms the sequence $S_A = \left(s_A^1, s_A^1, \ldots s_A^n\right)$, the particle at the second position forms the sequence $S_B = \left(s_B^1, s_B^2, \ldots s_B^n\right)$, and the particle at the third position forms the sequence $S_T = \left(s_T^1, s_T^2, \ldots s_T^n\right)$; S_A, S_B, and S_T are random quantum sequences of $|0\rangle$ or $|1\rangle$ from the $|W\rangle$ and $|H\rangle$ states; S_A^i, S_B^i and S_T^i represents the first state, the second state, and the third state, respectively.

Step 2: TP sends the particle in the travel sequence S_A to Alice and the state in the travel sequence S_B to Bob, while it remains in TP's own hands. Note that only TP knows whether the states come from $|W\rangle$ or from $|H\rangle$.

Step 3: Alice and Bob randomly perform both MEASURE and REFLECT operations when receiving S_A and S_B. Note that the probability that Alice and Bob choose both the MEASURE operation and the REFLECT operation is 1/2. Therein, Alice and Bob each select n quantum states to perform the MEASURE operation and select n quantum states to perform the REFLECT operation. The sequence sent back by Alice and bob is noted as $\hat{S}_A$ and $\hat{S}_B$. Meanwhile, according to the measurement results of MEASURE operation, Alice and Bob record 1 if it is $|1\rangle$; otherwise, if the outcome is $|0\rangle$, they record it as 0.

Step 4: TP yields a new sequence of states after receiving all the sequences returned from Alice and Bob, respectively. Consequently, Alice and Bob each announce the position that is performed by the MEASURE operation. TP performs channel detection based on Alice's and Bob's operations. Specific operations are as follows:

TP selects the pairs in which Alice and Bob both perform the REFLECT operation, uses the Bell basis joint measurement (S_A^i, S_B^i), and uses Z-basis to measure the retained in his own hand. Then, TP checks to see if the joint measurements match the state in S_T^i, that is, when the S_T^i is from $|W\rangle$, the joint measurement result should be either $|\phi^+\rangle$ or $|\phi^-\rangle$; conversely, when the S_T^i is from $|H\rangle$, the joint measurement result must only be $|\phi^+\rangle$. In particular, if the measurement in $|H\rangle$ appears $|\phi^-\rangle$, then the channel has an eavesdropper.

Step 5: After the channel detection is complete, TP picks out the particles that both Alice and Bob choose the MEASURE operation. In this case, Alice's and Bob's measurements may agree or not, but TP cannot determine it by measurement outcome. TP makes a Z-basis measurement for S_T^i at these locations and publishes the measurement outcome, the published result in the corresponding position is marked 1 or 0. If the measurement is $|0\rangle$, it is recorded as 0. Otherwise, it is recorded as 1.

Step 6: Alice and Bob negotiate whether TP is honest according to the position published by TP; for the position marked 1 by TP, Alice and Bob check that the measurements are consistent, and conversely, for the position marked 0, Alice and Bob check that the measurements are opposite. If the results show that the TP is honest, Alice and Bob share the key K_{AB} through negotiation. When the measurement results of both parties are the same, K_{AB} is the default value, that is the measurement result; when the measurement results are different, K_{AB} is the random value, that is 0 or 1.

Step 7: Alice and Bob share the key with TP, respectively. For Alice and Bob take different operations, Alice and Bob keep a secret sequence of their measurements denoted as K_{AT}, K_{BT}. Concretely, when Alice adopts MEASURE and Bob adopts REFLECT, TP adopts the Bell base joint measurement for (S_A^i, S_T^i). When Alice adopts REFLECT and Bob adopts MEASURE, TP adopts the Bell base joint measurement for (S_B^i, S_T^i). According to Equations (2) and (3), if the measurement is $|\phi^+\rangle$ or $|\phi^-\rangle$, TP yields K_{AT} or K_{BT} 1; otherwise, if the measurement result is $|\psi^+\rangle$, TP yields K_{AT} or K_{BT} 0.

