sensors

MDPI

Article

Authenticated Semi-Quantum Key Distribution Protocol Based on W States

Hung-Wen Wang [1], Chia-Wei Tsai [2], Jason Lin [3] and Chun-Wei Yang [1,*]

[1] Master Program for Digital Health Innovation, College of Humanities and Sciences, China Medical University, No. 100, Sec. 1, Jingmao Rd., Beitun Dist., Taichung 406040, Taiwan; u109217001@cmu.edu.tw
[2] Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, No. 129, Sec. 3, Sanmin Rd., North Dist., Taichung 40401, Taiwan; cwtsai@nttu.edu.tw
[3] Department of Computer Science and Engineering, National Chung Hsing University, No. 145, Xingda Rd., South Dist., Taichung 40227, Taiwan; jasonlin@nchu.edu.tw
* Correspondence: cwyang@mail.cmu.edu.tw

Abstract: In 2019, Wen et al. proposed authenticated semi-quantum key distribution (ASQKD) for identity and message using the teleportation of W states and GHZ-like states without pre-shared keys. However, the ASQKD protocol presents a vital issue in the teleportation of W states owing to its inappropriate design. Bob recovers the teleported W states without obtaining the position of the corresponding photons and then returns the recovered photons back to Alice. Hence, the teleportation of W states in Wen et al.'s ASQKD protocol was malfunctioning. Moreover, Wen et al.'s ASQKD protocol requires quantum memory, which strongly disobeys the definition of semi-quantum proposed by Boyer et al. Therefore, in this study, we discover the flaws of Wen et al.'s ASQKD protocol and propose an authenticated semi-quantum key distribution protocol. When compared to Wen et al.'s ASQKD protocol, the proposed ASQKD protocol has the following advantages: legal semi-quantum environment (i.e., does not require quantum memory), reduced quantum hardware requirement (i.e., based only on W states), does not involve classical cryptography (i.e., the hash function), and provided 1.6 times higher qubit efficiency.

Keywords: authentication; semi-quantum key distribution; w state; quantum cryptography

check for updates

Citation: Wang, H.-W.; Tsai, C.-W.; Lin, J.; Yang, C.-W. Authenticated Semi-Quantum Key Distribution Protocol Based on W States. *Sensors* **2022**, *22*, 4998. https://doi.org/10.3390/s22134998

Academic Editor: Javier R. Fonollosa

Received: 19 May 2022
Accepted: 30 June 2022
Published: 2 July 2022

1. Introduction

To ensure security, applications perform encryption techniques to secure data. Mainstream encryption based on prime factorization mostly relies on public-key cryptography to distribute secured keys. However, in 1994, Shor [1] proposed a quantum algorithm for determining the prime factors of an integer in polynomial time, which revealed the insecurity of popular public-key cryptography (PKC) systems, such as RSA encryption. This revelational breakthrough indicated the unsafe cryptography of classical computers and led to the research on quantum cryptography. Thus, the design of a protocol that can withstand quantum computer attacks has become an important topic in quantum cryptography.

In 1984, Bennett and Brassard proposed the first quantum key distribution (QKD) protocol based on single photons [2]. The QKD protocols distribute keys between two participants based on quantum mechanics. Participants can detect eavesdropping during transmission by using quantum states. Eventually, a secret key is shared using quantum and authenticated classical channels. QKD protocols have been adapted to various versions based on different security and environmental issues. Since then, researchers conducted research on quantum cryptography (i.e., quantum secure direct communication [3–7] and quantum secret sharing [8–12]). However, QKD protocols assume an authenticated classical channel between Alice and Bob (i.e., the transmitted classical messages can be eavesdropped upon but not modified). If an authenticated classical channel does not exist between Alice and Bob, then QKD protocols can suffer from an impersonation attack. Mutual identity authentication is required to prevent impersonation attacks in QKD protocols. Therefore, authenticated QKD (AQKD) protocols [13–15] have been proposed to circumvent these security problems.

However, the AQKD protocols [13–15] mentioned above typically assume that both participants possess full quantum capabilities. Quantum hardware, which is prohibitively expensive, is still in the development phase. Hence, assuming that all participants have full quantum capabilities is not practical. In light of this, in 2007, Boyer et al. [16] proposed the semi-quantum key distribution (SQKD) protocol. Boyer et al. [17] defined an environment that involves two types of users: suppose one user (Alice) obtains full quantum capabilities, and another user (Bob) retains classical capabilities with limited quantum capabilities. Bob can perform three operations by the following abilities: (1) measuring qubits in Z-basis (i.e., $\{|0\rangle, |1\rangle\}$); (2) preparing Z-basis qubits; (3) using delay line to reorder qubits; and (4) reflecting qubits without any disturbance. Boyer et al. [17] defined two schemes for SQKD protocols: randomization-based and measure-resend. In the randomization SQKD protocol, Bob can perform (1) Z-basis measurement, (3) reordering qubits through delay lines, and (4) reflecting qubits without any disturbance. In the measure-resend SQKD protocol, Bob can perform (1) Z-basis measurements, (2) prepare Z-basis qubits, and (4) reflect qubits without any disturbance. After the proposal, miscellaneous protocols have been applied within a "semi" environment. For example, SQKD protocols [18–28], semi-quantum secret sharing protocols [29–39], semi-quantum secure direct communication [40–49], semi-quantum key agreement [50–53], and semi-quantum private comparison [54–58].

In 2014, Yu et al. [59] presented the first authenticated semi-quantum key distribution (ASQKD) protocol that does not require authenticated classical channels. By pre-sharing a master secret key between two communicants, a sender with advanced quantum devices can transmit a working key to a receiver who can only perform classical operations. The concept of ASQKD enables the establishment of a key hierarchy in security systems that also eases key management problems. In 2016, Li et al. [60] presented two advanced ASQKD protocols. When compared with Yu et al.'s [59] ASQKD protocols, the proposed protocols ensure better qubit efficiency and require fewer pre-shared keys. In 2016, Meslouhi and Hassouni [61] identified a vulnerability that allows a malicious person to recover a partial master key and launch a successful man-in-the-middle attack. In 2020, Tsai and Yang [62] proposed a lightweight authenticated semi-quantum key distribution (LASQKD) protocol. By pre-sharing a master key and adopting a one-way communication strategy, the proposed protocol allows a quantum user and classical user to share secret keys without using an authenticated classical channel or a Trojan horse detection device. In 2020, Zwbboudj et al. [63] presented a new ASQKD protocol without entanglement, which can realize higher security than the schemes of Yu et al. [59] and Li et al. [60]. The proposed scheme is also simpler and demands less advanced quantum devices than ASQKD schemes that use entanglement. In 2021, Chang et al. [64] proposed a new measure-resend ASQKD protocol. The proposed ASQKD protocol uses only single photons, requires fewer pre-shared keys, and provides better qubit efficiency than state-of-the-art ASQKD protocols. However, an eavesdropper can launch a reflective attack to forge the receiver's identity without being detected. In addition, Chang et al.'s ASQKD protocol assumes an authenticated classical channel between the sender and the receiver. It is considered illogical to have an authenticated channel in the ASQKD protocol. Therefore, in 2022, Wang et al. [65] proposed an efficient and secure ASQKD protocol to circumvent these problems using only single photons.

In 2019, Wen et al. [66] proposed a authenticated semi-quantum key distribution for message and identity based on W state and GHZ-like state. Wen et al.'s ASQKD protocol exhibits the following advantages when compared to other related protocols:

(1) It reduces the quantum hardware equipment when compared to other ASQKD protocols.
(2) It does not require pre-share keys.
(3) Wen et al. demonstrated that the proposed ASQKD protocol is robust against typical attacks.
(4) It is highly efficient than some of the existing ASQKD protocols.

Although Wen et al.'s ASQKD protocol is highly efficient and secure, in this study, we discover the design flaws of Wen et al.'s ASQKD protocol as follows: (1.) Wen et al.'s ASQKD protocol is impossible to execute. In Wen et al.'s ASQKD protocol, Bob recovers the teleportation of W states without obtaining the positions of the corresponding qubits. Theoretically, Alice and Bob cannot perform a security check on the transmission qubits because Bob is unable to perform teleportation of the W state appropriately. (2.) Wen et al.'s ASQKD protocol requires quantum memory, which strongly disobeys the semi-quantum definition of Boyer et al. [17]. Hence, in this study, we propose an ASQKD protocol based only on the W states. When compared to Wen et al.'s ASQKD protocol [66], the proposed ASQKD protocol has several advantages.

1. The proposed ASQKD protocol ensures the procedure is functional.
2. The proposed ASQKD protocol does not require quantum memory and legally fulfills a semi-quantum environment [17].
3. The proposed ASQKD protocol, based on W states, only reduces the quantum hardware requirements.
4. The qubit efficiency of the proposed ASQKD protocol is 1.6 times higher than that of Wen et al.'s ASQKD protocol.
5. The proposed ASQKD protocol does not require classical cryptography (i.e., the hash function), which does not show the potential menace of the advance quantum computing.

The remainder of this paper is organized as follows. Section 2 provides a review of Wen et al.'s ASQKD protocol. Section 3 describes the security issues associated with Wen et al.'s ASQKD protocol. Section 4 describes the proposed measure-resend ASQKD protocol. Section 5 presents security analysis. Section 6 presents efficiency analysis. Finally, conclusions of the study are stated in Section 7.

