mathematics

MDPI

Article

Semi-Quantum Identification without Information Leakage

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

[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
[2] Department of Computer Science and Engineering, National Chung Hsing University, No. 145, Xingda Rd., South District, Taichung 40227, Taiwan
[3] 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
* Correspondence: cwtsai@nutc.edu.tw

Abstract: In 2019, Zhou et al. proposed semi-quantum identification (also known as semi-quantum authentication, SQA), which proceeds under a measure-resend and measurement-free environment. However, Zhou et al.'s SQA protocol suffers from severe information leakages. An eavesdropper can obtain an intact authentication key without being detected under this environment. In particular, Zhou et al.'s measure-resend SQA protocol is vulnerable to double *CNOT* attacks, while the measurement-free SQA protocol is vulnerable to man-in-the-middle attacks. Hence, this study reveals the severe security issues of Zhou et al.'s SQA protocol and proposes an improved protocol with guaranteed security. The proposed measure-resend SQA protocol is immune to double *CNOT* attacks. Since the photons sent back and forth are identical, Eve cannot obtain any information by cross-comparing these photons. In the proposed measurement-free SQA protocol, the eavesdropper cannot obtain the order of the transmitted photons because it was previously a pre-shared key to decide the order of the photons. Hence, the proposed measurement-free SQA protocol can withstand man-in-the-middle attacks.

Keywords: authentication; identification; semi-quantum; single photon; quantum cryptography

MSC: 81P94

Citation: Yang, C.-W.; Wang, H.-W.; Lin, J.; Tsai, C.-W. Semi-Quantum Identification without Information Leakage. *Mathematics* **2023**, *11*, 452. https://doi.org/10.3390/math11020452

Academic Editor: Jonathan Blackledge

Received: 22 December 2022
Revised: 11 January 2023
Accepted: 13 January 2023
Published: 14 January 2023

1. Introduction

To increase the convenience of quantum protocols, Boyer et al. [1] proposed a semi-quantum key distribution (SQKD) in 2007. Under this protocol, the abilities of the two participants are specified as follows. Alice, a sender possesses full quantum capabilities, and Bob, the receiver possesses only classical capabilities with limited quantum capabilities. Bob is allowed to perform three of the following operations: (1) Z-basis measurement on qubits (i.e., $\{|0\rangle, |1\rangle\}$), (2) preparing Z-basis qubits, (3) reordering the qubits through delay lines, and (4) reflecting qubits without interference. There are four SQKD protocol schemes: measure-resend, randomization-based, measurement-free, and unitary-operation-based.

In the measure-resend SQKD protocol, Bob performs (1) Z-basis measurements on qubits (i.e., $\{|0\rangle, |1\rangle\}$), (2) preparation of Z-basis qubits, and (4) reflection of qubits without interference. In the randomization-based SQKD protocol, Bob performs (1) Z-basis measurement on qubits, (2) prepares Z-basis qubits, and (3) reorders the qubits through delay lines. In 2015, Zou et al. [2] presented a new measurement-free semiquantum environment. In the measurement-free SQKD protocol, the classical user is allowed to (2) prepare Z-basis qubits, (3) reorder the qubits through delay lines, and (4) reflect qubits without interference. Because the SQKD protocol is practical and novel, it has been further investigated. In 2019, Tsai et al. [3] proposed another semi-quantum environment: a unitary-operation-based protocol. In the unitary-operation-based SQKD protocol, the classical user is allowed to perform (1) Z-basis measurements on qubits and (2) unitary operations.

Although SQKD protocols [4–29] increase the convenience of quantum protocols, the SQKD protocols mentioned above cannot be secured without an authenticated classical channel. In the light of this, Yu et al. [30] proposed the first authenticated semi-quantum key distribution (ASQKD) in 2014, which does not require authenticated classical channels. The concept of ASQKD introduced a key hierarchy in security systems and reduced key management issues. Li et al. [31] proposed two ASQKD protocols in 2016 that required fewer pre-shared keys and provided better communication efficiency. In 2016, Meslouhi and Hassouni [32] discovered that a key can be recovered by a malicious person and is vulnerable to man-in-the-middle attacks. In 2019, Wen et al. [33] proposed a semi-quantum authentication protocol based on GHZ-like states and W states. Wen et al.'s protocol can determine the identities of two participants and ensure the credibility of the important information. Tsai and Yang [34] proposed a lightweight authenticated semi-quantum key-distribution (LASQKD) protocol in 2020. The two communicants pre-shared a master key and applied a one-way communication strategy. The proposed protocol ensures that quantum Alice and classical Bob can share secret keys without using an authenticated channel or a Trojan horse detection device. Chang et al. [35] proposed a new measure-resend ASQKD protocol using single photons in 2021, which requires fewer pre-shared keys and provides better qubit efficiency than the aforementioned ASQKD protocols. In 2022, Wang et al. [36] investigated Chang et al.'s ASQKD protocol when subjected to a reflecting attack and proposed an efficient and secure measure-resend ASQKD protocol against the reflecting attack. In 2022, Wang et al. [37] discover the flaws of Wen et al.'s ASQKD protocol [33] and propose an authenticated semi-quantum key distribution protocol with high qubit efficiency.

In 2019, Zhou et al. [38] proposed semi-quantum identification based on single photons. The proposed protocol includes two semi-environments: the measure-resend and measurement-free environments. Zhou et al.'s SQA protocol has the following advantages:

(1) It minimizes the quantum mechanical burden for classical Bob.
(2) It does not require an authenticated classical channel.
(3) The authentication key can be used circularly.

Although Zhou et al.'s SQA protocol has proven secure [38], this study discovers the severe information leakage it faces in the measure-resend and measurement-free environments. In the measure-resend environment, Eve can obtain the pre-shared key $\boldsymbol{K}$ by performing a double *CNOT* (i.e., controlled NOT gate) attack. In the measurement-free environment, Eve can successfully obtain the pre-shared key K through a man-in-the-middle attack. Hence, in this study, we propose an improved protocol that is immune to all these attacks.

The remainder of this paper is organized as follows. Section 2 presents a review of the SQA protocol proposed by Zhou et al. Section 3 addresses the security issues of Zhou et al.'s SQA protocol. The proposed SQA protocol is described in Section 4. Section 5 presents the security analysis of the proposed SQA protocol. Section 6 presents a performance analysis of the proposed SQA protocol. The paper ends with a conclusion in Section 7.

2. Review of Zhou et al.'s SQA Protocol

Suppose that Alice and Bob pre-share a binary key $\boldsymbol{K} = \{\boldsymbol{K}_1, \boldsymbol{K}_2, \ldots, \boldsymbol{K}_{2n}\}$, where $\boldsymbol{K}_j \in \{00, 01, 10, 11\}$ and $j = 1, 2, \ldots, 2n$. They generate photons based on $\boldsymbol{K}_{2i}$, $\boldsymbol{i} = 1, 2, \ldots, n$. Figures 1 and 2 clearly illustrate Zhou et al.'s measure-resend SQA protocol and measurement-free SQA protocol, respectively.