Step 8: TP implements privacy protection as follows. Suppose the private messages to be compared from Alice and Bob are $m_A = [m_{a1}, m_{a2}, \ldots m_{an}]$, $m_B = [m_{b1}, m_{b2}, \ldots m_{bn}]$. Alice computes

$$C_A = m_A \oplus K_{AT} \oplus K_{AB}, \tag{6}$$

Bob computes

$$C_B = m_B \oplus K_{BT} \oplus K_{AB}, \tag{7}$$

Alice and Bob send the computation result to TP, respectively.
Immediately after, TP computes

$$C = C_A \oplus C_B \oplus K_{AT} \oplus K_{BT}. \tag{8}$$

According to the law of modular two operations, if C is a bit sequence of 0, it means the privacy information is the same; if 1 appears in the sequence, it means the privacy information is different. Below, the operations and purposes of different situations in the protocol are summarized in Table 1.

Table 1. Summary table of state types and their corresponding operations.

State	Operation (Alice)	Operation (Bob)	Purpose	Population
$\|W\rangle$	REFLECT	REFLECT	Detection channel	$n/2$
$\|H\rangle$	REFLECT	REFLECT		$n/2$
$\|W\rangle$	MEASURE	REFLECT	Share Key	$n/2$
$\|H\rangle$	MEASURE	REFLECT		$n/2$
$\|W\rangle$	REFLECT	MEASURE		$n/2$
$\|H\rangle$	REFLECT	MEASURE		$n/2$
$\|W\rangle$	MEASURE	MEASURE	Comparison	$n/2$
$\|H\rangle$	MEASURE	MEASURE		$n/2$

If T is a bit.

4. Security and Efficiency Analysis

This chapter first gives the correctness analysis, then analyzes the security of semi-trusted third parties and users, and finally provides the attack with the analysis of malicious users.

4.1. Correctness

According to Equations (6) and (7), Equation (8) is can be written as

$$\begin{aligned} C &= (m_A \oplus K_{AT} \oplus K_{AB}) \oplus (m_B \oplus K_{BT} \oplus K_{AB}) \oplus K_{AT} \oplus K_{BT} \\ &= m_A \oplus m_B \end{aligned}, \tag{9}$$

Therefore, they will satisfy the following equality,

$$\begin{cases} C = m_A \oplus m_B = 1, m_A \neq m_B \\ C = m_A \oplus m_B = 0, m_A = m_B \end{cases}. \tag{10}$$

According to Equation (10), every bit of the binary sequence is performed modulo 2; if it is the same binary number in that position, the result is 0; otherwise it is 1.

To sum up, the privacy comparison of the protocol can be prepared to determine whether the binary sequence is consistent through the calculation results. If 1 appears in succession, it means that the information in this position is inverted; if C is a string of 0, it means that the two pieces of information are the same.

4.2. Outside Attack

Generally, there are three attack ways for external attackers to steal users' privacy information: intercept re-transmission attack, measurement-re-transmission attack, and entanglement measurement attack. For each type of attack, the following section provides a corresponding security analysis.

4.2.1. Intercept Re-Transmission Attack

Take the quantum channel of Alice and TP as an example. Assuming that Eve, as a fake TP, intercepts the sequence sent by TP to Alice, Eve sends Alice the fake sequence prepared in advance. Alice randomly performs MEASURE operations and REFLECT operations on the fake sequence. According to the protocol design, she will send the sequence to Eve (fake TP). Later, Alice and Bob will announce where they each took the non-stop action. At this point, Eve can use Alice's and Bob's disclosure to create a false key, denoted K'_{AT} and K'_{BT} respectively. However, Eve still does not have access to Alice and Bob's private information. According to protocol Step 8, Equations (6) and (7), even if Eve obtains Alice's and Bob's calculation results as a fake TP, he cannot obtain the privacy information m_A and m_B from the calculation results according to the one-time-secret nature of OTP [21–23]. To make matters worse, TP will discover Eve's presence by comparing fake sequences forwarded by Eve. Furthermore, since the qubits corresponding to the false sequence and the issuing sequence are different, TP and Alice or Bob cannot complete the shared key stage. According to Equations (6) and (7), TP cannot decrypt C_A and C_B through K_{AT} and K_{BT}. At this time, TP will again determine that there is an attacker intercepting the particles of the channel.