2. Review of Wen et al.'s ASQKD Protocol

Wen et al.'s ASQKD protocol, based on W states and GHZ-like states, allows quantum user Alice and classical user Bob to authenticate messages and identities mutually within the semi-quantum environment. In Wen et al.'s ASQKD protocol, Alice possesses all quantum capabilities, whereas Bob is treated as a classical user who can only perform measurements on a Z-basis, preparing Z-basis qubits, and reflecting qubits without disturbing. To initiate the protocol, Alice and Bob must pre-share a secret specific bases set, $\{|\kappa^+\rangle, |\kappa^-\rangle, |\gamma^+\rangle, |\gamma^-\rangle\}$. Alice and Bob mark these four bases. When Alice measures the qubits, she announces the notation $(\{\kappa^+, \kappa^-, \gamma^+, \gamma^-\})$ as opposed to the quantum basis to Bob. Alice and Bob determine the notation. They notify each other of the changes according to one binary string. The binary string includes nine numbers. The first number denotes the order of change, sequential or reverse. The remaining numbers indicate the notation and corresponding bases. The corresponding notation changes after each successful authentication process. Eventually, Alice will send the state string $|Y\rangle$, and the authentication information to Bob. $|Y\rangle$ will be conveyed by teleportation of W state. Wen et al.'s ASQKD protocol is as follows:

Step W1. Alice prepares n GHZ-like states as shown in Equation (1) and divides these states into three sequences: S_a, S_b, S_c. Every photon in S_a represents all the first particles in GHZ-like states, and S_b and S_c represent all the second and third particles in GHZ-like states. Then, she inserts random decoy states $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ into S_a and obtains S'_a as follows:

$$\begin{aligned} |G\rangle_{abc} &= \tfrac{1}{2}(|001\rangle + |010\rangle + |100\rangle + |111\rangle)_{abc} \\ &= \tfrac{1}{2}(|0\rangle_a|\psi^+\rangle_{bc} + |1\rangle_a|\phi^+\rangle_{bc}) \end{aligned} \tag{1}$$

Alice prepares $2n$ W states, as in Equation (2), and divides these states into three sequences: S_1, S_2, S_3. Photons in S_1 include all the first particles in the W state. Similarly, S_2 and S_3 include all the second and third particles in the W state.

$$|W\rangle_{123} = \frac{1}{2}\Big(|100\rangle + |010\rangle + \sqrt{2}|001\rangle\Big) \tag{2}$$

Suppose one of the four W bases is selected as follows:

$$|\kappa^{\pm}\rangle = \frac{1}{2}\Big(|010\rangle + |001\rangle \pm \sqrt{2}|100\rangle\Big) \tag{3}$$

$$|\gamma^{\pm}\rangle = \frac{1}{2}\Big(|110\rangle + |101\rangle \pm \sqrt{2}|000\rangle\Big) \tag{4}$$

These bases are utilized to measure W states' first and second particles ($|W\rangle_{12}$) and a single particle m, $|\varphi\rangle_m = (\alpha|0\rangle + \beta|1\rangle)_m$. Then, the measurement result is as follows:

$$\begin{aligned}
&|\varphi\rangle_{\mathrm{m}}|W\rangle_{123}\\
&= (\alpha|0\rangle + \beta|1\rangle)_{\mathrm{m}} \otimes \tfrac{1}{2}(|100\rangle{+}|010\rangle + \sqrt{2}|001\rangle)_{123}\\
&= \tfrac{1}{2}[\alpha(|010\rangle{+}|001\rangle)_{\mathrm{m12}}|0\rangle_3 + \sqrt{2}\alpha|000\rangle_{\mathrm{m12}}|1\rangle_3\\
&+\beta(|110\rangle{+}|101\rangle)_{\mathrm{m12}}|0\rangle_3 + \sqrt{2}\beta|100\rangle_{\mathrm{m12}}|1\rangle_3]\\
&= \tfrac{1}{2}[|\kappa^{+}\rangle_{\mathrm{m12}}\,(\alpha|0\rangle + \beta|1\rangle)_3 + |\kappa^{-}\rangle_{\mathrm{m12}}(\alpha|0\rangle - \beta|1\rangle)_3\\
&+|\gamma^{+}\rangle_{\mathrm{m12}}(\alpha|1\rangle + \beta|0\rangle)_3 + |\gamma^{-}\rangle_{\mathrm{m12}}(-\alpha|0\rangle + \beta|1\rangle)_3)
\end{aligned}$$

Eventually, Alice sends S'_a and S_3 to Bob.

Step W2. Alice encodes state string $|Y\rangle$ according to the specific coding rule (see also Table 1), generates a binary message string $L = \{L_i|i = 1, 2, \ldots, 2n.\}$, then recodes the binary string L according to the following rules: binary message {0,1} recodes into the Z-basis $\{|0\rangle, |1\rangle\}$. Eventually, Alice obtains the new particle string $|\varphi_L\rangle = \{|\varphi_{L_j}\rangle \mid j = 1,\ 2,\ \ldots, 2n.\}$. Alice performs W-basis measurement on $(|Y\rangle,\ |S_1\rangle,\ |S_2\rangle)$ and $(|\varphi_L\rangle,\ |S_1\rangle,\ |S_2\rangle)$ and performs Bell measurement on $(|S_b\rangle, |S_c\rangle)$. Then, Alice can obtain the measurement results MR_Y, MR_L, MR_{Bell}, respectively. Alice informs Bob of the measurement results via a classical channel. It should be noted that MR_Y, MR_L is presented in notation format $\{|\kappa^+\rangle, |\kappa^-\rangle, |\gamma^+\rangle, |\gamma^-\rangle\}$.

Table 1. Coding rule of generating L.

$\lvert Y\rangle$=$\lvert 0\rangle$	$\lvert Y\rangle$=$\lvert 1\rangle$	$\lvert Y\rangle$=$\lvert +\rangle$	$\lvert Y\rangle$=$\lvert -\rangle$
$L = 00$	$L = 01$	$L = 10$	$L = 11$

Step W3. Bob receives the measurement results, MR_Y, MR_L from Alice. He can perform the unitary operation on S_3 to recover the states $|Y\rangle$ and $|\varphi_L\rangle$ based on the measurement result MR_Y, MR_L. Bob measures $|\varphi_L\rangle$ in S_3 using a Z-basis. Then, he records the measurement results as $M_3 = \{m_3^1, m_3^2, \ldots\ldots, m_3^{2n}\}$. According to the notation and the measurement result of M_3, Bob applies the corresponding coding rule and obtains $M'_3 = \left\{m'^1_3,\ m'^2_3, \ldots,\ m'^{2n}_3\right\}$ as shown in Table 2 below.

Table 2. Coding rule of generating M'_3.

	m_3=0	m_3=1
κ^+	$m'_3 = 0$	$m'_3 = 1$
κ^-	$m'_3 = 0$	$m'_3 = 1$
γ^+	$m'_3 = 1$	$m'_3 = 0$
γ^-	$m'_3 = 1$	$m'_3 = 0$

Step W4. Bob obtains $|Y\rangle$ and M_3' and returns $|Y'\rangle$ based on M_3'. If $M_3' = 00$ or $M_3' = 01$, then he measures $|Y\rangle$ in the Z-basis, prepares the same photon as $|Y'\rangle$, and resends it back to Alice. If $M_3' = 10$ or $M_3' = 11$, then Bob returns $|Y\rangle$ as $|Y'\rangle$ directly to Alice. Furthermore, Alice checks the received decoy states using the correct corresponding basis.

Step W5. Alice measures $|Y'\rangle$ on the correct basis and checks if $|Y'\rangle$ equals to the original $|Y\rangle$. Alice then announces the position of $|\varphi_L\rangle$ and decoy photons in S_a' to Bob via the classical channel. According to this announcement, Bob removes the decoy state in S_a' and recovers sequence S_a. Then, Bob measures S_a on the Z-basis to check its correlation with MR_{Bell}.

Step W6. Based on the measurement results of S_a, Bob generates binary string $L_B = \left\{ L_{B_j} \,|j = 1,\, 2,\, \ldots,\, 2n \right\}$ according to the following coding rules: if the measurement result is $|0\rangle$, then he encodes $L_{B_j} = 00$. Furthermore, while the measurement result is $|1\rangle$, he encodes $L_{B_j} = 01$. Bob hashes L_B to obtain the hash value $H(L_B)$. Bob then sends $H(L_B)$ to Alice.

Step W7. Alice calculates $H(L)$ and checks if $H(L_B)$ equals $H(L)$.

3. Security Issues in Wen et al.'s ASQKD Protocol

Wen et al.'s ASQKD protocol proved security analysis under popular attacks. However, the protocol suffers from vital flaws in the procedure. Hence, it can be considered as a malfunctioning protocol. Moreover, the protocol requires classical Bob to equip quantum memory, which strongly disobeys the principle of the semi-quantum environment as stated by Boyer et al. [17]. The issues in the teleportation of W states and quantum environment are described as follows.

3.1. Teleportation of W States in Wen et al.'s ASQKD Protocol

In Wen et al.'s ASQKD protocol, teleportation of W states between Alice and Bob is a vital procedure flaw. In Step W1, Bob receives S'_a and S_3 from Alice. In Step W3, Bob recovers corresponding photons in S_3 into $|Y\rangle$ and $|\varphi_L\rangle$ based on MR_Y, MR_L, and the measurement result of S_3. In Step W4, Bob returns $|Y'\rangle$ to Alice. It should be noted that Alice announces the position of $|\varphi_L\rangle$ in Step W5, and it is inferred that Bob does not obtain any position of $|Y\rangle$ and $|\varphi_L\rangle$ in line with S_3 in Step W3. This implies that the insufficient information on the corresponding position of $|Y\rangle$ and $|\varphi_L\rangle$ cannot allow Bob to distinguish between $|Y\rangle$ and $|\varphi_L\rangle$. Thus, Bob cannot perform any recovery in Step W3, which eventually leads to the failure of the teleportation of W states. Hence, Wen et al.'s ASQKD protocol teleportation of W states cannot be performed under all circumstances.