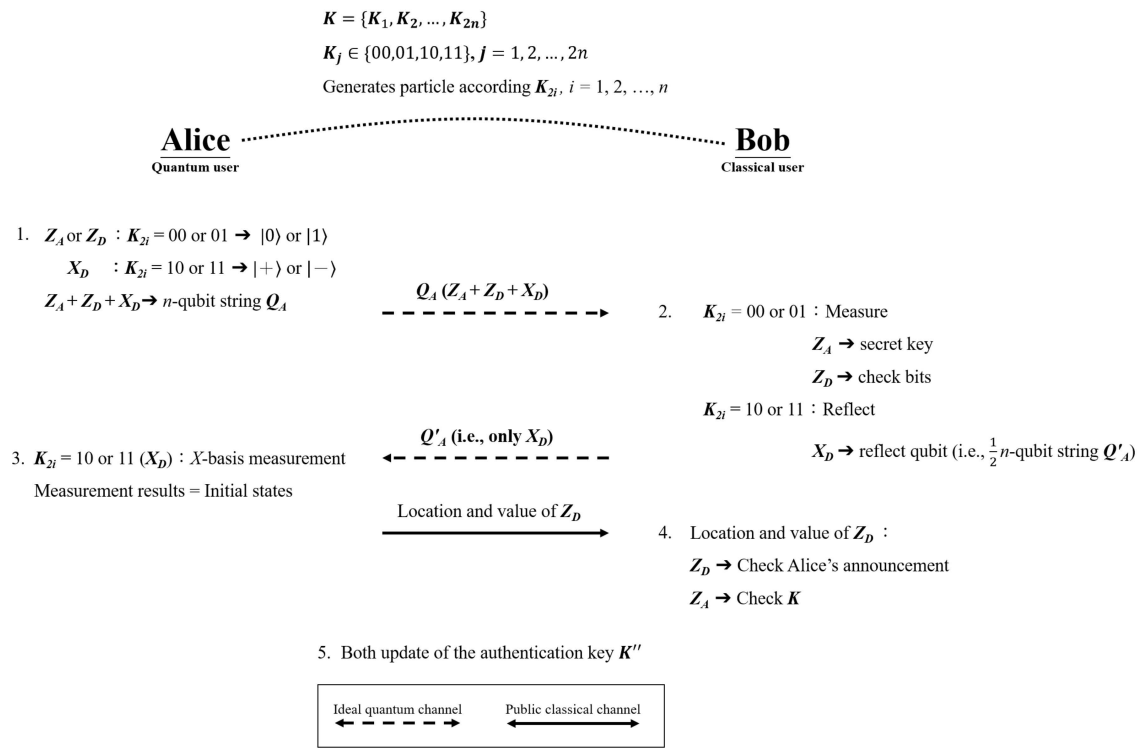

Figure 1. Zhou et al.'s measure-resend SQA protocol.

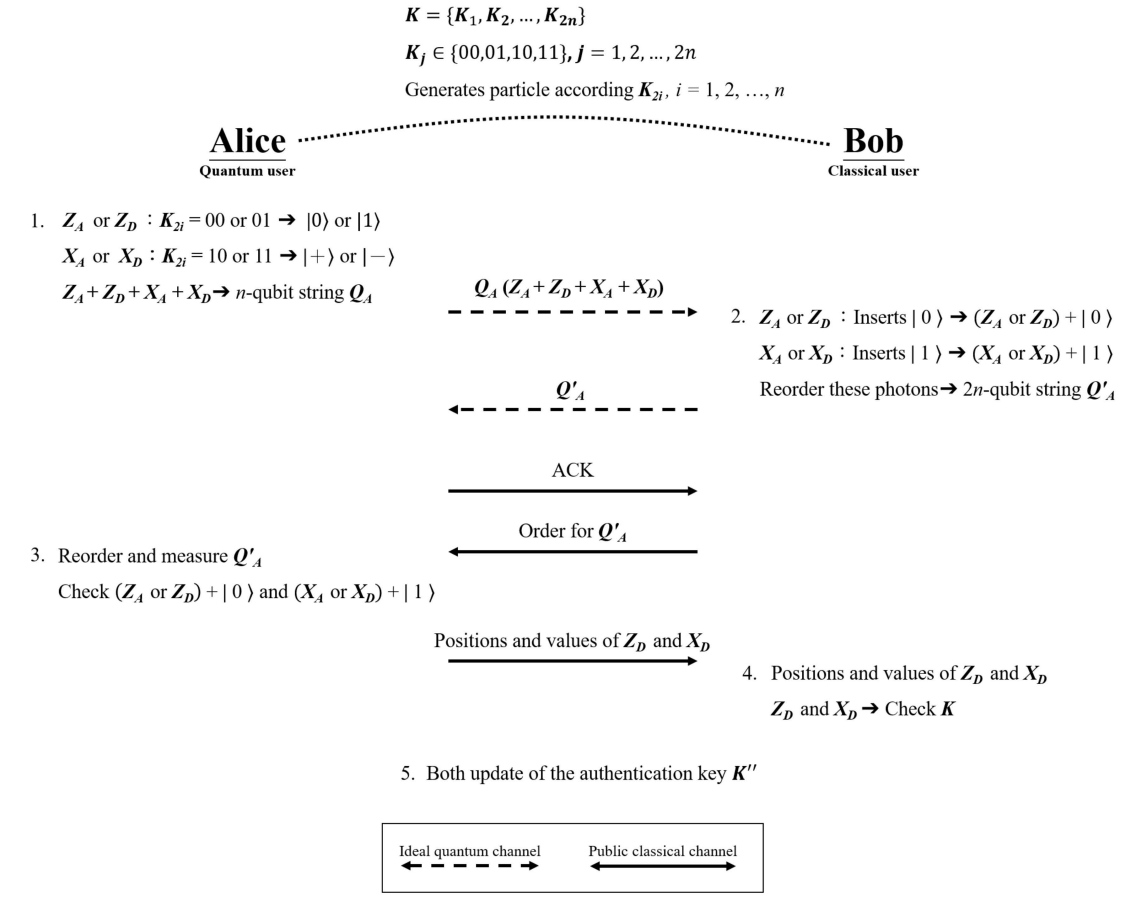

Figure 2. Zhou et al.'s measurement-free SQA protocol.

2.1. Measure-Resend SQA Protocol

Step A1. Alice generates n photon sequence s based on the pre-share d key $\boldsymbol{K}$.

- If $\boldsymbol{K}_{2i} = 00$ or 01, then Alice generates Z-basis qubits $|0\rangle = \begin{bmatrix}1\\0\end{bmatrix}$ or $\left|1\right\rangle = \begin{bmatrix}0\\1\end{bmatrix}$. Half of the Z-basis qubits are recorded as authenticated use ($\boldsymbol{Z_A}$), and the remaining as decoy use ($\boldsymbol{Z_D}$).
- If $\boldsymbol{K}_{2i} = 10$ or 11, then she generates X-basis photons $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ or $\left|-\right\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$, recorded as $\boldsymbol{X_D}$.

Alice sends all the generated photons ($\boldsymbol{Q_A}$) to Bob.

Step A2. Bob receives $\boldsymbol{Q_A}$ and performs operations based on $\boldsymbol{K}$.

- If $\boldsymbol{K}_{2i} = 00$ or 01, Bob performs a Z-basis measurement on the qubits and does not return the qubits.
- If $\boldsymbol{K}_{2i} = 10$ or 11, then Bob reflects the qubits without interference.

Then, Bob resends the $\frac{1}{2}n$ photon sequence ($\boldsymbol{Q'_A}$) back to Alice.

Step A3. Alice receives $\boldsymbol{Q'_A}$ and measures it on the X basis. She checks whether the states are identical to the initial states to secure the channel. She then publishes the position and value of $\boldsymbol{Z_D}$.

Step A4. Bob obtains the position and value of $\boldsymbol{Z_D}$ and infers the positions of $\boldsymbol{Z_A}$. Bob compares whether $\boldsymbol{Z_D}$ is identical to the announcement from Alice and checks whether $\boldsymbol{Z_A}$ is based on the generated $\boldsymbol{K}$. If the error rate is higher than a preset threshold, the protocol aborts.

Step A5. Alice and Bob both update the authentication key based on $\boldsymbol{Z_A}$ and $\boldsymbol{K}$ to obtain the new authentication key denoted as $\boldsymbol{K''} = \left\{\boldsymbol{K''_1}, \boldsymbol{K''_2}, \ldots, \boldsymbol{K''_{2n}}\right\}$ through the following rules: if Bob does not measure the received photons, then Alice and Bob generate $\boldsymbol{K^i_{AB}} = \boldsymbol{K}_{2i}$; if Bob measures the photons, then $\boldsymbol{K^i_{AB}} = 00$ or 01 is generated based on measurement results $|0\rangle$ or $|1\rangle$. Eventually, Alice and Bob update the authentication key as $\boldsymbol{K''_{2i}} = \boldsymbol{K}_{2i} \oplus \boldsymbol{K}_{2i-i} \oplus \boldsymbol{K^i_{AB}}$ and $\boldsymbol{K''_{2i-i}} = \boldsymbol{K}_{2i}$, where $\oplus$ represents mutually exclusive or (XOR) operation.

2.2. Measurement-Free SQA Protocol

Step B1. Alice generates n photon sequence s based on a pre-share d key $\boldsymbol{K}$.

- If $\boldsymbol{K}_{2i} = 00$ or 01, then Alice generates Z-basis qubits $|0\rangle$ or $|1\rangle$. Half of the Z-basis qubits are recorded as authenticated use ($\boldsymbol{Z_A}$), and the remaining as decoy use ($\boldsymbol{Z_D}$).
- If $\boldsymbol{K}_{2i} = 10$ or 11, then she generates X-basis photons $|+\rangle$ or $|-\rangle$. Half of the X-basis qubits are recorded as authenticated use ($\boldsymbol{X_A}$) and the remaining as decoy use ($\boldsymbol{X_D}$).