4.2.2. Measure Re-Transmission Attack

In the measurement re-transmission attack, the attacker intercepts the TP sequence sent to the user, measures it, and forwards it. Taking Alice's channel as an example, it is assumed that Eve intercepts the sequence S_A and makes a Z-basis measurement of its particles, and then Eve sends the measured sequence S_A to Alice. According to the physical properties of the collapse measured by the entangled particles, Alice's random operation will not change the state of the particles. Therefore, when Alice sends the particle back to TP, TP will find Eve's attack behavior through the detection of Step 4.

Compared with the previous scheme, our scheme will have a higher interception detection rate. If Alice chooses the MEASURE operation and Bob chooses the REFLECT operation, the attack will not be detected. If Alice performs the MEASURE operation, Bob performs the REFLECT operation, and TP performs the Bell measurement and single measurement; then, if the single particle measurement is $|0\rangle$, the attack behavior is detected with a probability of $1/4$, if the single particle measurement is $|1\rangle$, the probability in $|W\rangle$ and $|H\rangle$ are $1/2$ and $1/4$. If Alice and Bob both take the return operation, TP compares the relationship between the Bell measurement and the single particle measurement; then, if the single particle measurement is $|0\rangle$, the attack behavior is detected with a probability of $1/4$, and if it is $|1\rangle$, the probability in $|W\rangle$ and $|H\rangle$ is $1/2$ and $1/4$. Therefore, the probability that Eve's attack behavior is detected under the measurement of repeated attacks is

$$\begin{aligned} p &= \tfrac{1}{2}\left[\tfrac{1}{3}\left(\tfrac{1}{4}\times\tfrac{1}{4}+\tfrac{1}{4}\times\tfrac{1}{4}\right)+\tfrac{2}{3}\left(\tfrac{1}{4}\times\tfrac{1}{2}+\tfrac{1}{4}\times\tfrac{1}{2}\right)\right] \\ &+\tfrac{1}{2}\left[\tfrac{1}{2}\left(\tfrac{1}{4}\times\tfrac{1}{4}+\tfrac{1}{4}\times\tfrac{1}{4}\right)+\tfrac{1}{2}\left(\tfrac{1}{4}\times\tfrac{1}{2}+\tfrac{1}{4}\times\tfrac{1}{2}\right)\right] \\ &= \tfrac{19}{96} \end{aligned}, \tag{11}$$

In this regard, the eavesdropping detection probability of n particle length sequence is $1-\left(\frac{19}{96}\right)^{n}$, as n increases, it approaches 1.

4.2.3. Entanglement Measurement Attack

It is possible for an attacker to construct a new quantum system by introducing auxiliary particles to avoid eavesdropping detection and monitor the whole system by measuring other particles. To achieve the purpose of obtaining private information.

A group of auxiliary particles is introduced to construct a two-dimensional Hilbert space, and a group of orthonormal basis is selected to describe the space vector, which can be expressed as $|\tau_{00}\rangle$, $|\tau_{01}\rangle$, $|\tau_{10}\rangle$, $|\tau_{11}\rangle$. To distinguish the source of the particles, we will represent Alice's particles from $|W\rangle$ and $|H\rangle$ as $\{|0\rangle_{AW}, |1\rangle_{AW}, |0\rangle_{AH}, |1\rangle_{AH}\}$, and Bob's particles from $|W\rangle$ and $|H\rangle$ as $\{|0\rangle_{BW}, |1\rangle_{BW}, |0\rangle_{BH}, |1\rangle_{BH}\}$.

For a particle in the $|H\rangle$, $|0\rangle_H$ represents auxiliary particles. The unitary operations performed on qubits.

$$U_H(|0\rangle_{AH}|0\rangle_H) = |0\rangle_{AH}|\tau_{00}\rangle + |1\rangle_{AH}|\tau_{01}\rangle, \tag{12}$$

$$U_H(|1\rangle_{AH}|0\rangle_H) = |0\rangle_{AH}|\tau_{10}\rangle + |1\rangle_{AH}|\tau_{11}\rangle. \tag{13}$$