3.2. Quantum Environment Issue in Wen et al.'s ASQKD Protocol

In Wen et al.'s ASQKD protocol, Alice sends photons (S_a' and S_3) to Bob in Step W1, and Bob obtains all received photons. Then, Bob receives the measurement results from Alice in Step W2. In Step W4, Bob performs corresponding unitary operations on each photon in S_3, recovers S_3 into $|Y\rangle$ and $|\varphi_L\rangle$ based on MR_Y, MR_L, and the measurement result of S_3, respectively. Eventually, Bob returns $|Y'\rangle$ to Alice. The interval between receiving the photons (Step W1), measuring the S_3 photon sequence, calculating and performing the recovery based on notations and measurement results (Step W3), and returning $|Y'\rangle$ based on M_3' (Step W4) obviously requires quantum memory to store the photons for performing all the procedures until resending back to Alice. Hence, the classical Bob in Wen et al.'s ASQKD protocol is equipped with quantum memory, which strongly disobeys the definition of a semi-quantum environment [17].

4. Proposed Measure-Resend ASQKD Protocol

The proposed ASQKD protocol ensures that the quantum environment fulfills the definition of semi-quantum, which was defined by Boyer et al. [17] by using W states only. Assume that Alice is a quantum user and Bob is a classical user with limited quantum capabilities. Alice and Bob pre-share three binary keys, $K_1, K_2 K_3$. Specifically, K_1 determines the initial state of the prepared W state and K_2 represents measure-resending or reflecting photons. K_3 determines the photon to be the check sequence or key sequence. Figure 1 illustrates the proposed scheme. The steps involved in the proposed ASQKD protocol are as follows:

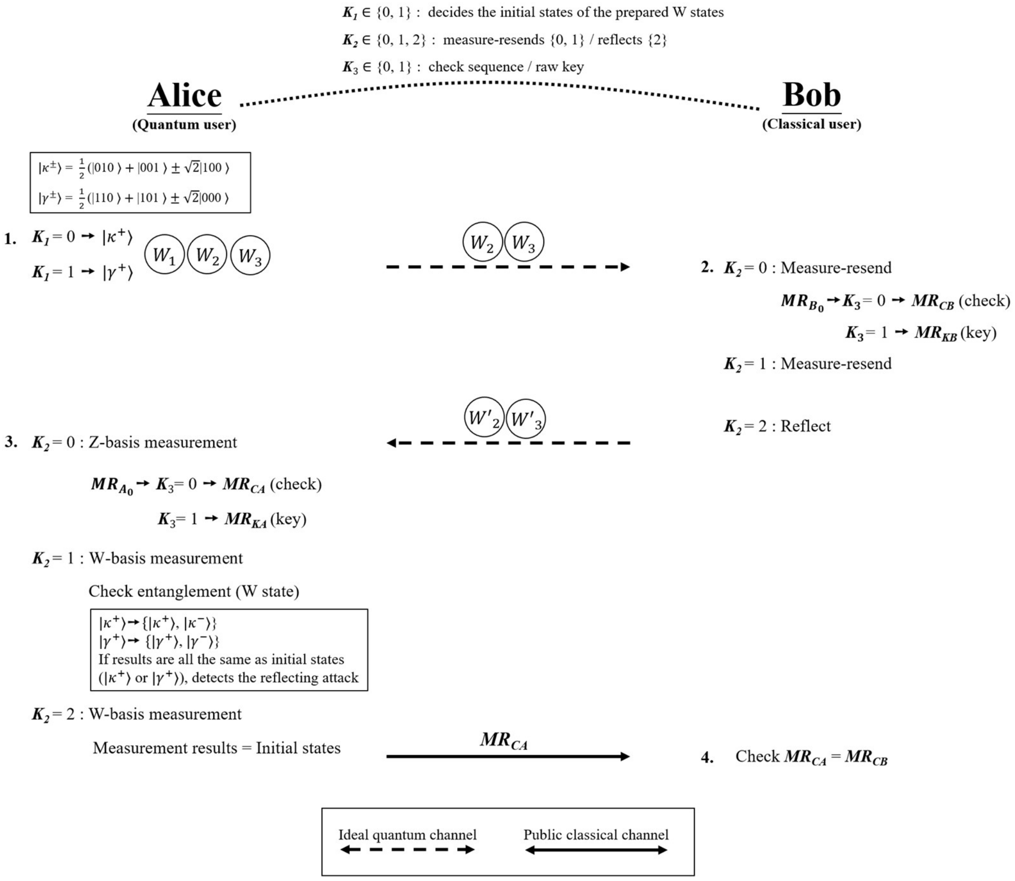
$K_1 \in \{0, 1\}$: decides the initial states of the prepared W states
$K_2 \in \{0, 1, 2\}$: measure-resends {0, 1} / reflects {2}
$K_3 \in \{0, 1\}$: check sequence / raw key
Alice
(Quantum user)
Bob
(Classical user)
$|\kappa^{\pm}\rangle = \frac{1}{2}(|010\rangle + |001\rangle \pm \sqrt{2}|100\rangle)$
$|\gamma^{\pm}\rangle = \frac{1}{2}(|110\rangle + |101\rangle \pm \sqrt{2}|000\rangle)$
1. $K_1 = 0 \rightarrow |\kappa^+\rangle$
$K_1 = 1 \rightarrow |\gamma^+\rangle$
W_1 W_2 W_3
W_2 W_3
2. $K_2 = 0$: Measure-resend
$MR_{B_0} \rightarrow K_3 = 0 \rightarrow MR_{CB}$ (check)
$K_3 = 1 \rightarrow MR_{KB}$ (key)
$K_2 = 1$: Measure-resend
W'_2 W'_3
$K_2 = 2$: Reflect
3. $K_2 = 0$: Z-basis measurement
$MR_{A_0} \rightarrow K_3 = 0 \rightarrow MR_{CA}$ (check)
$K_3 = 1 \rightarrow MR_{KA}$ (key)
$K_2 = 1$: W-basis measurement
Check entanglement (W state)
$|\kappa^+\rangle \rightarrow \{|\kappa^+\rangle, |\kappa^-\rangle\}$
$|\gamma^+\rangle \rightarrow \{|\gamma^+\rangle, |\gamma^-\rangle\}$
If results are all the same as initial states
($|\kappa^+\rangle$ or $|\gamma^+\rangle$), detects the reflecting attack
$K_2 = 2$: W-basis measurement
Measurement results = Initial states
MR_{CA}
4. Check $MR_{CA} = MR_{CB}$
Ideal quantum channel
Public classical channel

Figure 1. Proposed ASQKD protocol.

Step 1. Alice prepares the initial W states based on K_1. If $K_1 = 0$, then Alice prepares $|\kappa^+\rangle$, and while $K_1 = 1$, she prepares $|\gamma^+\rangle$. Alice then divides the W states into three sequences: W_1, W_2, and W_3. W_1 represents all the first particles of W states. Similarly, W_2 and W_3 represent all the second and third particles of W states, respectively. Alice sends W_2 and W_3 to Bob one photon at a time.

Step 2. For every received photon, Bob performs measure-resending or reflects photons based on K_2.

- If $K_2 = 0$, then Bob measures the received photon on a Z-basis, prepares the same photon as the measurement result, and resends it to Alice. For the measured sequence at $K_2 = 0$, if $K_3 = 0$, then Bob records the measurement results to the check sequence MR_{CB}; if $K_3 = 1$, then Bob records the measurement results to the key sequence MR_{KB}.
- If $K_2 = 1$, then Bob measures the received photon on a Z-basis, prepares the same photon as the measurement result, and resends it to Alice.
- If $K_2 = 2$, then Bob reflects the received photon back to Alice without any influence.

Step 3. Alice receives W'_2 and W'_3 from Bob. She performs Z-basis or W-basis measurements based on K_2.

- If $K_2 = 0$, then Alice performs a Z-basis measurement and classifies it into two measured sequences based on K_3. If $K_3 = 0$, then Alice records the measurement results as a check sequence MR_{CA}, whereas if $K_3 = 1$, Alice records the measurement results to the key sequence MR_{KA}.

- If $K_2 = 1$, then Alice performs a W-basis measurement to check the entanglement correlation of the W states. Hence, according to the uncertainty principle, if the initial state is $|\kappa^+\rangle$ or $|\gamma^+\rangle$, then the measured states should collapse into $\{|\kappa^+\rangle, |\kappa^-\rangle\}$ or $\{|\gamma^+\rangle, |\gamma^-\rangle\}$. Otherwise, if the states remain the same as the initial state, then it is inferred that Bob does not measure the photons and Alice will detect that the protocol may suffer from the reflecting attack.
- If $K_2 = 2$, then Alice performs a W-basis measurement for the eavesdropping check. Alice compares the measurement results with the initial states. This implies that if the states remain the same as the original states, neither Bob nor Eve measure the photons, proving the security of the transmission.

After the eavesdropping check, Alice announces MR_{CA} to Bob.

Step 4. Bob checks if $MR_{CA} = MR_{CB}$ to secure the channel. Eventually, Alice and Bob share a raw key as the measurement result of MR_{KA}, MR_{KB} (i.e., if one measures $|00\rangle, |01\rangle, |10\rangle, |11\rangle$, represents classical bits "00", "01", "10", "11", respectively.). Then, they perform a privacy amplification process [67,68] on the raw key to distill the private key.