Alice sends all the generated photons ($\boldsymbol{Q_A}$) to Bob.

Step B2. Bob receives $\boldsymbol{Q_A}$ and performs insertion based on $\boldsymbol{K}$.

- If the photon $\boldsymbol{Q_A}$ is generated based on $\boldsymbol{K}_{2i} = 00$ or 01, then Bob prepares a Z-basis qubit $|0\rangle$ and inserts it after the corresponding photon $\boldsymbol{Q_A}$.
- If photon $\boldsymbol{Q_A}$. is generated based on $\boldsymbol{K}_{2i} = 10$ or 11, then Bob prepares Z-basis qubit $|1$ and inserts it after the corresponding photon $\boldsymbol{Q_A}$.

After insertion, Bob reorders the photon sequence randomly and resends the $2n$ photon sequence ($\boldsymbol{Q'_A}$) back to Alice.

Step B3. Alice receives $\boldsymbol{Q'_A}$ and informs Bob via the classical public channel. Bob then sends the correct order for $\boldsymbol{Q'_A}$. Alice reorders the photon sequence to the correct position according to the announcement from Bob. Alice measures $\boldsymbol{Z_D}$ and $\boldsymbol{X_D}$ on the correct basis to check if they are equal to the initial states. She then measures the inserted qubits on the Z-basis to check whether Bob's insertion is based on $\boldsymbol{K}$, that is, $|0\rangle$ should be inserted after $\boldsymbol{Z_D}$, and $|1\rangle$ should be inserted after $\boldsymbol{X_D}$. After the eavesdropping check, Alice announces the positions of $\boldsymbol{Z_D}$ and $\boldsymbol{X_D}$.

Step B4. Bob receives the positions of $\boldsymbol{Z_D}$ and $\boldsymbol{X_D}$. Bob then requires Alice to announce the values of $\boldsymbol{Z_D}$ and $\boldsymbol{X_D}$. Bob checks whether the photon values are generated based on $\boldsymbol{K}$. If the error rate is higher than a preset threshold, the protocol is aborted. Alice compares whether $\boldsymbol{Z_A}$ and $\boldsymbol{Z_D}$ are generated in correlation with $\boldsymbol{K}$.

Step B5. Alice and Bob both update the authentication key through the rules listed in Table 1, based on $\boldsymbol{K}$ and the Z-basis qubits inserted by Bob to obtain the new authentication key, denoted as $\boldsymbol{K}^{''} = \{\boldsymbol{K}_1^{''}, \boldsymbol{K}_2^{''}, \ldots, \boldsymbol{K}_{2n}^{''}\}$. Finally, Alice and Bob update the authentication key as $\boldsymbol{K}_{2i}^{''} = \boldsymbol{K}_{2i} \oplus \boldsymbol{K}_{2i-i} \oplus \boldsymbol{K}_{AB}^{i}$ and $\boldsymbol{K}_{2i-i}^{''} = \boldsymbol{K}_{2i}$, where $\oplus$ represents XOR operation.

Table 1. Coding rule of $\boldsymbol{K_{AB}}$.

$\boldsymbol{K_{2i}}$	The State Inserted by Bob	$\boldsymbol{K_{AB}^{i}}$
00	$\|0\rangle$	00
01	$\|0\rangle$	10
10	$\|1\rangle$	01
11	$\|1\rangle$	10

3. Security Issues in Zhou et al.'s SQA Protocols

Although Zhou et al.'s SQA protocol has been shown to be secure against several attacks [38], the protocol suffers from severe information leakage. Moreover, this information leakage exposes the entire authentication key $\boldsymbol{K}$ without detection. This study reveals that Zhou et al.'s SQA protocol is vulnerable to a double *CNOT* attack and man-in-the-middle attack. These security issues are described as follows:

3.1. Double CNOT Attack on Zhou et al.'s Measure-Resend SQA Protocol

In Zhou et al.'s measure-resend protocol, an eavesdropper Eve can obtain the authentication key $\boldsymbol{K}$ intact without being detected by performing a double *CNOT* attack. To proceed with the attack, Eve prepares probe qubits $\boldsymbol{q_e^i} = |Z\rangle_e^i = \{|0\rangle, |1\rangle\}$, intercepts each qubit of $\boldsymbol{Q_A}$(denotes as $\boldsymbol{Q_A^i}$), and performs the first *CNOT* operation. The *CNOT* operation is defined as $(|00\rangle\langle 00| + |01\rangle\langle 01| + |11\rangle\langle 10| + |10\rangle\langle 11|)$; $\boldsymbol{Q_A^i}$ is the control qubit, and $\boldsymbol{Q_e^i}$ is the target qubit. To demonstrate the attack clearly, consider the X-basis qubits of $\boldsymbol{Q_A^i}$ ($\boldsymbol{X_D}$) as $|+\rangle$ and the Z-basis qubits of $\boldsymbol{Q_A^i}$ ($\boldsymbol{Z_A}, \boldsymbol{Z_D}$) as $|1$. It should be noted that the choice of X-basis qubits (i.e., $|+\rangle, |-\rangle$) and Z-basis qubits (i.e., $|0\rangle, |1, \rangle$) does not affect the analysis. The first *CNOT* operation is presented as follows:

Assume the X-basis qubits of $\boldsymbol{Q_A^i}$ ($\boldsymbol{X_D}$) as $|+\rangle$:

$$CNOT\left(|+\rangle_A^i \otimes |Z\rangle_e^i\right) = \frac{1}{\sqrt{2}}\left(|0Z\rangle + |1\overline{Z}\rangle\right)_{Ae}^{i} \tag{1}$$

Assume the Z-basis qubits of $\boldsymbol{Q_A^i}$ ($\boldsymbol{Z_A}, \boldsymbol{Z_D}$) as $|1\rangle$:

$$CNOT\left(|1\rangle_A^i \otimes |Z\rangle_e^i\right) = |1\overline{Z}, \rangle_e^i = |1\rangle_A^i \otimes |\overline{Z}, \rangle_e^i \tag{2}$$

After Eve completes the first *CNOT* operation (Equations (1) and (2)), she sends $\boldsymbol{Q_A^i}$ to Bob. After receiving $\boldsymbol{Q_A^i}$, Bob performs a Z-basis measurement on $\boldsymbol{Z_A}, \boldsymbol{Z_D}$, keeps those qubits, reflects $\boldsymbol{X_D}$ back to Alice, and forms photon sequence $\boldsymbol{Q_A'}$, which only contains X-basis qubits ($\boldsymbol{X_D}$). Then, Eve intercepts each photon of $\boldsymbol{Q_A'}$ (denoted as $\boldsymbol{Q_{A'}^i}$), and performs the second *CNOT* operation on $\boldsymbol{Q_{A'}^i}$ and probe qubits $\boldsymbol{q_e^i}$. The second *CNOT* operation is as follows:

Assume the X-basis qubits of $\boldsymbol{Q_{A'}^i}$ ($\boldsymbol{X_D}$) as $|+\rangle$:

$$CNOT\left(\frac{1}{\sqrt{2}}\left(|0Z\rangle + |1\overline{Z}\rangle\right)_{A'e}^{i}\right) = \frac{1}{\sqrt{2}}\left(|0Z\rangle + |1Z\rangle\right)_{A'e}^{i} = |+\rangle_{A'}^{i} \otimes |Z_e^i\rangle \tag{3}$$

Eve then sends Q'_A to Alice. It should be noted that Alice sends Z-basis qubits and X-basis qubits (Q_A) to Bob, and Bob only returns X-basis qubits (Q'_A). Hence, Eve can cross-compare the positions of the qubits of Q_A and Q'_A to infer the position of the Z-basis qubits and X-basis qubits. After Eve obtains the position of the Z-basis qubits, she performs the Z-basis measurement on the probe qubits $q_e^i \left(\left| Z_e^i \right\rangle \right)$ in Equation (2), that were utilized for the first *CNOT* operation with the Z-basis qubits (Z_A, Z_D) of Q_A^i. Eve obtains $\overline{Z}$ (i.e., the measurement result of the probe state transforms into the inverse of the original state), which is the authentication key. Alice and Bob share and update circularly. According to Equation (2), after performing the first *CNOT* operation, the Z-basis qubits (Z_A, Z_D) remain the same. According to Equation (3), the X-basis qubits (X_D) are not altered after the two *CNOT* operations. Thus, we have proven that the attack cannot be detected and successfully revealed that the authentication key k is intact. Figure 3 clearly illustrates a double *CNOT* attack on Zhou et al.'s measure-resend SQA protocol.