Then, the whole system space can be expressed as

$$\begin{array}{l} (|0\rangle_{AH}|\tau_{00}\rangle + |1\rangle_{AH}|\tau_{01}\rangle)|0\rangle_{BH} + (|0\rangle_{AH}|\tau_{10}\rangle + |1\rangle_{AH}|\tau_{11}\rangle)|1\rangle_{BH} \\ = |00\rangle_{ABH}|\tau_{00}\rangle + |10\rangle_{ABH}|\tau_{01}\rangle + |01\rangle_{ABH}|\tau_{10}\rangle + |11\rangle_{ABH}|\tau_{11}\rangle \\ = |\phi^+\rangle(|\tau_{00}\rangle + |\tau_{11}\rangle) + |\phi^-\rangle(|\tau_{00}\rangle - |\tau_{11}\rangle) + (|\psi^+\rangle - |\psi^-\rangle)|\tau_{01}\rangle + (|\psi^+\rangle + |\psi^-\rangle)|\tau_{10}\rangle \end{array}, \tag{14}$$

As can be seen from the above equation, Eve's attacks must meet the following conditions in order to remain undetected

$$|\tau_{01}\rangle + |\tau_{10}\rangle = 0, \tag{15}$$

$$|\tau_{00}\rangle - |\tau_{11}\rangle = 0. \tag{16}$$

Therefore, for the particles from $|W\rangle$, Eve cannot obtain any information from the state of the auxiliary particle, because its state is independent of the state of the other particles.

For a particle in the $|W\rangle$, U_W represents unitary operations performed on qubits.

$$U_W|0\rangle_{AW} = |0\rangle_{AW}|\tau_{00}\rangle + |1\rangle_{AW}|\tau_{01}\rangle, \tag{17}$$

$$U_W|1\rangle_{AW} = |0\rangle_{AW}|\tau_{10}\rangle + |1\rangle_{AW}|\tau_{11}\rangle, \tag{18}$$

At this point, the whole system can be described as

$$\begin{array}{l} |W\rangle = \frac{1}{\sqrt{3}}(|0\rangle_{AW}|\tau_{00}\rangle + |1\rangle_{AW}|\tau_{01}\rangle)|01\rangle_{BTW} + (|0\rangle_{AW}|\tau_{00}\rangle + |1\rangle_{AW}|\tau_{01}\rangle)|10\rangle_{BTW} \\ +(|0\rangle_{AW}|\tau_{10}\rangle + |1\rangle_{AW}|\tau_{11}\rangle)|00\rangle_{BTW} \\ = \frac{1}{\sqrt{3}}\left(\begin{array}{c} |01\rangle_{ABW}|\tau_{00}\rangle|0\rangle_{TW} + |11\rangle_{ABW}|\tau_{01}\rangle|0\rangle_{TW} + |00\rangle_{ABW}|\tau_{00}\rangle|1\rangle_{TW} \\ +|00\rangle_{ABW}|\tau_{10}\rangle|0\rangle_{TW} + |10\rangle_{ABW}|\tau_{01}\rangle|1\rangle_{TW} + |10\rangle_{ABW}|\tau_{11}\rangle|0\rangle_{TW} \end{array} \right) \\ = \frac{1}{\sqrt{6}}\left[\begin{array}{c} ((|\phi^+\rangle + |\phi^-\rangle)_{ABW}|\tau_{00}\rangle + (|\psi^+\rangle - |\psi^-\rangle)_{ABW}|\tau_{01}\rangle)|1\rangle_{TW} \\ +(|\psi^+\rangle + |\psi^-\rangle)_{ABW}|\tau_{00}\rangle + (|\phi^+\rangle - |\phi^-\rangle)_{ABW}|\tau_{01}\rangle + \\ (|\psi^+\rangle + |\psi^-\rangle)_{ABW}|\tau_{11}\rangle|0\rangle_{TW} + (|\phi^+\rangle + |\phi^-\rangle)_{ABW}|\tau_{10}\rangle \end{array} \right] \end{array}, \tag{19}$$

Therefore, in order for Eve to pass eavesdropping detection, it needs to meet

$$|\tau_{00}\rangle = |\tau_{01}\rangle = |\tau_{01}\rangle = |\tau_{11}\rangle = 0. \tag{20}$$

However, Eve will not be able to distinguish between Alice's measurements and will not be able to obtain useful information.