5. Security Analysis

In this section, the security of the proposed ASQKD protocol is analyzed with respect to the five main attacks.

5.1. Impersonation Attack

5.1.1. Assume Eve Essayed to Impersonate Alice

Suppose Eve attempts to impersonate Alice. In Step 1, Eve may generate photon sequences, E_2 and E_3, to impersonate the photons sent by Alice, W_2 and W_3. Bob receives E_2 and E_3, performs the measure-resend mode or the reflected mode based on K_2, obtains MR_{CB} and MR_{KB}. In Step 4, Alice announces the check sequence MR_{CA}. After Bob receives it, he verifies Alice by collating the check sequence with MR_{CB}. Bob detects eavesdropping because $MR_{CB} \neq MR_{CA}$. Eve cannot impersonate any check sequence MR_{CA} because it was generated based on K_3, which was previously pre-shared privately. Hence, Eve cannot successfully impersonate Alice in the proposed ASQKD protocol.

5.1.2. Assume Eve Essayed to Impersonate Bob

Suppose that Eve attempts to impersonate Bob. Eve may generate photons E_2' and E_3' to impersonate W_2' and W_3'. In Step 3, Alice performs an eavesdropping check. She measured E_2' and E_3' to check the entanglement of the W states. According to the uncertainty principle, if $K_2 = 1$, then the measure-resend photons should collapse into $\{|\kappa^+\rangle, |\kappa^-\rangle\}$ or $\{|\gamma^+\rangle, |\gamma^-\rangle\}$; if $K_2 = 2$, then the reflected state should be the same as the initial state. Thus, if the states are not related to the correct procedure based on K_2, then Alice detects impersonation of Eve.

5.2. Reflecting Attack

If Eve tries to perform the reflecting attack, then Eve may intercept the photon sequences W_2 and W_3 in Step 1 and subsequently resend the same photons back to Alice (i.e., W_2 and W_3). For every received photon in W_2 and W_3, Alice performs an eavesdropping check in Step 3 based on K_2. If Bob measure-resends W_2 and W_3, then the state should collapse into $\{|\kappa^+\rangle, |\kappa^-\rangle\}$ or $\{|\gamma^+\rangle, |\gamma^-\rangle\}$ according to the uncertainty principle. As mentioned, the photon sequence W_2 and W_3 is reflected by Eve and not measured by Bob, which does not collapse into $\{|\kappa^+\rangle, |\kappa^-\rangle\}$ or $\{|\gamma^+\rangle,|\gamma^-\rangle\}$. From the perspective of Alice, if the state remains in the same state as the initial state, then she can infer that Bob does not measure any photons and Alice detects that the protocol is suffering from the reflecting attack.

5.3. Man-in-the-Middle Attack

Assume that Eve attempts to perform a man-in-the-middle attack on the transmitted photon between Alice and Bob. In Step 1, Eve may intercept W_2 and W_3, in which the initial states of W states are $\{|\kappa^+\rangle, |\gamma^+\rangle\}$. Then, Eve measures W_2 and W_3 to obtain the information, and eventually, Eve generates photon sequences E_2 and E_3 based on the measurement results and sends them to Bob. It should be noted that the photon sequence E_2 and E_3 collapses into the random state $\{|\kappa^+\rangle, |\kappa^-\rangle\}$ or $\{|\gamma^+\rangle, |\gamma^-\rangle\}$. In Step 2, Bob measure-resends or reflects E_2 and E_3 based on K_2, namely E_2' and E_3'. After receiving E_2' and E_3', Alice proceeds with an eavesdropping check. If Eve can pass the eavesdropping check in Step 3, then she is able to successfully perform a man-in-the-middle attack. However, without knowing the pre-shared key K_2, Eve cannot compute the check sequence for the reflected photons. Once Eve measures W_2 and W_3, it can successfully pass the eavesdropping check with a probability of 1/2. Hence, the probability of Eve being detected in the proposed ASQKD protocol is $1-\left(\frac{1}{2}\right)^{\frac{n}{3}}$. While n is large enough, the detection probability is approximately 100%. Thus, in Step 3, Alice detects that the ASQKD protocol is attacked by Eve in Step 3.

5.4. Collective Attack

This section proves the proposed ASQKD protocol is immune to collective attack and does not show leakage if there is no error detected.

In the attack scheme, let Eve obtains all quantum abilities and gains the control of quantum channels. Eve may try to eavesdrop on private information from Alice and Bob through the collective attack. To initiate the attack, Eve prepares a probe qubit $|E_1\rangle$ and operates a unitary operation on the joint state $|q\rangle$, the qubits which transmit through the quantum channel. Eve performs the U_1 operation in Step 1, Eve entangles the probe qubits with the traveling qubit which sent by Alice. Then, Eve performs the U_2 operation in Step 2 and entangles the probe qubits with the transmitting qubit which is resent by Bob.

Theorem 1. *Eve can operate the collective attack to eavesdrop on private information without being detected. To initiate the attack, Eve performs the first unitary operation U_1 operation on the qubits sent by Alice. Then, Eve performs the second unitary operation U_2 operation on the qubits which are resent by Bob. However, no operation can provide Eve to deduce the private information without being detected.*

Proof of Theorem 1. Assume Eve operates a unitary operator to eavesdrop on the qubit sent from Alice in Step 1 by U_1, the possibilities are presented as follows:

$$\begin{gathered}
U_1(|00\rangle\otimes|E_1\rangle)=a_0|00\rangle|g_{A0}\rangle+a_1|01\rangle|g_{A1}\rangle+a_2|10\rangle|g_{A2}\rangle+a_3|11\rangle|g_{A3}\rangle\\
U_1(|01\rangle\otimes|E_1\rangle)=b_0|00\rangle|h_{A0}\rangle+b_1|01\rangle|h_{A1}\rangle+b_2|10\rangle|h_{A2}\rangle+b_3|11\rangle|h_{A3}\rangle\\
U_1(|10\rangle\otimes|E_1\rangle)=c_0|00\rangle|i_{A0}\rangle+c_1|01\rangle|i_{A1}\rangle+c_2|10\rangle|i_{A2}\rangle+c_3|11\rangle|i_{A3}\rangle\\
U_2(|00\rangle\otimes|E_1\rangle)=d_0|00\rangle|j_{A0}\rangle+d_1|01\rangle|j_{A1}\rangle+d_2|10\rangle|j_{A2}\rangle+d_3|11\rangle|j_{A3}\rangle\\
U_2(|01\rangle\otimes|E_1\rangle)=e_0|00\rangle|k_{A0}\rangle+e_1|01\rangle|k_{A1}\rangle+e_2|10\rangle|k_{A2}\rangle+e_3|11\rangle|k_{A3}\rangle\\
U_2(|10\rangle\otimes|E_1\rangle)=f_0|00\rangle|l_{A0}\rangle+f_1|01\rangle|l_{A1}\rangle+f_2|10\rangle|l_{A2}\rangle+f_3|11\rangle|l_{A3}\rangle
\end{gathered}$$

The initial state of Eve's probe qubit denotes $|E_i\rangle$. $|g_{A0}\rangle, |g_{A1}\rangle, |g_{A2}\rangle, |g_{A3}\rangle, |h_{A0}\rangle, |h_{A1}\rangle, |h_{A2}\rangle, |h_{A3}\rangle, |i_{A0}\rangle, |i_{A1}\rangle, |i_{A2}\rangle, |i_{A3}\rangle, |j_{A0}\rangle, |j_{A1}\rangle, |j_{A2}\rangle, |j_{A3}\rangle, |k_{A0}\rangle, |k_{A1}\rangle, |k_{A2}\rangle, |k_{A3}\rangle, |l_{A0}\rangle, |l_{A1}\rangle, |l_{A2}\rangle$ and $|l_{A3}\rangle$ are distinguished by Bob, where

$$\begin{aligned}
|a_0|^2+|a_1|^2+|a_2|^2+|a_3|^2 &= |b_0|^2+|b_1|^2+|b_2|^2+|b_3|^2=|c_0|^2+|c_1|^2+|c_2|^2+|c_3|^2\\
&= |d_0|^2+|d_1|^2+|d_2|^2+|d_3|^2=|e_0|^2+|e_1|^2+|e_2|^2+|e_3|^2\\
&= |f_0|^2+|f_1|^2+|f_2|^2+|f_3|^2=1
\end{aligned}$$

