mathematics

Article

Efficient and Secure Measure-Resend Authenticated Semi-Quantum Key Distribution Protocol against Reflecting Attack

Hung-Wen Wang [1], Chia-Wei Tsai [2], Jason Lin [3], Yu-Yun Huang [1] 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 District, Taichung 406040, Taiwan; u109217001@cmu.edu.tw (H.-W.W.); u108020702@cmu.edu.tw (Y.-Y.H.)
[2] Department of Computer Science and Information Engineering, National Taitung University, No. 369, Sec. 2, University Rd., Taitung 95092, Taiwan; cwtsai@nttu.edu.tw
[3] Department of Computer Science and Engineering, National Chung Hsing University, No. 145, Xingda Rd., South District, Taichung 40227, Taiwan; jasonlin@nchu.edu.tw
* Correspondence: cwyang@mail.cmu.edu.tw

Abstract: In 2021, Chang et al. proposed an authenticated semi-quantum key-distribution (ASQKD) protocol using single photons and an authenticated channel. 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. If these security issues are not addressed, the ASQKD protocol will fail to deliver the secret key. Therefore, this study proposes an efficient and secure ASQKD protocol to circumvent these problems using only single photons. Security analysis proves that the proposed ASQKD protocol can effectively avoid reflecting attacks, collective attacks, and other typical attacks. Compared with the existing ASQKD protocols, this study has the following advantages: based on a single photon, it demands less advanced quantum devices, the communication efficiency is higher than most protocols, it reduces the length of the required pre-shared keys, endures reflecting attacks, collective attacks, and there is no need for the classical channel.

Keywords: authentication; measure-resend; quantum cryptography; reflecting attack; semi-quantum key distribution; single photon

MSC: 81P94

Citation: 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. https://doi.org/10.3390/math10081241

Academic Editor: Dmitry Makarov

Received: 28 February 2022
Accepted: 7 April 2022
Published: 10 April 2022

1. Introduction

Quantum key distribution (QKD) protocols have been an important research field in quantum cryptography since the beginning. The main objective of the QKD protocol is to enable the two participants to use quantum mechanics to share a secret key. In the QKD protocol, two participants can detect an eavesdropper trying to eavesdrop on the transmission of information with quantum states. In 1984, Bennett and Brassard [1] proposed the first QKD protocol, also known as BB84, which is based on single photons. The protocol allows two participants (Alice and Bob) to share a secure key with a quantum channel and authenticated classical channel. Since the BB84 protocol was proposed, various QKD protocols [2–18] have been proposed to manage different security issues.

However, these QKD protocols [2–13] typically assume that both participants have the requisite hardware, which is not a practical assumption as quantum computing hardware is prohibitively expensive. With an aim of increasing the accessibility of these protocols for everyone, Boyer et al. [14] proposed the first semi-quantum key distribution (SQKD) protocol in 2007. Boyer et al. [15] specified an environment that involves two types of

participants: one with unlimited quantum capabilities and the other with classical capabilities and limited quantum capabilities, where the user Bob is considered a classical user and the user Alice possesses full quantum abilities. In Boyer et al.'s SQKD protocol [15], Bob can possess three of the following abilities: (1) Z-basis (i.e., $\{|0\rangle, |1\rangle\}$) measurements, (2) generating Z-basis qubits, (3) reordering qubits using different delay lines, and (4) reflecting qubits without disturbance. Boyer et al. mentioned two types of SQKD protocols: randomization-based and measure-resend. In the measure-resend SQKD protocol, classical user Bob is allowed to perform: (1) Z-basis measurement, (2) generating Z-basis qubits, and (4) reflecting qubits. In the randomization-based SQKD protocol, Bob performs: (1) Z-basis measurement, (3) reordering qubits using different delay lines, and (4) reflecting qubits. After the proposal, miscellaneous protocols have been applied within a 'semi' environment (e.g., SQKD protocols [16–35], semi-quantum secret sharing protocols [36–39], and semi-quantum secure direct communication [40–44]).