4.3. Inside Attack

Without loss of generality, Bob is a dishonest actor, assuming he is trying to obtain Alice's privacy while making a private comparison with her. Bob may take any attack form of the external attacker to obtain information. Unlike the external attacker, Bob has the same key K_{AB} with Alice, so as long as he can obtain the correct K_{AT}, he can really get the private information. However, in this case, he cannot obtain the correct and valid K_{AT}, If Bob takes a measurement re-transmission attack to obtain K, Bob has no way of knowing what specific operation Alice has chosen. Alice has a $1/2$ probability of measuring the quantum state, so once Bob returns all the intercepted S_A, there is a $1/2$ probability of choosing the wrong operation. At this time, the interception detection rate is $1/4$, so the sequence's interception detection rate is $1 - \left(\frac{3}{4}\right)^n$, When n is large enough, the eavesdropping detection rate will approach 1.

On the other hand, if Bob tries to attack by measuring re-transmissions or entanglement measurements, he will be regarded as an external attacker. As analyzed in Sections 4.2.2 and 4.2.3, any attack strategy will inevitably introduce a certain error rate and fail to obtain any information.

4.4. Efficiency Analysis

The SQPC protocol efficiency calculation method is proposed in [24], which can be described as

$$\eta = \frac{c}{q+b}, \tag{21}$$

where the c represents the classical particle of comparison, q represents the total qubits used for exchange, and b represents the qubit used by the two participants.

The SQPC protocol uses a three-particle pure state for privacy comparisons. TP prepared 12 qubits and sent them to two participants. When Alice and Bob measured the particles, they each prepared 1 qubit. Hence the scheme of efficiency is

$$\eta = \frac{1}{12+2} \approx 0.07143 \tag{22}$$

Here, as shown in Table 2, a comparison table of schemes is given to show the preponderance of this work in the following.

Table 2. The comparison of related work.

SQPC Protocol	Ref. [8]	Ref. [11]	Ref. [9]	Ref. [10]	Our Scheme
Quantum states	Bell	Single photon	GHZ	GHZ-like	W-state
Consumption of key sharing	0	$16n$	$24n$	0	0
Consumption of comparison	$160n$	$24n$	$8n$	$32n$	$14n$
Consumption of communication	$160n$	$40n$	$32n$	$32n$	$14n$
Qubit efficiency	0.625%	2.5%	3.125%	3.125%	7.134%

Compared with the previous scheme, the proposed scheme does not require pre-shared keys, and does not consume resources for key sharing; moreover, it improves qubit efficiency.

5. Conclusions

A secure and efficient SQPC protocol based on W-state is proposed. Two classic participants can compare the equality of their private information with the help of a semi-honest assistant named TP. Alice and Bob cannot know each other's privacy information, and the semi-honest third-party TP cannot obtain any privacy information compared between Alice and Bob. The proposed protocol can resist attacks and guarantee high efficiency and a high interception detection rate. Moreover, it doubles the bit efficiency of previous protocols.

Author Contributions: Conceptualization, J.L.; methodology, J.Y.; validation, J.L., J.Y. and Z.W.; formal analysis, C.Y.; investigation, F.C.; writing—original draft preparation, J.L. and Z.W.; writing—review and editing, J.Y.; visualization, J.L.; supervision, J.L.; project administration, J.Y.; funding acquisition, J.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Key Research and Development Program of Ningxia Hui Autonomous Region, grant number "2021BEG02007" and the Open Research Fund of Key Laboratory of Cryptography of Zhejiang Province, grant number "No. ZCL21006".

Institutional Review Board Statement: Not applicable.

Data Availability Statement: The data that support the findings of this study are available from the corresponding author upon reasonable request.