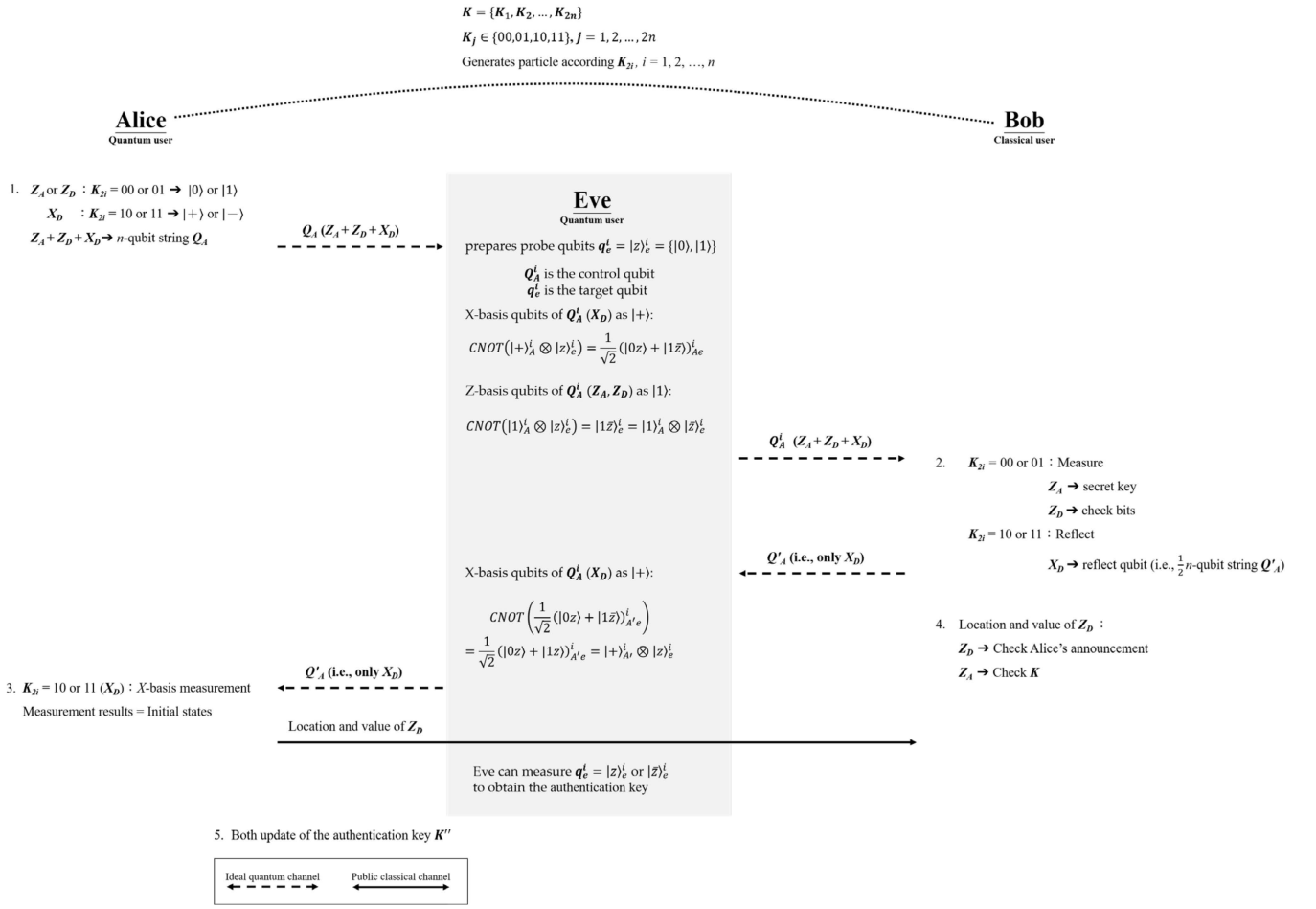

Figure 3. The double *CNOT* attack on Zhou et al.'s measure-resend SQA protocol.

3.2. Man-in-the-Middle Attack on Zhou et al.'s Measurement-Free SQA Protocol

In Zhou et al.'s measurement-free protocol, Eve obtains the entire authentication key K without being detected by performing a man-in-the-middle attack. To perform the attack, Eve intercepts Q'_A and preserves Q'_A through quantum memory temporarily for the following procedure: Eve impersonates Alice to require Bob to announce the correct order of Q'_A (i.e., the channel is not authenticated, and Bob cannot notice the requirement is forged by Eve). Bob then announces the correct order of Q'_A. Eve reorders Q'_A back to the correct order, according to the announcement from Bob. Eve can now easily acknowledge the basis of each photon of Q_A by performing the Z-basis measurement on each of the corresponding

inserted qubits. Then, Eve measures each photon of Q_A with the correct basis to obtain the pre-shared key K (i.e., if the inserted qubit is $|0\rangle$, Eve measures the corresponding Q_A qubits in the Z-basis; if the inserted qubit is $|1\rangle$, Eve measures the corresponding Q_A qubits in the X-basis). After eavesdropping, Eve disorders the photons back to the position as initially done by Bob (Q'_A) and sends them to Alice. Accordingly, the attack does not alter any photons; hence, the eavesdropping check cannot detect abnormalities. Thus, we prove that the attack can eavesdrop on the entire authentication key k without being detected. Figure 4 clearly illustrates a man-in-the-middle attack on Zhou et al.'s measurement-free SQA protocol.