Nevertheless, semi-quantum cryptographic protocols assume the existence of an authenticated classical channel, which means that when an authenticated channel is not available, these protocols cannot endure man-in-the-middle attacks. To prevent man-in-the-middle attacks, the lack of authentication of the participants must be fixed. In 2014, Yu et al. [45] proposed two authenticated semi-quantum key distribution (ASQKD) protocols based on Bell states. The main objective of the ASQKD protocol is to enable two participants to use the pre-shared master key to distribute a session key and perform authentication between the quantum and classical participants. In 2016, Li et al. [46] proposed two ASQKD protocols that use Bell states and single photons. Compared with Yu et al.'s ASQKD protocols [45], Li et al.'s ASQKD protocols ensure better communication efficiency and require fewer pre-shared keys. In 2016, Meslouhi and Hassouni [47] pointed out a vulnerability that allows an eavesdropper to recover a partial master key and launch a successful man-in-the-middle attack on Yu et al.'s ASQKD protocols [45] and Li et al.'s ASQKD protocols [46]. In 2020, Zebboudj et al. [48] presented a new ASQKD protocol without any entanglement. Zebboudj et al.'s ASQKD protocol can achieve higher security than the existing schemes. In 2020, Tsai and Yang [49] proposed a lightweight authenticated semi-quantum key distribution (LASQKD) protocol based on the Bell states. Tsai and Yang's LASQKD protocol allows a quantum user and a classical user to share secret keys without using an authenticated classical channel or Trojan horse detection device. Compared to the existing ASQKD protocols, Tsai and Yang's LASQKD protocol provides improved practicality, indicating its potential for use in modern quantum systems.

In 2021, Chang et al. [50] proposed a measure-resend ASQKD protocol only using single photons. Compared with the existing ASQKD protocols, Chang et al.'s ASQKD protocol has the following advantages:

(1) Chang et al.'s ASQKD protocol is more practical because it uses single qubits instead of Bell states.
(2) Chang et al.'s ASQKD protocol reduces the number of pre-shared keys.
(3) Chang et al. showed that the proposed ASQKD protocol is robust under a collective attack.
(4) It is significantly more efficient than some existing ASQKD protocols.

Although Chang et al. showed that their ASQKD protocol is robust even for an eavesdropper, Eve tries to perform a collective attack. This study demonstrates that Chang et al.'s ASQKD protocol cannot withstand the reflecting attack. In Chang et al.'s ASQKD protocol, Alice prepares several qubits to encode the secret key and hash value and then sends these qubits to Bob. Bob can select the measure-resend or reflecting mode for Alice. However, the sent qubits and the received qubits have the same quantum states. Thus, Eve intercepts the qubits sent from Alice and reflects them back to Alice. Alice cannot distinguish whether these were sent by Bob or forged by Eve—both scenarios would pass the eavesdropping check. In other words, if Eve performs a reflecting attack, Alice will not notice and continue this protocol, treating Eve as Bob. Although Eve cannot obtain the secret key, she is able to launch the replay attack.

More than that, Chang et al.'s ASQKD protocol assumes having an authenticated classical channel between Alice and Bob is illogical (i.e., the transmitted classical messages can be eavesdropped upon, but not modified). ASQKD protocols perform authentication when an authenticated classical channel is unavailable. In other words, research on ASQKD protocols [45–49] assumes that the classical channel is a public classical channel (i.e., it can be modified).

To circumvent these security problems, this study proposes an efficient and secure ASQKD protocol that uses only single photons. Based on the measurement uncertainty of a single photon, Alice can authenticate Bob without using a classical channel. In the proposed ASQKD protocol, Alice generates a single photon as the checking qubit by using the X-basis (i.e., $\left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$). When Bob receives the photon, he measures the checking qubit in the Z-basis (i.e., $\{|0\rangle, |1\rangle\}$) and resends the same state to Alice. Alice receives and measures the checking qubit in the X-basis. If the checking qubit is always the same as the initial state, Alice indicates that Bob does not receive and measure-resends the photon. Thus, the protocol suffers from a reflective attack. Otherwise, Alice would acknowledge that Bob received and measure-resend it. Thus, the proposed protocol can effectively avoid reflecting attacks and does not require a classical channel.