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

References

1. Yao, A.C. Protocols for secure computations. In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science, Chicago, IL, USA, 3–5 November 1982; IEEE: Piscataway, NJ, USA, 1982; pp. 160–164.
2. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on Foundation of Computer Science, Washington, DC, USA, 20–22 November 1994; IEEE: Piscataway, NJ, USA, 1994; pp. 124–134.
3. Grover, L.K. Quantum mechanics helps in searching for a needle in a haystack. *Phys. Rev. Lett.* **1997**, *79*, 325. [CrossRef]
4. Hughes, R.J.; Alde, D.M.; Dyer, P.; Luther, G.G.; Morgan, G.L.; Schauer, M. Quantum cryptography. *Contemp. Phys.* **1995**, *36*, 149–163. [CrossRef]
5. Nielsen, M.A.; Chuang, I.L. *Quantum Computation and Quantum Information*; Cambridge University Press: Cambridge, UK, 2000.
6. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2001**, *74*, 145–195. [CrossRef]
7. Chou, W.H.; Hwang, T.; Gu, J. Semi-quantum private comparison protocol under an almost-dishonest third party. *arXiv* **2016**, arXiv:1607.07961v2.
8. Li, Z.; Liu, T.; Zhu, H. Private Comparison Protocol for Multiple Semi-Quantum Users Based on Bell States. *Int. J. Theor. Phys.* **2022**, *61*, 177. [CrossRef]
9. Yan, L.L.; Zhang, S.B.; Chang, Y.; Sheng, Z.; Sun, Y. Semi-quantum key agreement and private comparison protocols using Bell states. *Int. J. Theor. Phys.* **2019**, *58*, 3852–3862. [CrossRef]
10. Tian, Y.; Li, J.; Chen, X.B.; Ye, C.Q.; Li, C.-Y.; Hou, Y.-Y. An efficient semi-quantum private comparison without pre-shared keys. *Quantum Inf. Process.* **2021**, *20*, 360. [CrossRef]
11. Ye, T.Y.; Ye, C.Q. Measure-resend semi-quantum private comparison without entanglement. *Int. J. Theor. Phys.* **2018**, *57*, 3819–3834. [CrossRef]
12. Thapliyal, K.; Sharma, R.D.; Pathak, A. Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. *Int. J. Quantum Inf.* **2018**, *16*, 1850047. [CrossRef]
13. Lang, Y.F. Semi-quantum private comparison using single photons. *Int. J. Theor. Phys.* **2018**, *57*, 3048–3055.
14. Lin, P.H.; Hwang, T.; Tsai, C.W. Efficient semi-quantum private comparison using single photons. *Quantum Inf. Process.* **2019**, *18*, 207. [CrossRef]
15. Tian, Y.; Li, J.; Ye, C.Q.; Chen, X.B.; Li, C.Y. W-state-based semi- quantum private comparison. *Int. J. Theor. Phys.* **2022**, *61*, 18. [CrossRef]
16. Wang, B.; Liu, S.Q.; Gong, L.H. Semi-quantum private comparison protocol of size relation with d-dimensional GHZ states. *Chin. Phys. B* **2022**, *231*, 010302. [CrossRef]
17. Geng, M.J.; Xu, T.J.; Chen, Y.; Ye, T.-Y. Semi-quantum private comparison of size relationship based on d-level single-particle states. *arXiv* **2022**, arXiv:2201.04787.
18. He, Z.; Lou, X. Security analysis and improvement in a semi-quantum private comparison without pre-shared key. *Quantum. Inf. Process.* **2023**, *22*, 150. [CrossRef]
19. Gong, L.; Chen, Z.; Qin, L.; Huang, J.-H. Robust Multi-Party Semi-Quantum Private Comparison Protocols with Decoherence-Free States against Collective Noises. *Adv. Quantum Technol.* **2023**, *6*, 2300097. [CrossRef]
20. Lian, Y.; Li, X.; Ye, T. Multi-party quantum private comparison of size relationship with two third parties based on -dimensional Bell states. *Phys. Scr.* **2023**, *98*, 035011. [CrossRef]
21. Miller, F. *Telegraphic Code to Insure Privacy and Secrecy in the Transmission of Telegrams*; Bookouture: London, UK, 1882.
22. Bellovin, S.M.; Frank, M. Inventor of the One-Time Pad. *Cryptologia* **2011**, *35*, 203–222. [CrossRef]

23. Shannon, C.E. Communication theory of secrecy systems. *Bell Syst. Tech. J.* **1949**, *28*, 656–715. [CrossRef]
24. Cabello, A. Quantum key distribution in the Holevo limit. *Phys. Rev. Lett.* **2000**, *85*, 5635. [CrossRef] [PubMed]

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