To demonstrate the attack clearly, assume Alice chooses $|k^+\rangle=\frac{1}{2}\left(|010\rangle+|001\rangle+\sqrt{2}|100\rangle\right)$ as the initial state. It should be noted that the choice of initial state does not affect the security analysis. Suppose Eve performs the U_1 operation, the possibilities are described as follows:

$$\begin{aligned}
U_1(|k^+\rangle_{ABC}\otimes|E_1\rangle) &= \tfrac{1}{2}\begin{pmatrix}
|0\rangle_A\otimes(c_0|00\rangle_{BC}|i_{A0}\rangle+c_1|01\rangle_{BC}|i_{A1}\rangle+c_2|10\rangle_{BC}|i_{A2}\rangle+c_3|11\rangle_{BC}|i_{A3}\rangle)+\\
|0\rangle_A\otimes(b_0|00\rangle|h_{A0}\rangle+b_1|01\rangle|h_{A1}\rangle+b_2|10\rangle|h_{A2}\rangle+b_3|11\rangle|h_{A3}\rangle)+\\
\sqrt{2}(|1\rangle_A\otimes(a_0|00\rangle_{BC}|g_{A0}\rangle+a_1|01\rangle_{BC}|g_{A1}\rangle+a_2|10\rangle_{BC}|g_{A2}\rangle+a_3|11\rangle_{BC}|g_{A3}\rangle))
\end{pmatrix}\\
&= \tfrac{1}{2}((c_0|000\rangle_{ABC}|i_{A0}\rangle+c_1|001\rangle_{ABC}|i_{A1}\rangle+c_2|010\rangle_{ABC}|i_{A2}\rangle+c_3|011\rangle_{ABC}|i_{A3}\rangle)\\
&\quad +(b_0|000\rangle_{ABC}|h_{A0}\rangle+b_1|001\rangle_{ABC}|g_{A1}\rangle+b_2|010\rangle_{ABC}|g_{A2}\rangle+b_3|011\rangle_{ABC}|g_{A3}\rangle)\\
&\quad +\sqrt{2}(a_0|100\rangle_{ABC}|g_{A0}\rangle+a_1|101\rangle_{ABC}|g_{A1}\rangle+a_2|110\rangle_{ABC}|g_{A2}\rangle+a_3|111\rangle_{ABC}|g_{A3}\rangle)))\\
&= \tfrac{1}{2}\begin{pmatrix}
|000\rangle_{ABC}\otimes(c_0|i_{A0}\rangle+b_0|h_{A0}\rangle))+\\
|001\rangle_{ABC}\otimes(c_1|i_{A1}\rangle+b_1|g_{A1}\rangle)+\\
|010\rangle_{ABC}\otimes(c_2|i_{A2}\rangle+b_2|g_{A2}\rangle)+\\
|011\rangle_{ABC}\otimes(c_3|i_{A3}\rangle+b_3|g_{A3}\rangle)+\\
\sqrt{2}(|100\rangle_{ABC}\otimes(a_0|g_{A0}\rangle)+\\
|101\rangle_{ABC}\otimes(a_1|g_{A1}\rangle)+\\
|110\rangle_{ABC}\otimes(a_2|g_{A2}\rangle)+\\
|111\rangle_{ABC}\otimes(a_3|g_{A3}\rangle))
\end{pmatrix}
\end{aligned}$$

Bob performs Z-basis measurement on the received qubits and saves the measurement results MR_{CB} based on K_2. If the qubits are modified, MR_{CB} will be altered and detected by Bob. Hence, the attack is assumed not to modify the value of the Z-basis qubits to pass the eavesdropping check. The restriction limits the possibilities of U_1 as follows:

$$U_1\big(|k^+\rangle_{ABC}\otimes|E_1\rangle\big)=\frac{1}{2}\begin{pmatrix}
|001\rangle_{ABC}\otimes(c_1|i_{A1}\rangle+b_1|g_{A1}\rangle)+\\
|010\rangle_{ABC}\otimes(c_2|i_{A2}\rangle+b_2|g_{A2}\rangle)+\\
\sqrt{2}(|100\rangle_{ABC}\otimes(a_0|g_{A0}\rangle)
\end{pmatrix}$$

Then, Eve performs the second unitary operation U_2 on the qubits that are resent by Bob. The possibilities are described as follows:

$$\begin{aligned}
U_2U_1(|k^+\rangle_{ABC}\otimes|E_1\rangle) &= \tfrac{1}{2}\begin{pmatrix}
|0\rangle_A\otimes(e_0|00\rangle|k_{A0}\rangle+e_1|01\rangle|k_{A1}\rangle+e_2|10\rangle|k_{A2}\rangle+e_3|11\rangle|k_{A3}\rangle)\otimes(c_1|i_{A1}\rangle+b_1|g_{A1}\rangle)+\\
|0\rangle_A\otimes(f_0|00\rangle|l_{A0}\rangle+f_1|01\rangle|l_{A1}\rangle+f_2|10\rangle|l_{A2}\rangle+f_3|11\rangle|l_{A3}\rangle)\otimes(c_2|i_{A2}\rangle+b_2|g_{A2}\rangle)+\\
\sqrt{2}(|1\rangle_A\otimes d_0|00\rangle|j_{A0}\rangle+d_1|01\rangle|j_{A1}\rangle+d_2|10\rangle|j_{A2}\rangle+d_3|11\rangle|j_{A3}\rangle\otimes(a_0|g_{A0}\rangle))
\end{pmatrix}\\
&= \tfrac{1}{2}\begin{pmatrix}
(e_0|000\rangle_{ABC}|k_{A0}\rangle+e_1|001\rangle_{ABC}|k_{A1}\rangle+e_2|010\rangle_{ABC}|k_{A2}\rangle+e_3|011\rangle_{ABC}|k_{A3}\rangle)\otimes(c_1|i_{A1}\rangle+b_1|g_{A1}\rangle)+\\
(f_0|000\rangle_{ABC}|l_{A0}\rangle+f_1|001\rangle_{ABC}|l_{A1}\rangle+f_2|010\rangle_{ABC}|l_{A2}\rangle+f_3|011\rangle_{ABC}|l_{A3}\rangle)\otimes(c_2|i_{A2}\rangle+b_2|g_{A2}\rangle)+\\
\sqrt{2}(d_0|100\rangle_{ABC}|j_{A0}\rangle+d_1|101\rangle_{ABC}|j_{A1}\rangle+d_2|110\rangle_{ABC}|j_{A2}\rangle+d_3|111\rangle_{ABC}|j_{A3}\rangle\otimes(a_0|g_{A0}\rangle))
\end{pmatrix}\\
&= \tfrac{1}{2}\begin{pmatrix}
(e_0|000\rangle_{ABC}|k_{A0}\rangle c_1|i_{A1}\rangle+e_1|001\rangle_{ABC}|k_{A1}\rangle c_1|i_{A1}\rangle+e_2|010\rangle_{ABC}|k_{A2}\rangle c_1|i_{A1}\rangle+e_3|011\rangle_{ABC}|k_{A3}\rangle c_1|i_{A1}\rangle)+\\
(e_0|000\rangle_{ABC}|k_{A0}\rangle b_1|g_{A1}\rangle+e_1|001\rangle_{ABC}|k_{A1}\rangle b_1|g_{A1}\rangle+e_2|010\rangle_{ABC}|k_{A2}\rangle b_1|g_{A1}\rangle+e_3|011\rangle_{ABC}|k_{A3}\rangle b_1|g_{A1}\rangle)\\
(f_0|000\rangle_{ABC}|l_{A0}\rangle c_2|i_{A2}\rangle+f_1|001\rangle_{ABC}|l_{A1}\rangle c_2|i_{A2}\rangle+f_2|010\rangle_{ABC}|l_{A2}\rangle c_2|i_{A2}\rangle+f_3|011\rangle_{ABC}|l_{A3}\rangle c_2|i_{A2}\rangle)+\\
(f_0|000\rangle_{ABC}|l_{A0}\rangle b_2|g_{A2}\rangle+f_1|001\rangle_{ABC}|l_{A1}\rangle b_2|g_{A2}\rangle+f_2|010\rangle_{ABC}|l_{A2}\rangle b_2|g_{A2}\rangle+f_3|011\rangle_{ABC}|l_{A3}\rangle b_2|g_{A2}\rangle)+\\
\sqrt{2}(d_0|100\rangle_{ABC}|j_{A0}\rangle a_0|g_{A0}\rangle+d_1|101\rangle_{ABC}|j_{A1}\rangle a_0|g_{A0}\rangle+d_2|110\rangle_{ABC}|j_{A2}\rangle a_0|g_{A0}\rangle+d_3|111\rangle_{ABC}|j_{A3}\rangle a_0|g_{A0}\rangle))
\end{pmatrix}\\
&= \tfrac{1}{2}\begin{pmatrix}
|000\rangle_{ABC}\otimes(e_0|k_{A0}\rangle c_1|i_{A1}\rangle+e_0|k_{A0}\rangle b_1|g_{A1}\rangle+f_0|l_{A0}\rangle c_2|i_{A2}\rangle+f_0|l_{A0}\rangle b_2|g_{A2}\rangle)+\\
|001\rangle_{ABC}\otimes(e_1|k_{A1}\rangle c_1|i_{A1}\rangle+e_1|k_{A1}\rangle b_1|g_{A1}\rangle+f_1|l_{A1}\rangle c_2|i_{A2}\rangle+f_1|l_{A1}\rangle b_2|g_{A2}\rangle)+\\
|010\rangle_{ABC}\otimes(e_2|k_{A2}\rangle c_1|i_{A1}\rangle+e_2|k_{A2}\rangle b_1|g_{A1}\rangle+f_2|l_{A2}\rangle c_2|i_{A2}\rangle+f_2|l_{A2}\rangle b_2|g_{A2}\rangle)+\\
|011\rangle_{ABC}\otimes(e_3|k_{A3}\rangle c_1|i_{A1}\rangle+e_3|k_{A3}\rangle b_1|g_{A1}\rangle+f_3|l_{A3}\rangle c_2|i_{A2}\rangle+f_3|l_{A3}\rangle b_2|g_{A2}\rangle)+\\
\sqrt{2}(|100\rangle_{ABC}\otimes(d_0|j_{A0}\rangle a_0|g_{A0}\rangle)+\\
|101\rangle_{ABC}\otimes(d_1|j_{A1}\rangle a_0|g_{A0}\rangle)+\\
|110\rangle_{ABC}\otimes(d_2|j_{A2}\rangle a_0|g_{A0}\rangle)+\\
|111\rangle_{ABC}\otimes(d_3|j_{A3}\rangle a_0|g_{A0}\rangle)
\end{pmatrix}
\end{aligned}$$