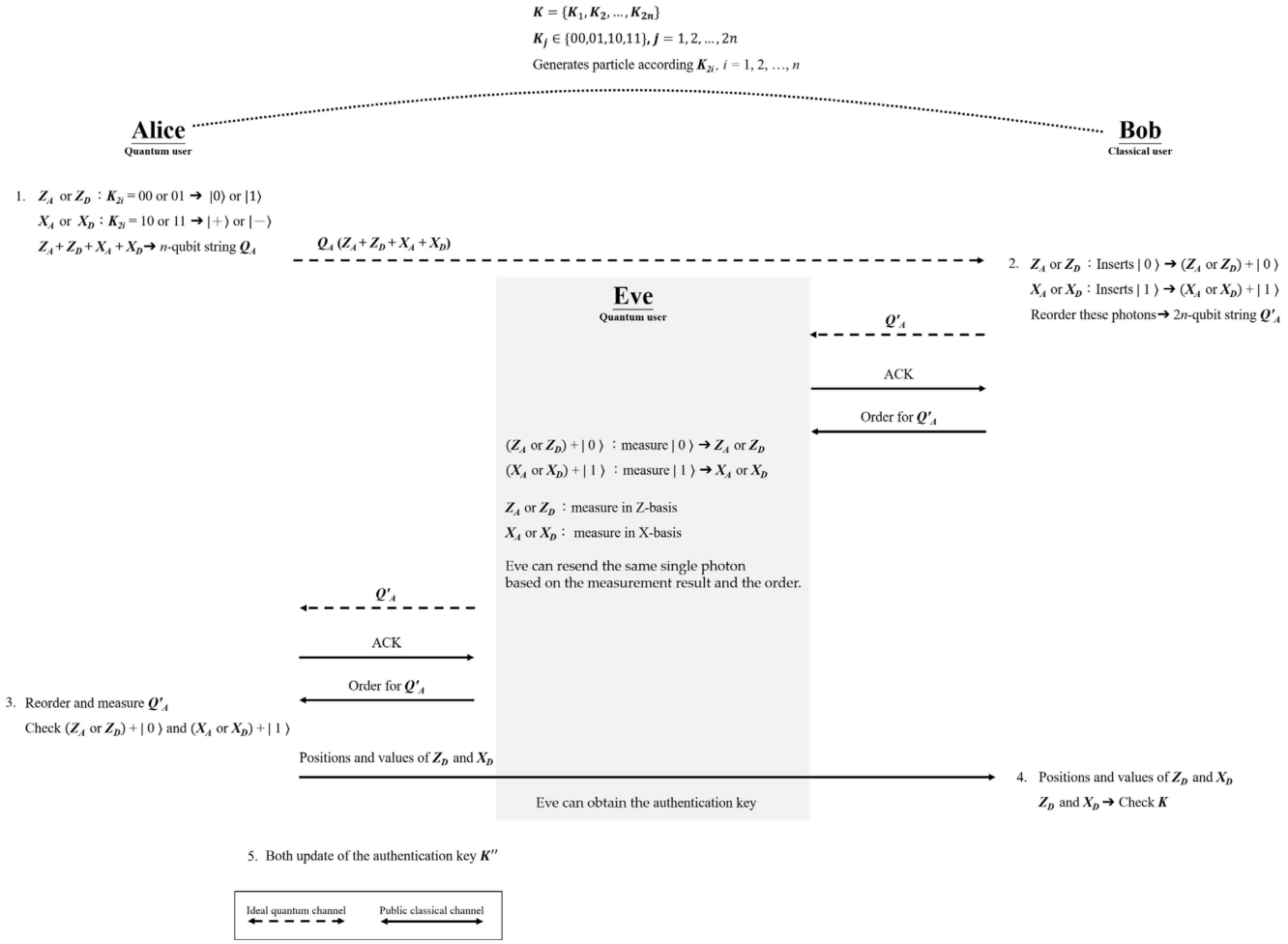

Figure 4. The man-in-the-middle attack on Zhou et al.'s measurement-free SQA protocol.

4. Proposed SQA Protocol

This section describes the proposed SQA protocol based on an improvement of Zhou et al.'s SQA protocol. Suppose that the protocol proceeds in a semi-quantum environment, where Alice is a quantum user, and Bob is a classical user with limited quantum capabilities. The proposed protocol includes two semi-quantum environments: measure-resend and measurement-free. The proposed protocol circumvents all the security flaws mentioned in Zhou et al.'s SQA protocol. The details are as follows:

4.1. Proposed Measure-Resend SQA Protocol

Suppose that Alice and Bob pre-share a binary key $K = \{K_1, K_2, \ldots, K_{2n}\}$, where $K_j \in \{00, 01, 10, 11\}$ and $j = 1, 2, \ldots, 2n$. They generate photons based on K_{2i}, $i = 1, 2, \ldots, n$. Figure 5 clearly illustrates the proposed measure-resend SQA protocol.

Step C1. This process is identical to Step A1. Alice generates Z_A , Z_D, and X_D based on K, forming n photon sequence (Q_A) . Then, Alice sends Q_A to Bob.
Step C2. Bob receives Q_A and performs operations based on K.

- If $K_{2i} = 00$ or 01, Bob performs a Z-basis measurement on the qubits and resends the same single photon based on the measurement result.
- If $K_{2i} = 10$ or 11, Bob reflects qubits without interference.

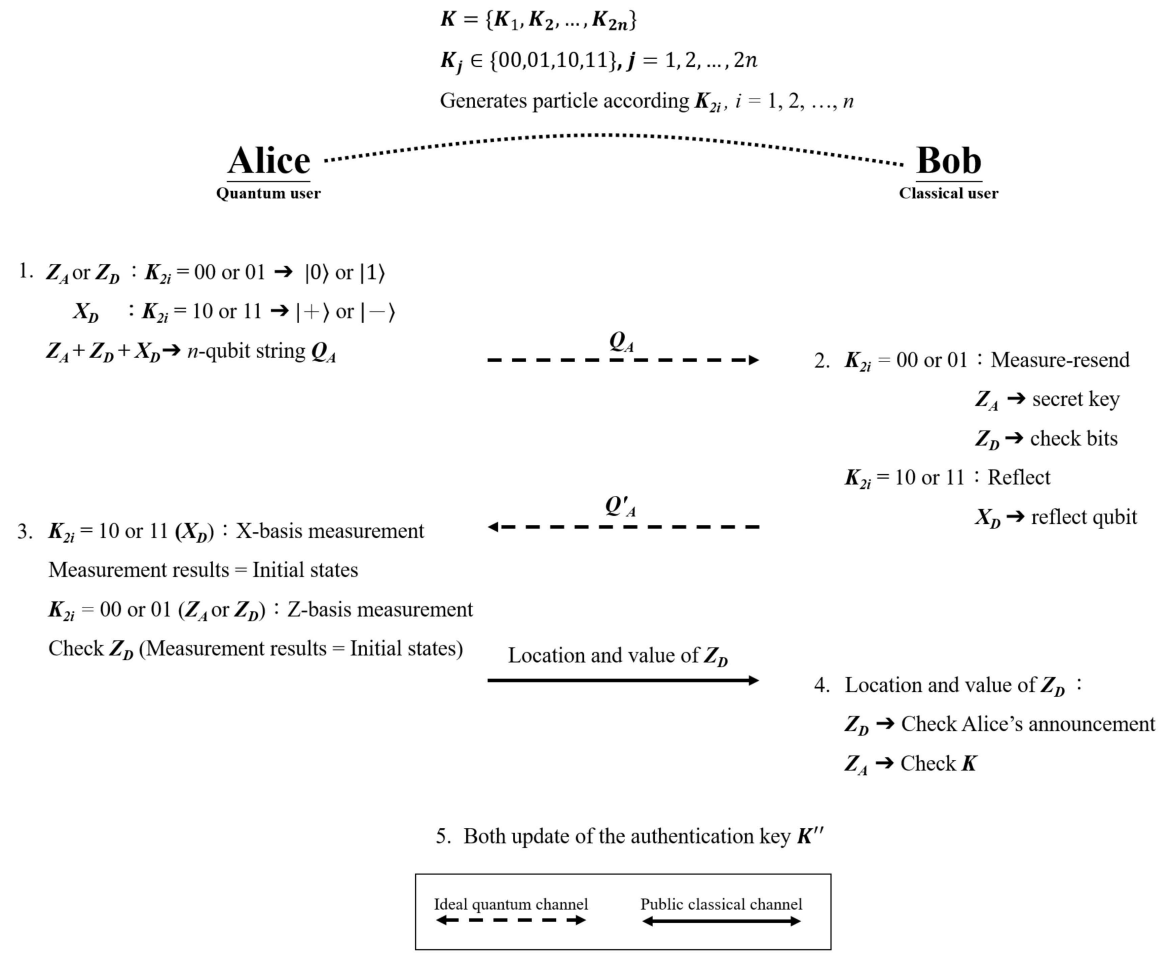

Figure 5. The proposed measure-resend SQA protocol.

Bob then resends the n photon sequence (Q'_A) back to Alice.
Step C3. Alice receives Q'_A and measures it on the correct basis. She checks if the states are identical to the initial states, that is, X_D remains in the same initial state. Alice then publishes the position and value of Z_D.
Step C4. According to Alice's announcement, Bob can infer the position of Z_A. Bob compares whether Z_D and Z_A are generated based on K. If the error rate is higher than a preset threshold, the protocol is aborted.
Step C5. Alice and Bob both update the authentication key through the same rule mentioned in Step A5, obtain ing the new authentication key denoted as $K'' = \{K''_1, K''_2, \ldots, K''_{2n}\}$.

The proposed measure-resend SQA protocol is immune to double *CNOT* attacks. Since Q_A and Q'_A are identical, Eve cannot obtain any information by cross-comparing Q_A and Q'_A. To perform the double *CNOT* attack, Eve must obtain the basis of the photons (i.e., if Eve performs the double *CNOT* attack on both photon sequences (Q_A, Q'_A), performing the *CNOT* operation twice on the same photon cannot obtain any information). Hence, the proposed measure-resend SQA protocol is immune to double *CNOT* attacks.

4.2. Proposed Measurement-Free SQA Protocol

Suppose Alice and Bob pre-share two binary keys, $\boldsymbol{K} = \{\boldsymbol{K}_1, \boldsymbol{K}_2, \ldots, \boldsymbol{K}_{2n}\}$, where $\boldsymbol{K}_j \in \{00, 01, 10, 11\}$, $\boldsymbol{j} = 1, 2, \ldots, 2n$, and $\boldsymbol{K_A}$ represents the order of $\boldsymbol{Q}'_{\boldsymbol{A}}$. They generate photons based on $\boldsymbol{K}_{2i}$, $\boldsymbol{i} = 1, 2, \ldots, n$. Figure 6 clearly illustrates the proposed measurement-free SQA protocol.