Alice receives the photons which are resent by Bob and performs the eavesdropping check. If the quantum state is not equal to W states, Alice will detect the attack. To pass the eavesdropping check, suppose $e_0|k_{A0}\rangle c_1|i_{A1}\rangle+e_0|k_{A0}\rangle b_1|g_{A1}\rangle+f_0|l_{A0}\rangle c_2|i_{A2}\rangle+f_0|l_{A0}\rangle b_2|g_{A2}\rangle$ $=e_3|k_{A3}\rangle c_1|i_{A1}\rangle+e_3|k_{A3}\rangle b_1|g_{A1}\rangle+f_3|l_{A3}\rangle c_2|i_{A2}\rangle+f_3|l_{A3}\rangle b_2|g_{A2}\rangle=d_1|j_{A1}\rangle a_0|g_{A0}\rangle$ $=d_2|j_{A2}\rangle a_0|g_{A0}\rangle=d_3|j_{A3}\rangle a_0|g_{A0}\rangle=\vec{0}$. Hence, it is assumed that the attack cannot modify the value of the Z-basis photons. With the restriction mentioned above, limits U_2 possibilities as follows:

$$U_2U_1\left(|k^+\rangle_{ABC}\otimes|E_1\rangle\right)=\frac{1}{2}\begin{pmatrix}|001\rangle_{ABC}\otimes(e_0|k_{A0}\rangle c_1|i_{A1}\rangle+e_0|k_{A0}\rangle b_1|g_{A1}\rangle+f_0|l_{A0}\rangle c_2|i_{A2}\rangle+f_0|l_{A0}\rangle b_2|g_{A2}\rangle)+\\|010\rangle_{ABC}\otimes(e_2|k_{A2}\rangle c_1|i_{A1}\rangle+e_2|k_{A2}\rangle b_1|g_{A1}\rangle+f_2|l_{A2}\rangle c_2|i_{A2}\rangle+f_2|l_{A2}\rangle b_2|g_{A2}\rangle)+\\\sqrt{2}(|100\rangle_{ABC}\otimes(d_0|j_{A0}\rangle a_0|g_{A0}\rangle)\end{pmatrix}$$

Suppose Eve wants to pass the eavesdropping check, Eve must set all the measurement result of probe qubits $|E_1\rangle$ to be equal (i.e., $e_0|k_{A0}\rangle c_1|i_{A1}\rangle+e_0|k_{A0}\rangle b_1|g_{A1}\rangle+f_0|l_{A0}\rangle c_2|i_{A2}\rangle$ $+f_0|l_{A0}\rangle b_2|g_{A2}\rangle=e_2|k_{A2}\rangle c_1|i_{A1}\rangle+e_2|k_{A2}\rangle b_1|g_{A1}\rangle+f_2|l_{A2}\rangle c_2|i_{A2}\rangle+f_2|l_{A2}\rangle b_2|g_{A2}\rangle$ $=d_0|j_{A0}\rangle a_0|g_{A0}\rangle$)). Without altering $|k^+\rangle_{ABC}$, Eve can pass the eavesdropping check. In contrast, Eve cannot distinguish the corresponding measurement result of $|E_1\rangle$. Hence, Eve cannot deduce any useful information. On the other hand, suppose Eve wants to deduce the information from the measurement result of probe qubits $|E_1\rangle$, Eve must set all the measurement results of probe qubits $|E_1\rangle$ not to be equal, so Eve can distinguish the corresponding result. In contrast, Eve will get detected by the eavesdropping check because the value of $|k^+\rangle_{ABC}$ is altered. Thus, the proposed ASQKD protocol is proven to be immune to the collective attack. □

5.5. Key Leakage Problem

Assume Eve tries to eavesdrop on the raw key from the traveling qubits. Eve may perform Z-basis measurement on the photon sequence sent by Alice, W_2 and W_3. Eve obtains the measurement results of W_2 and W_3 (i.e., $|00\rangle, |01\rangle, |10\rangle, |11\rangle$), which implies the raw key (i.e., "00", "01", "10", "11"). Suppose Shannon entropy is defined as $E=-\Sigma_i \rho i \log_2 \rho i$, where ρi denotes probability distribution. The entropy E_1 can be computed as $E_1=-4\times\frac{1}{4}\log_2\frac{1}{4}=2$ bits. However, the protocol provides an eavesdropping check, which limits the possibility of the measurement results of W_2 and W_3 being used as the raw key, hence the probability is $\frac{1}{4}$ (i.e., Bob receives W_2 and W_3 and performs measure-resend or reflect based on K_2. If $K_2=0$, Bob records the measurement results as MR_{CB} or MR_{KB}. If $K_2=1$ or 2, Bob measure-resend or reflect for eavesdropping check. Assume Alice and Bob consume half of the transmitted photons as eavesdropping check, hence $K_2=0$ and $K_2=1$ or 2 consume each half of the measurement results. While in $K_2=0$, the measurement results of $K_3=0$ denote as check bit, $K_3=1$ denote as key bit, thus half of the $K_2=0$ measurement results are used as sharing raw key. Eventually, the probability of Eve eavesdrops the raw key from the measurement results of W_2 and W_3 is $\frac{1}{2}\times\frac{1}{2}=\frac{1}{4}$). Hence, the entire entropy denotes $\frac{1}{4}\times E_1=0.5$ bit. Even though Eve can obtain 0.5 bit by performing eavesdropping, eventually the attack will be detected by an eavesdropping check. Even if Eve passes the eavesdropping check, one can still perform the privacy amplification process [67,68] on the transmitted information to distill the private key, avoiding the key leakage problem. Thus, Eve cannot obtain any private key under an eavesdropping attack.

6. Efficiency Analysis

Table 3 provides a comparison of the Yu et al. [59], Li et al. [60], Zebboudj et al. [63], Chang et al. [64], and Wang et al. [65], and Wen et al.'s [66] measure-resend ASQKD protocols with the proposed ASQKD protocol. The efficiency of the protocol is calculated using the following equation: $\eta=\frac{c}{q}$, where c denotes the number of shared classical bits and q denotes the sum of consumed qubits. We assume that Alice generates a binary string of length n as the secret key. The length of the hash, decoy photon, and checking bit m is assumed to equal that of the secret key (i.e., n = m).

Table 3. Comparison of [59,60,63–66] and the proposed ASQKD protocol.

	Yu et al.'s ASQKD Protocol [59]	**Li et al.'s ASQKD Protocol [60]**	**Zebboudj et al.'s ASQKD Protocol [63]**	**Chang et al.'s ASQKD Protocol [64]**	**Wang et al.'s ASQKD Protocol [65]**	**Wen et al.'s ASQKD Protocol [66]**	**The Proposed ASQKD Protocol**
Quantum resource	Bell states	Bell states, Single photons	Single photons	Single photons	Single photons	GHZ-like states W states	W states
Qubit efficiency	10%	11%	14%	17%	14%	7%	11%
Required pre-shared keys (in bits)	6n	4n	3n	3n	3n	4n	5n
Classical participant's quantum capabilities	Generate Reflect Measure	Generate Reflect Measure	Generate Reflect Measure	Generate Reflect Measure	Generate Reflect Measure	Generate Reflect Measure Quantum memory	Generate Reflect Measure
Classical participant does not require quantum memory	Yes	Yes	Yes	Yes	Yes	No	Yes
Legal semi-quantum environment	Yes	Yes	Yes	Yes	Yes	No	Yes
The protocol does not require the hash function	Yes	No	No	No	No	No	Yes
Runnable protocol	Yes	Yes	Yes	Yes	Yes	No	Yes
Required classical channel	Yes	Yes	Yes	Yes	No	Yes	Yes
Robustness of the reflecting attack	Yes	Yes	Yes	No	Yes	Yes	Yes

The efficiency analysis of Yu et al., Li et al., Zebboudj et al., Chang et al., and Wang et al.'s ASQKD protocol have been discussed in Wang et al.'s study [65]. For clarity and readability, this study is briefly summarized as follows: the efficiency of Yu et al., Li et al., Zebboudj et al., Chang et al., and Wang et al.'s ASQKD protocol is 10%, 11%, 14%, 17%, 14%, respectively.

In Wen et al.'s ASQKD protocol, Alice generated n GHZ-like states (i.e., $3n$ qubits) and n decoy states. She then generates $3n$ W states (i.e., $9n$ qubits) for teleportation of the state $|Y\rangle$ and decoy state $|\varphi_L\rangle$. Bob measures and generates $|Y'\rangle$ (i.e., n qubits). Thus, the efficiency of the ASQKD protocol proposed by Wen et al. is $\eta = \frac{n}{3n+n+9n+n} = \frac{1}{14} \approx 7\%$.

In the proposed ASQKD protocol, Alice prepares four pairs of W states (i.e., $12n$ qubits), Bob measures the second and third W states and generates three pairs of two single photons (i.e., based on K_0 generates $2n + 2n$ qubits, K_1 generates $2n$ qubits). Eventually, Alice and Bob share a secret key of $2n$ bits. Hence, the efficiency of the proposed ASQKD protocol is $\eta = \frac{2n}{12n+2n+2n+2n} = \frac{1}{9} \approx 11\%$.

The proposed ASQKD protocol improves the malfunction issue in the ASQKD protocol of Wen et al. [66]. As mentioned in Section 3.1, in Wen et al.'s ASQKD protocol, Bob cannot perform the teleportation due to the insufficient information on the corresponding position of $|Y\rangle$ and $|\varphi_L\rangle$. The proposed ASQKD protocol pre-shares keys for the information of the photon's position privately, ensuring that the unfunctional situation with Bob will not occur under all circumstances.