Step D1. This process is identical to Step B1. Alice generates $\boldsymbol{Z_A}$, $\boldsymbol{Z_D}$, $\boldsymbol{X_A}$, and $\boldsymbol{X_D}$ based on $\boldsymbol{K}$, to form n photon sequence ($\boldsymbol{Q_A}$). Then, Alice sends $\boldsymbol{Q_A}$ to Bob.
Step D2. Bob performs insertion according to the rule mentioned in Step B2. Bob then reorders the photon sequence based on $\boldsymbol{K_A}$. Bob then resends the $2n$ photon sequence ($\boldsymbol{Q}'_{\boldsymbol{A}}$) back to Alice.
Step D3. Alice receives $\boldsymbol{Q}'_{\boldsymbol{A}}$ and reorders it to the correct order based on $\boldsymbol{K_A}$. She measures the inserted qubits in the Z-basis to check if the correlations are based on $\boldsymbol{K}$ (i.e., $|0\rangle$ should be inserted after $\boldsymbol{Z_A}$ and $\boldsymbol{Z_D}$, $|1\rangle$ should be inserted after $\boldsymbol{X_A}$ and $\boldsymbol{X_D}$). After the eavesdropping check, Alice announces the positions and the value>s of $\boldsymbol{Z_D}$ and $\boldsymbol{X_D}$.
Step D4. Bob receives the positions and the values of $\boldsymbol{Z_D}$ and $\boldsymbol{X_D}$. He checks whether the announced position is correlated with $\boldsymbol{K}$. If the error rate is higher than a preset threshold, the protocol is aborted.
Step D5. Alice and Bob both update the authentication key based on the coding rule (see also Table 2) and obtain the new authentication key denoted as $\boldsymbol{K''} = \{\boldsymbol{K}''_1, \boldsymbol{K}''_2, \ldots, \boldsymbol{K}''_{2n}\}$.

Table 2. Coding rule of $\boldsymbol{K''}$.

{$\boldsymbol{K}$, the Inserted Qubit}	$\boldsymbol{K}'_{\boldsymbol{i}}$
$\|0\rangle$, $\|0\rangle$	00
$\|1\rangle$,$\|0\rangle$	01
$\|+\rangle$, $\|1\rangle$	10
$\|-\rangle$, $\|1\rangle$	11

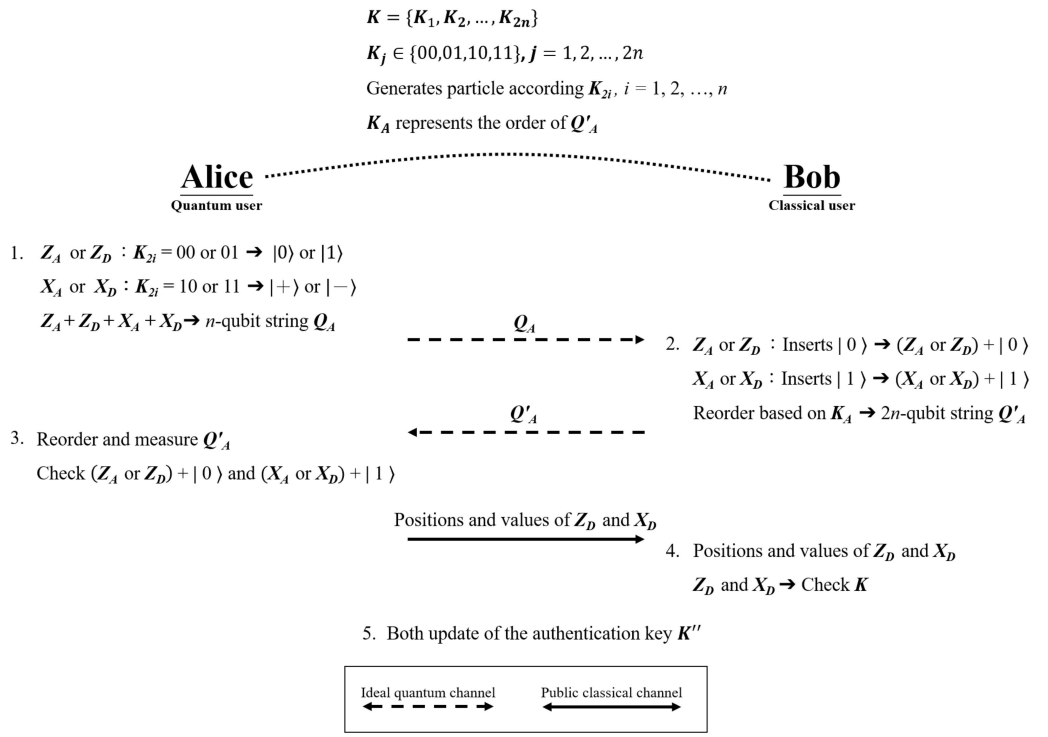

Figure 6. The proposed measurement-free SQA protocol.

The proposed measurement-free SQA protocol can endure man-in-the-middle attacks. In Zhou et al.'s SQA protocol, Eve intercepts and preserves Q'_A in quantum memory and forges Alice to request Bob for the order of Q'_A, so Eve can obtain the basis of each photon of Q_A by measuring the corresponding the inserted photons. Eve then measures Q_A in the correct basis to obtain K without being detected. Under the proposed measurement-free SQA protocol, Eve cannot obtain the order of Q'_A because it was previously pre-shared in K_A. Hence, the proposed measurement-free SQA protocol can withstand man-in-the-middle attacks.

5. Security Analysis

This section discusses the security analysis of the proposed SQA protocol with respect to three main attacks: (1) typical eavesdropping attack, (2) double *CNOT* attack, and (3) man-in-the-middle attack. The proposed SQA protocol is based on Zou et al.'s SQA protocol; hence, the security of the proposed protocol has been proven in Zou et al. In this section, the security of the proposed SQA protocol with respect to these three main attacks is discussed.

5.1. Security against Typical Eavesdropping Attack

5.1.1. Attack on the Proposed Measure-Resend SQA Protocol

Assume that Eve conducts a typical eavesdropping attack to eavesdrop on the authentication key k. In Step C1, Alice generates photons (Q_A) based on k_{2i} and sends them to Bob. Eve intercepts each photon of Q_A and performs a measurement on Q_A on a random basis (i.e., Z-basis or X-basis). After the measurement, Eve prepares the qubits as measurement results (E_A). Eve then sends E_A to Bob. In Step C2, Bob receives E_A and performs measure-resend or reflects photons based on K_{2i} (that is, if $K_{2i} = 00$ or 01, Bob measures on the Z-basis and prepares the same qubit as the measurement result. If $K_{2i} = 10$ or 11, Bob reflects a photon without any disturbance). Bob resends all the photons back to Alice (E'_A). In Step C3, Alice performs an eavesdropping check on E'_A (i.e., Alice checks whether the X-basis photons are equal to the initial state). To pass the eavesdropping check, E'_A must be equal to Q_A. In other words, Eve must acknowledge every basis for the photons of Q_A. Q_A contains four states (i.e., $|0\rangle, |1\rangle, |+\rangle, |-\rangle$) based on k_{2i} while E'_A contains the random basis of the four states. Thus, the possibility of passing the eavesdropping check is $\left(\frac{1}{4}\right)^n$. In other words, the possibility of an attack being detected by Alice is $1 - \left(\frac{1}{4}\right)^n$. Hence, the proposed measure-resend SQA protocol is resistant to eavesdropping.

5.1.2. Attack on the Proposed Measurement-Free SQA Protocol

Suppose Eve performs a typical eavesdropping attack on authentication key k from the traveling qubits between Alice and Bob. In Step D1, Alice generates photons (Q_A) based on k_{2i} and sends Q_A to Bob. Eve intercepts Q_A and performs measurements on photons on a random basis (i.e., Z-basis or X-basis). After the measurement, Eve prepares the qubits as measurement results (E_A). She then resends E_A to Bob. In Step D2, Bob receives E_A and inserts photons based on K_{2i} (i.e., if the received qubit is Z-basis, $|0$ is inserted; if Bob receives X-basis photons, $|1$ is inserted). The inserted photon sequence forms E'_A. Then, Bob reorders E'_A based on k_A and sends it to Alice. In Step D3, Alice receives and recovers E'_A based on k_A, and measures every photon on the correct basis. To pass the eavesdropping check, E'_A must be equal to Q_A. Q_A is generated in four states (i.e., $|0\rangle, |1\rangle, |+\rangle, |-\rangle$) based on k_{2i}, and E_A is generated on a random basis; thus, the possibility of passing the eavesdropping check is $\left(\frac{1}{4}\right)^n$. That is, the possibility of an attack being detected by Alice is $1 - \left(\frac{1}{4}\right)^n$. Hence, the proposed measurement-free SQA protocol is resistant to typical eavesdropping.

5.2. Security against Double CNOT Attack on the Proposed Measure-Resend SQA Protocol

Suppose an eavesdropper, Eve, performs a double *CNOT* attack to eavesdrop on authentication key $\boldsymbol{k}$. To initiate the attack, Eve prepares ancillary qubits $\boldsymbol{q}_e^i = |\boldsymbol{Z}_e^i = \{|0\rangle,|1\rangle\}$ to perform the *CNOT* operation with each traveling qubit of $\boldsymbol{Q_A}$ (denotes as $\boldsymbol{Q}_A^i$). The *CNOT* operation is defined as $(|00\rangle\langle 00|+|01\rangle\langle 01|+|11\rangle\langle 10|+|10\rangle\langle 11|)$; $\boldsymbol{Q}_A^i$ is the control qubit, and $\boldsymbol{q}_e^i$ is the target qubit. For clarity, assume that the X-basis photon of $\boldsymbol{Q}_A^i$ contains $|+$ and the Z-basis photon of $\boldsymbol{Q}_A^i$ contains $|1\rangle$. The choice of the X-basis (i.e., $|+\rangle, |-\rangle$) and Z-basis (i.e., $|0,\rangle\,|1\rangle$) does not affect the security analysis. Eve performs the first *CNOT* operation as follows:

Assume the X-basis photon of $\boldsymbol{Q}_A^i$ contains $|+\rangle$:

$$CNOT\Big(|+\rangle_A^i \otimes |Z\rangle_e^i\Big) = \frac{1}{\sqrt{2}}(|0Z\rangle+|1\overline{Z}\rangle)_{Ae}^i \tag{4}$$

Assume the Z-basis photon of $\boldsymbol{Q}_A^i$ contains $|1\rangle$:

$$CNOT\Big(|1\rangle_A^i \otimes |Z\rangle_e^i\Big) = \big|1\overline{Z}\big\rangle_e^i = |1\rangle_A^i \otimes \big|\overline{Z}\big\rangle_e^i \tag{5}$$

After the first *CNOT* operation, Eve sends $\boldsymbol{Q_A}$ to Bob. After receiving $\boldsymbol{Q_A}$, Bob utilizes the measure-resend mode or reflect mode based on $\boldsymbol{k}_{2i}$ and returns $\boldsymbol{Q}_A'$ to Alice. In the improved SQA protocol, because Bob must send a qubit back to Alice for every received qubit, Eve does not know which qubit will be present in the reflect mode. That is, Eve does not know which qubit is sent back by Bob to perform the *CNOT* operation. Therefore, Eve intercepts each photon of $\boldsymbol{Q}_A'$ (denoted as $\boldsymbol{Q}_{A'}^i$), performs the second *CNOT* operation on $\boldsymbol{Q}_{A'}^i$ with $\boldsymbol{q}_e^i$, and then resends it to Alice. The second *CNOT* operation is as follows:

Assume the X-basis of $\boldsymbol{Q}_{A'}^i$ contains $|+\rangle$:

$$CNOT\Big(\frac{1}{\sqrt{2}}(|0Z\Big\rangle+|1\overline{Z}\rangle)_{A'e}^i\Big) = \frac{1}{\sqrt{2}}(|0Z\rangle+|1Z)_{A'e}^i = |+\rangle_A^i \otimes |Z\rangle_e^i \tag{6}$$

Assume the Z-basis of $\boldsymbol{Q}_{A'}^i$ contains $|1\rangle$:

$$CNOT\Big(|1\rangle_{A'}^i \otimes \big|\overline{Z}\big\rangle_e^i\Big) = |1Z\rangle_e^i = |1\rangle_A^i \otimes |Z\rangle_e^i \tag{7}$$

In Equations (6) and (7), the measurement result of $\boldsymbol{q}_e^i$ remains the same. In other words, Eve cannot measure an ancillary qubit to obtain private information. Hence, we prove that the proposed measure-resend SQA protocol can endure a double *CNOT* attack.

5.3. Security against Man-in-the-Middle Attack on the Proposed Measurement-Free SQA Protocol

Suppose Eve performs a man-in-the-middle attack to eavesdrop on authentication key $\boldsymbol{k}$. Alice authenticates Bob in Step D3, where Alice checks if the photons sent by Bob are secured based on $\boldsymbol{k}_{2i}$. Bob authenticates Alice in Step D4 and deduces whether Alice announces the correct position of $\boldsymbol{Z_A}$ and $\boldsymbol{Z_D}$ based on $\boldsymbol{K}$. In other words, authentication is based on the individual pre-shared key; hence, impersonation cannot exist under any circumstance.

6. Performance Analysis

This section provides a comparative study of the latest SQA protocols with the proposed SQA protocols. Based on single photons, Table 3 provides a comparison between the proposed SQA protocols and Zhou et al.'s protocol [38], Zebboudj et al.'s protocol [39], Chang et al.'s protocol [35], and Wang et al.'s protocol [36]. The qubit 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. The efficiency analysis of

Zebboudj et al., Chang et al., and Wang et al.'s SQA protocols have been discussed in the study [36].

Table 3. Comparison of [35,36,38,39] and the proposed SQA protocols.

	Zhou et al.'s Protocols [38]		**Zebboudj et al.'s Protocol [39]**	**Chang et al.'s Protocol [35]**	**Wang et al.'s Protocol [36]**	**The Proposed Protocols**	
Quantum resource	Single photons		Single photons	Single photons	Single photons	Single photons	
Semi-quantum environment	Measure-resend	Measurement-free	Measure-resend	Measure-resend	Measure-resend	Measure-resend	Measurement-free
Quantum efficiency	33%	17%	14%	17%	14%	20%	17%
Required pre-shared keys (in bits)	$6n$	$4n$	$3n$	$3n$	$3n$	$6n$	$5n$
Vulnerability to double *CNOT* attack	Yes	No	No	No	No	No	No
Vulnerability to man-in-the-middle attack	No	Yes	No	No	No	No	No

In Zhou et al.'s measure-resend SQA protocol, Alice prepares $3n$ single photons in Z_A, Z_D and X_D. Bob measures Z_A, Z_D and reflects X_D. Eventually, both share n authentication key. Thus, the qubit efficiency of Zhou et al.'s measure-resend SQA protocol is $\frac{n}{3n} \approx 33\%$.

In Zhou et al.'s measurement-free SQA protocol, Alice prepares $4n$ single photons in Z_A, Z_D, X_A and X_D. Bob generates $2n$ photons (i.e., $|0\rangle$ or $|1\rangle$) and inserts them. Eventually, both share n authentication key. Thus, the qubit efficiency of Zhou et al.'s measurement-free SQA protocol is $\frac{n}{4n+2n} \approx 17\%$.

In the proposed measure-resend SQA protocol, Alice prepares $3n$ single photons in Z_A, Z_D and X_D. Bob measures Z_A, Z_D and generates $2n$ single photons. Thus, the qubit efficiency of the proposed measure-resend SQA protocol is $\frac{n}{3n+2n} = 20\%$.

In the proposed measurement-free SQA protocol, Alice prepares $4n$ single photons in Z_A, Z_D, X_A and X_D. Bob generates $2n$ single photons (i.e., $|0\rangle$ or $|1\rangle$). Thus, the qubit efficiency of the proposed measurement-free SQA protocol is $\frac{n}{4n+2n} \approx 17\%$.

Compared to Zebboudj et al. [39], Chang et al. [35], and Wang et al.'s [36] measure-resend SQA protocols with the proposed SQA protocols, the proposed SQA protocols have higher qubit efficiency. Although the qubit efficiency is lower than that of Zhou et al. [38], the proposed SQA protocols do not suffer from the double *CNOT* attack and the man-in-the-middle attack. Based on the comparative studies, the proposed SQA protocols obtain the following advantages:

(1.) The qubit efficiency of the proposed SQA protocols is significantly higher than most protocols [35,36,39].
(2.) The proposed SQA protocols do not exist information leakage and are proven secure under the double *CNOT* attack and the man-in-the-middle attack.