As mentioned in Section 3.2, in Wen et al.'s ASQKD protocol [66], Bob must preserve all photons sent by Alice in Step W1 for the measurements and calculations to perform the teleportation of W states later. This implies that Bob must possess quantum memory, which strongly disobeys the definition of semi-quantum environment [17]. In the proposed ASQKD protocol, Alice sends the photons individually to Bob, and Bob performs measurements or reflects the photons as he receives them. The proposed ASQKD protocol ensures that Bob does not need to equip quantum memory, which is a legal semi-quantum environment.

From the perspective of entangle states applying ASQKD protocols, the proposed ASQKD protocol provided higher qubit efficiency compared to Yu et al. [59] and Li et al. [60]. Although Chang et al. [64] have higher qubit efficiency, their protocol suffers from the reflecting attack [65], the protocol must apply more qubits to secure the channel. Thus, Chang et al. [64] provided lower qubit efficiency than the proposed ASQKD protocol. Zebboudj et al. [63] and Wang [65] take advantages in qubit efficiency, however, the security of those protocols is based on classical cryptography, the mathematics of the hash function. With the advance of quantum computing, powerful quantum computing may be a potential menace to classical cryptography. The proposed protocol does not require the hash function, thus is secured even in the future.

From the perspective of quantum hardware, in Wen et al.'s ASQKD protocol [66], Alice generates GHZ-like states and W states, and Bob equips quantum memory, which requires advanced quantum mechanics. In the proposed ASQKD protocol, Alice generates only W states, and Bob does not require quantum memory, which is more practical. Moreover, the proposed ASQKD protocol has higher efficiency than Wen et al.'s ASQKD protocol.

By combining all the benefits mentioned above, the proposed ASQKD protocol reduces the quantum hardware requirement and elevates the efficiency significantly when equipped with a secure legal semi-quantum environment. When compared to Wen et al.'s ASQKD protocol [66], the proposed ASQKD protocol has several advantages.

1. The proposed ASQKD protocol ensures the procedure is functional.
2. The proposed ASQKD protocol does not require quantum memory and legally fulfills a semi-quantum environment [17].
3. The proposed ASQKD protocol, based on W states, only reduces the quantum hardware requirements.
4. The qubit efficiency of the proposed ASQKD protocol is 1.6 times higher than that of Wen et al.'s ASQKD protocol.

5. The proposed ASQKD protocol does not require classical cryptography (i.e., the hash function), which does not show the potential menace of the advance quantum computing.

7. Conclusions

In this study, several important issues in Wen et al.'s ASQKD protocol were addressed and an improvement was proposed. In 2019, Wen et al. proposed an ASQKD protocol for identity and messages using the teleportation of W states and GHZ-like states without pre-shared keys. However, Wen et al.'s ASQKD protocol exhibits significant design flaws. The teleportation of W states in Wen et al.'s ASQKD protocol was malfunctioning. Moreover, Wen et al.'s ASQKD protocol requires the classical user to equip quantum memory, which strongly disobeys the definition of the semi-quantum environment defined by Boyer et al. Therefore, in this study, we proposed an ASQKD protocol based only on the W states. When compared with Wen et al.'s ASQKD protocol, the proposed ASQKD protocol circumvented the aforementioned flaws and obtained the following advantages: runnable ASQKD protocol, legal semi-quantum environment (i.e., does not require quantum memory), reduced quantum hardware requirement (i.e., based only on W states), does not involve classical cryptography (i.e., the hash function) and provided 1.6 times higher qubit efficiency, which significantly elevated security and efficiency. To obtain a higher efficiency in the ASQKD protocol, further research is required.

Author Contributions: Conceptualization, H.-W.W. and C.-W.Y.; methodology, H.-W.W., C.-W.T., and C.-W.Y.; investigation, J.L. and C.-W.Y.; formal analysis, C.-W.Y.; writing—original draft, H.-W.W. and C.-W.Y.; writing—review and editing, C.-W.T. and C.-W.Y.; project administration, C.-W.Y. All authors have read and agreed to the published version of the manuscript.

Funding: This research was partially supported by the Ministry of Science and Technology, Taiwan, R.O.C. (Grant Nos. MOST 110-2221-E-039-004, MOST 110-2221-E-143-003, MOST 110-2221-E-259-001, MOST 110-2221-E-143-004, MOST 110-2222-E-005-006, MOST 110-2634-F-005-006, and MOST 111-2218-E-005-007-MBK), and China Medical University, Taiwan (Grant Nos. CMU110-S-21 and CMU110-MF-121).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

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

References

1. Shor, P.W. Algorithms for quantum computation: Discrete logarithms and factoring. In Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Los Alamitos, CA, USA, 20–22 November 1994; pp. 124–134.
2. 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, 9–12 December 1984; pp. 175–179.
3. Boström, K.; Felbinger, T. Deterministic Secure Direct Communication Using Entanglement. *Phys. Rev. Lett.* **2002**, *89*, 187902. [CrossRef] [PubMed]
4. Deng, F.-G.; Long, G.; Liu, X.-S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A* **2003**, *68*, 042317. [CrossRef]
5. Man, Z.X.; Zhang, Z.J.; Li, Y. Deterministic secure direct communication by using swapping quantum entanglement and local unitary operations. *Chin. Phys. Lett.* **2005**, *22*, 18–21.
6. Zhang, Z.J.; Jun, L.; Liu, Y.M.; Cao, H.J.; Shi, S.H. Revisiting quantum secure direct communication with W state. *Chin. Phys. Lett.* **2006**, *23*, 2652–2655.
7. Zhang, Z.J.; Yuan, H.; Liu, Y.M.; Zhang, W. Eavesdropping on quantum secure direct communication with W state in noisy channel. *Commun. Theor. Phys.* **2008**, *49*, 103–106.
8. Zhang, Z.J.; Li, Y.; Man, Z.X. Multiparty quantum secret sharing. *Phys. Rev. A* **2005**, *71*, 044301. [CrossRef]
9. Zhang, Z.J.; Man, Z.X. Multiparty quantum secret sharing of classical messages based on entanglement swapping. *Phys. Rev. A* **2005**, *72*, 022303. [CrossRef]
10. Zhang, Z.J.; Liu, Y.M.; Fang, M.; Wang, D. Multiparty quantum secret sharing scheme of classical messages by swapping qudit-state entanglement. *Int. J. Mod. Phys. C* **2007**, *18*, 1885–1901. [CrossRef]