7. Conclusions

This study revealed severe information leakage under Zhou et al.'s SQA protocol, and a secure SQA protocol was proposed. An eavesdropper can obtain an intact authentication key by performing a double *CNOT* attack and a man-in-the-middle attack without being detected. In Zhou et al.'s measure-resend SQA protocol, Eve can obtain the authentication key by performing a double *CNOT* attack without being detected based on the cross-comparison of send and resend photon sequences ($Q_A, Q\prime_A$). In Zhou et al.'s measurement-free SQA protocol, Eve can eavesdrop on the authentication key by performing a man-in-the-middle attack based on the announcement (the order of $Q\prime_A$). In contrast, the proposed SQA protocol is immune to the double *CNOT* attack, man-in-the-middle attack, and typical eavesdropping attack. Although the qubit efficiency is lower than that of Zhou et al.'s SQA

protocol, the proposed protocol ensures information security. How to increase the qubit efficiency while remaining secure is the subject of future research.

Author Contributions: Conceptualization, C.-W.Y. and H.-W.W.; methodology, C.-W.Y., H.-W.W. and C.-W.T.; investigation, J.L. and H.-W.W.; formal analysis, C.-W.Y.; writing—original draft, C.-W.Y. and H.-W.W.; writing—review & editing, C.-W.T. and J.L.; 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 National Science and Technology Council, Taiwan, R.O.C. (Grant Nos. NSTC 111-2221-E-039-014, NSTC 111-2221-E-005-048, NSTC 111-2634-F-005-001, NSTC 111-2218-E-005-007-MBK, NSTC 111-2221-E-143-006-MY2, and NSTC 111-2221-E-025-010) and China Medical University, Taiwan (Grant No. CMU111-S-28).

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. Boyer, M.; Kenigsberg, D.; Mor, T. Quantum Key Distribution with Classical Bob. *Phys. Rev. Lett.* **2007**, *99*, 140501. [CrossRef] [PubMed]
2. Zou, X.; Qiu, D.; Zhang, S.; Mateus, P. Semiquantum key distribution without invoking the classical party's measurement capability. *Quantum Inf. Process.* **2015**, *14*, 2981–2996. [CrossRef]
3. Tsai, C.-W.; Yang, C.-W.; Lee, N.-Y. Lightweight mediated semi-quantum key distribution protocol. *Mod. Phys. Lett. A* **2019**, *34*, 1950281. [CrossRef]
4. Boyer, M.; Gelles, R.; Kenigsberg, D.; Mor, T. Semiquantum key distribution. *Phys. Rev. A* **2009**, *79*, 032341. [CrossRef]
5. 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]
6. Wang, J.; Zhang, S.; Zhang, Q.; Tang, C.J. Semiquantum Key Distribution Using Entangled States. *Chin. Phys. Lett.* **2011**, *28*, 100301. [CrossRef]
7. Sun, Z.-W.; Du, R.-G.; Long, D.-Y. Quantum Key Distribution With Limited Classical Bob. *Int. J. Quant. Infor.* **2013**, *11*, 1350005. [CrossRef]
8. Boyer, M.; Gelles, R.; Mor, T. Attacks on fixed-apparatus quantum-key-distribution schemes. *Phys. Rev. A* **2014**, *90*, 012329. [CrossRef]
9. Krawec, W.O. Restricted attacks on semi-quantum key distribution protocols. *Quantum Inf. Process.* **2014**, *13*, 2417–2436. [CrossRef]
10. Krawec, W.O. Mediated semiquantum key distribution. *Phys. Rev. A* **2015**, *91*, 032323. [CrossRef]
11. Yang, Y.-G.; Sun, S.-J.; Zhao, Q.-Q. Trojan-horse attacks on quantum key distribution with classical Bob. *Quantum Inf. Process.* **2015**, *14*, 681–686. [CrossRef]
12. Krawec, W.O. Security of a semi-quantum protocol where reflections contribute to the secret key. *Quantum Inf. Process.* **2016**, *15*, 2067–2090. [CrossRef]
13. Li, Q.; Chan, W.H.; Zhang, S. Semiquantum key distribution with secure delegated quantum computation. *Sci. Rep.* **2016**, *6*, 19898. [CrossRef]
14. Boyer, M.; Katz, M.; Liss, R.; Mor, T. Experimentally feasible protocol for semiquantum key distribution. *Phys. Rev. A* **2017**, *96*, 062335. [CrossRef]
15. Yu, K.-F.; Gu, J.; Hwang, T.; Gope, P. Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing. *Quantum Inf. Process.* **2017**, *16*, 194. [CrossRef]
16. Zhang, M.-H.; Li, H.-F.; Peng, J.-Y.; Feng, X.-Y. Fault-tolerant Semiquantum key Distribution Over a Collective-dephasing Noise Channel. *Int. J. Theor. Phys.* **2017**, *56*, 2659–2670. [CrossRef]
17. Liu, Z.-R.; Hwang, T. Mediated Semi-Quantum Key Distribution Without Invoking Quantum Measurement. *Ann. Phys.* **2018**, *530*, 1700206. [CrossRef]
18. Tsai, C.-L.; Hwang, T. Semi-quantum Key Distribution Robust Against Combined Collective Noise. *Int. J. Theor. Phys.* **2018**, *57*, 3410–3418. [CrossRef]
19. Zhang, W.; Qiu, D.; Mateus, P. Security of a single-state semi-quantum key distribution protocol. *Quantum Inf. Process.* **2018**, *17*, 135. [CrossRef]
20. Zhu, K.-N.; Zhou, N.-R.; Wang, Y.-Q.; Wen, X.-J. Semi-Quantum Key Distribution Protocols with GHZ States. *Int. J. Theor. Phys.* **2018**, *57*, 3621–3631. [CrossRef]

21. Amer, O.; Krawec, W.O. Semiquantum key distribution with high quantum noise tolerance. *Phys. Rev. A* **2019**, *100*, 022319. [CrossRef]
22. Lin, P.-H.; Tsai, C.-W.; Hwang, T. Mediated Semi-Quantum Key Distribution Using Single Photons. *Ann. Phys.* **2019**, *531*, 1800347. [CrossRef]
23. Tsai, C.-W.; Yang, C.-W. Cryptanalysis and Improvement of the Semi-Quantum Key Distribution Robust against Combined Collective Noise. *Int. J. Theor. Phys.* **2019**, *58*, 2244–2250. [CrossRef]
24. Wang, M.-M.; Gong, L.-M.; Shao, L.-H. Efficient semiquantum key distribution without entanglement. *Quantum Inf. Process.* **2019**, *18*, 260. [CrossRef]
25. Zhou, N.-R.; Zhu, K.-N.; Zou, X.-F. Multi-Party Semi-Quantum Key Distribution Protocol With Four-Particle Cluster States. *Ann. Phys.* **2019**, *531*, 1800520. [CrossRef]
26. Lu, Y.-C.; Tsai, C.-W.; Hwang, T. Collective Attack and Improvement on "Mediated Semi-Quantum Key Distribution Using Single Photons". *Ann. Phys.* **2020**, *532*, 1900493. [CrossRef]
27. Hajji, H.; El Baz, M. Qutrit-based semi-quantum key distribution protocol. *Quantum Inf. Process.* **2021**, *20*, 4. [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]
29. Yang, C.-W. Encryption chain based on measurement result and its applications on semi-quantum key distribution protocol. *Sci. Rep.* **2022**, *12*, 18381. [CrossRef]
30. 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]
31. 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]
32. Meslouhi, A.; Hassouni, Y. Cryptanalysis on authenticated semi-quantum key distribution protocol using Bell states. *Quantum Inf. Process.* **2016**, *16*, 18. [CrossRef]
33. 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]
34. Tsai, C.-W.; Yang, C.-W. Lightweight authenticated semi-quantum key distribution protocol without trojan horse attack. *Laser Phys. Lett.* **2020**, *17*, 075202. [CrossRef]
35. 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]
36. 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]
37. 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. [CrossRef]
38. Zhou, N.-R.; Zhu, K.-N.; Bi, W.; Gong, L.-H. Semi-quantum identification. *Quantum Inf. Process.* **2019**, *18*, 197. [CrossRef]
39. Zebboudj, S.; Djoudi, H.; Lalaoui, D.; Omar, M. Authenticated semi-quantum key distribution without entanglement. *Quantum Inf. Process.* **2020**, *19*, 77. [CrossRef]