11. Han, L.F.; Liu, Y.M.; Liu, J.; Zhang, Z.J. Multiparty quantum secret sharing of secure direct communication using single photons. *Opt. Commun.* **2008**, *281*, 2690–2694. [CrossRef]
12. Wang, X.; Liu, Y.M.; Han, L.F.; Zhang, Z.J. Multiparty Quantum Secret Sharing of Secure Direct Communication with High-Dimensional Quantum Superdense Coding. *Int. J. Quantum Inf.* **2008**, *6*, 1155–1163. [CrossRef]
13. Zeng, G.H.; Zhang, W.P. Identity verification in quantum key distribution. *Phys. Rev. A* **2000**, *61*, 5. [CrossRef]
14. Hwang, T.; Lee, K.C.; Li, C.M. Provably secure three-party authenticated quantum key distribution protocols. *IEEE Trans. Dependable Secur. Comput.* **2007**, *4*, 71–80. [CrossRef]
15. Shih, H.C.; Lee, K.C.; Hwang, T. New Efficient Three-Party Quantum Key Distribution Protocols. *IEEE J. Sel. Top. Quantum* **2009**, *15*, 1602–1606. [CrossRef]
16. Boyer, M.; Kenigsberg, D.; Mor, T. Quantum Key Distribution with Classical Bob. *Phys. Rev. Lett.* **2007**, *99*, 140501. [CrossRef]
17. Boyer, M.; Gelles, R.; Kenigsberg, D.; Mor, T. Semiquantum key distribution. *Phys. Rev. A* **2009**, *79*, 032341. [CrossRef]
18. Zou, X.; Qiu, D.; Li, L.; Wu, L.; Li, L. Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A* **2009**, *79*, 052312. [CrossRef]
19. Krawec, W.O. Restricted attacks on semi-quantum key distribution protocols. *Quantum Inf. Process.* **2014**, *13*, 2417–2436. [CrossRef]
20. Krawec, W.O. Mediated semiquantum key distribution. *Phys. Rev. A* **2015**, *91*, 032323. [CrossRef]
21. Krawec, W.O. Security of a semi-quantum protocol where reflections contribute to the secret key. *Quantum Inf. Process.* **2016**, *15*, 2067–2090. [CrossRef]
22. Li, Q.; Chan, W.H.; Zhang, S. Semiquantum key distribution with secure delegated quantum computation. *Sci. Rep.* **2016**, *6*, 19898. [CrossRef]
23. Boyer, M.; Katz, M.; Liss, R.; Mor, T. Experimentally feasible protocol for semiquantum key distribution. *Phys. Rev. A* **2017**, *96*, 062335. [CrossRef]
24. Tsai, C.-W.; Yang, C.-W.; Lee, N.-Y. Lightweight mediated semi-quantum key distribution protocol. *Mod. Phys. Lett. A* **2019**, *34*, 1950281. [CrossRef]
25. Wang, M.-M.; Gong, L.-M.; Shao, L.-H. Efficient semiquantum key distribution without entanglement. *Quantum Inf. Process.* **2019**, *18*, 260. [CrossRef]
26. Hajji, H.; El Baz, M. Qutrit-based semi-quantum key distribution protocol. *Quantum Inf. Process.* **2021**, *20*, 4. [CrossRef]
27. Han, S.; Huang, Y.; Mi, S.; Qin, X.; Wang, J.; Yu, Y.; Wei, Z.; Zhang, Z. Proof-of-principle demonstration of semi-quantum key distribution based on the Mirror protocol. *EPJ Quantum Technol.* **2021**, *8*, 28. [CrossRef]
28. Tsai, C.-W.; Yang, C.-W. Lightweight mediated semi-quantum key distribution protocol with a dishonest third party based on Bell states. *Sci. Rep.* **2021**, *11*, 23222. [CrossRef] [PubMed]
29. Li, Q.; Chan, W.H.; Long, D.Y. Semiquantum secret sharing using entangled states. *Phys. Rev. A* **2010**, *82*, 022303. [CrossRef]
30. Gheorghiu, V. Generalized semiquantum secret-sharing schemes. *Phys. Rev. A* **2012**, *85*, 052309. [CrossRef]
31. Li, L.Z.; Qiu, D.W.; Mateus, P. Quantum secret sharing with classical Bobs. *J. Phys. A-Math. Theor.* **2013**, *46*, 045304. [CrossRef]
32. Xie, C.; Li, L.; Qiu, D. A Novel Semi-Quantum Secret Sharing Scheme of Specific Bits. *Int. J. Theor. Phys.* **2015**, *54*, 3819–3824. [CrossRef]
33. Li, Z.; Li, Q.; Liu, C.; Peng, Y.; Chan, W.H.; Li, L. Limited resource semiquantum secret sharing. *Quantum Inf. Process.* **2018**, *17*, 285. [CrossRef]
34. Yin, A.H.; Tong, Y. A novel semi-quantum secret sharing scheme using entangled states. *Mod. Phys. Lett. B* **2018**, *32*, 1850256. [CrossRef]
35. Tsai, C.-W.; Yang, C.-W.; Lee, N.-Y. Semi-quantum secret sharing protocol using W-state. *Mod. Phys. Lett. A* **2019**, *34*, 1950213. [CrossRef]
36. Xiang, Y.; Liu, J.; Bai, M.-q.; Yang, X.; Mo, Z.-w. Limited Resource Semi-Quantum Secret Sharing Based on Multi-Level Systems. *Int. J. Theor. Phys.* **2019**, *58*, 2883–2892. [CrossRef]
37. Li, C.; Ye, C.; Tian, Y.; Chen, X.-B.; Li, J. Cluster-state-based quantum secret sharing for users with different abilities. *Quantum Inf. Process.* **2021**, *20*, 385. [CrossRef]
38. 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]
39. Tsai, C.-W.; Yang, C.-W.; Lin, J. Multiparty mediated quantum secret sharing protocol. *Quantum Inf. Process.* **2022**, *21*, 63. [CrossRef]
40. Zhang, M.-H.; Li, H.-F.; Xia, Z.-Q.; Feng, X.-Y.; Peng, J.-Y. Semiquantum secure direct communication using EPR pairs. *Quantum Inf. Process.* **2017**, *16*, 117. [CrossRef]
41. Xie, C.; Li, L.; Situ, H.; He, J. Semi-quantum Secure Direct Communication Scheme Based on Bell States. *Int. J. Theor. Phys.* **2018**, *57*, 1881–1887. [CrossRef]
42. Yan, L.; Sun, Y.; Chang, Y.; Zhang, S.; Wan, G.; Sheng, Z. Semi-quantum protocol for deterministic secure quantum communication using Bell states. *Quantum Inf. Process.* **2018**, *17*, 315. [CrossRef]
43. Sun, Y.; Yan, L.; Chang, Y.; Zhang, S.; Shao, T.; Zhang, Y. Two semi-quantum secure direct communication protocols based on Bell states. *Mod. Phys. Lett. A* **2019**, *34*, 1950004. [CrossRef]

44. Tao, Z.; Chang, Y.; Zhang, S.; Dai, J.; Li, X. Two Semi-Quantum Direct Communication Protocols with Mutual Authentication Based on Bell States. *Int. J. Theor. Phys.* **2019**, *58*, 2986–2993. [CrossRef]
45. Wang, M.-M.; Liu, J.-L.; Gong, L.-M. Semiquantum secure direct communication with authentication based on single-photons. *Int. J. Quantum Inf.* **2019**, *17*, 1950024. [CrossRef]
46. Rong, Z.; Qiu, D.; Zou, X. Semi-Quantum Secure Direct Communication Using Entanglement. *Int. J. Theor. Phys.* **2020**, *59*, 1807–1819. [CrossRef]
47. Yang, C.-W. Efficient and secure semi-quantum secure direct communication protocol against double CNOT attack. *Quantum Inf. Process.* **2020**, *19*, 50. [CrossRef]
48. Yang, C.-W.; Tsai, C.-W. Advanced semi-quantum secure direct communication protocol based on bell states against flip attack. *Quantum Inf. Process.* **2020**, *19*, 126. [CrossRef]
49. Zhang, X.; Zhou, R.-G. An Efficient and Novel Semi-Quantum Deterministic Secure Quantum Communication Protocol. *Int. J. Theor. Phys.* **2022**, *61*, 94. [CrossRef]
50. Liu, W.-J.; Chen, Z.-Y.; Ji, S.; Wang, H.-B.; Zhang, J. Multi-party Semi-quantum Key Agreement with Delegating Quantum Computation. *Int. J. Theor. Phys.* **2017**, *56*, 3164–3174. [CrossRef]
51. Shukla, C.; Thapliyal, K.; Pathak, A. Semi-quantum communication: Protocols for key agreement, controlled secure direct communication and dialogue. *Quantum Inf. Process.* **2017**, *16*, 295. [CrossRef]
52. Yan, L.; Zhang, S.; Chang, Y.; Sheng, Z.; Yang, F. Mutual semi-quantum key agreement protocol using Bell states. *Mod. Phys. Lett. A* **2019**, *34*, 1950294. [CrossRef]
53. Li, H.-H.; Gong, L.-H.; Zhou, N.-R. New semi-quantum key agreement protocol based on high-dimensional single-particle states. *Chin. Phys. B* **2020**, *29*, 110304. [CrossRef]
54. Ye, T.-Y.; Ye, C.-Q. Measure-Resend Semi-Quantum Private Comparison Without Entanglement. *Int. J. Theor. Phys.* **2018**, *57*, 3819–3834. [CrossRef]
55. Jiang, L.-Z. Semi-quantum private comparison based on Bell states. *Quantum Inf. Process.* **2020**, *19*, 180. [CrossRef]
56. Tsai, C.-W.; Lin, J.; Yang, C.-W. Cryptanalysis and improvement in semi-quantum private comparison based on Bell states. *Quantum Inf. Process.* **2021**, *20*, 120. [CrossRef]
57. Yan, L.; Zhang, S.; Chang, Y.; Wan, G.; Yang, F. Semi-quantum private comparison protocol with three-particle G-like states. *Quantum Inf. Process.* **2021**, *20*, 17. [CrossRef]
58. Tian, Y.; Li, J.; Ye, C.; Chen, X.-B.; Li, C. W-state-based Semi-quantum Private Comparison. *Int. J. Theor. Phys.* **2022**, *61*, 18. [CrossRef]
59. Yu, K.-F.; Yang, C.-W.; Liao, C.-H.; Hwang, T. Authenticated semi-quantum key distribution protocol using Bell states. *Quantum Inf. Process.* **2014**, *13*, 1457–1465. [CrossRef]
60. Li, C.-M.; Yu, K.-F.; Kao, S.-H.; Hwang, T. Authenticated semi-quantum key distributions without classical channel. *Quantum Inf. Process.* **2016**, *15*, 2881–2893. [CrossRef]
61. Meslouhi, A.; Hassouni, Y. Cryptanalysis on authenticated semi-quantum key distribution protocol using Bell states. *Quantum Inf. Process.* **2016**, *16*, 18. [CrossRef]
62. Tsai, C.-W.; Yang, C.-W. Lightweight authenticated semi-quantum key distribution protocol without trojan horse attack. *Laser Phys. Lett.* **2020**, *17*, 075202. [CrossRef]
63. Zebboudj, S.; Djoudi, H.; Lalaoui, D.; Omar, M. Authenticated semi-quantum key distribution without entanglement. *Quantum Inf. Process.* **2020**, *19*, 77. [CrossRef]
64. Chang, C.-H.; Lu, Y.-C.; Hwang, T. Measure-resend authenticated semi-quantum key distribution with single photons. *Quantum Inf. Process.* **2021**, *20*, 272. [CrossRef]
65. Wang, H.-W.; Tsai, C.-W.; Lin, J.; Huang, Y.-Y.; Yang, C.-W. Efficient and Secure Measure-Resend Authenticated Semi-Quantum Key Distribution Protocol against Reflecting Attack. *Mathematics* **2022**, *10*, 1241. [CrossRef]
66. Wen, X.-J.; Zhao, X.-Q.; Gong, L.-H.; Zhou, N.-R. A semi-quantum authentication protocol for message and identity. *Laser Phys. Lett.* **2019**, *16*, 075206. [CrossRef]
67. Bennett, C.H.; Brassard, G.; Robert, J.M. Privacy Amplification by Public Discussion. *SIAM J. Comput.* **1988**, *17*, 210–229. [CrossRef]
68. Bennett, C.H.; Brassard, G.; Crepeau, C.; Maurer, U.M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **1995**, *41*, 1915–1923. [CrossRef]