The remainder of this paper is organized as follows: Section 2 provides a review of Chang et al.'s ASQKD protocol. Section 3 describes the security issues of Chang et al.'s ASQKD protocol. Section 4 describes the proposed ASQKD protocol. Section 5 presents an analysis of the security of the proposed ASQKD protocol. Section 6 presents an efficiency analysis of the proposed scheme. The paper ends with a conclusion in Section 7.

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

Chang et al. proposed a measure-resend ASQKD protocol that uses single photons. In Chang et al.'s ASQKD protocol, Alice has full quantum capabilities, whereas Bob (the classical user) has only limited quantum capabilities. Bob can only perform measurement and generation of Z-basis qubits, and reflection of qubits. Alice and Bob must pre-share two secret keys in the protocol: K_1 and K_2, and a pool of universal hash functions. K_1 represents the position of the decoy photons, and K_2 determines the choice of the hash function from the universal hash function pool. Alice prepares a session key and its hash value in single photons and sends it to Bob. He measure-resends or reflects the qubits based on the pre-shared secret key, K_1. Finally, Alice and Bob inform each other of their checking results via an authenticated classical channel. The steps involved in the ASQKD protocol of Chang et al. are described below.

Step C1. Alice chooses a binary string of length n as the session key SK. Based on the pre-share key K_2, Alice selects a hash function from a pool of universal hash functions. She hashes SK using the selected hash function $H_{K_2}(\cdot)$, and obtains the m-bit hash value, $H_{K_2}(SK)$. Then, Alice concatenates SK and the hashed value $H_{K_2}(SK)$ to form $S_A = SK \,||\, H_{K_2}(SK)$, whose length is $n + m$ bits.

Step C2. Alice generates a binary string, $S_D \in \{0,1\}^{n+m}$. Based on the pre-shared key K_1, Alice inserts S_D into S_A. For example, if $K_1^i = 0$, S_D^i is inserted before S_A^i. Otherwise, S_A^i is inserted before S_D^i. Thus, Alice obtains a new binary string, whose length is $2n + 2m$. Alice converts the binary string into a sequence of single photons, Q_A, according to the following rules: binary bits {0, 1} in S_A encode into the Z-basis $\{|0\rangle, |1\rangle\}$, and binary bits {0, 1} in S_D encode into the X-basis $\left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$. Then, Alice sends Q_A to Bob one bit at a time through a quantum channel.

Step C3. Bob receives the qubits and distinguishes S_A from S_D based on K_1. For S_A, Bob measures the Z-basis and resends the same single photon as the measurement result. As for S_D, Bob reflects without any interference back to Alice.

Step C4. Alice receives a sequence of single photons, Q'_A, from Bob and measures S'_A in the Z-basis, and S'_D in the X-basis. Alice checks the measurement results $S'_A = S_A$ and

$S'_D = S_D$ to prevent an eavesdropping attack. Bob checks $H_{K_2}(SK') = H_{K_2}(SK)'$ to identify the secret key sent by Alice.

Step C5. For completion of the eavesdropping check, Alice and Bob must both send a message to inform each other regarding the checking result via the authenticated channel. If the transmission is secured, the pre-shared keys are recycled; otherwise, the results and the pre-shared key K_2 should be abandoned.

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

Although Chang et al.'s ASQKD protocol provides security analyses, the protocol is illogical in using an authenticated classical channel and suffers reflecting attacks, which are described in Sections 3.1 and 3.2, respectively.

3.1. Using an Authenticated Classical Channel in ASQKD Protocol

ASQKD protocols involve authenticating communicators without using an authenticated classical channel [45–49]. In Chang et al.'s ASQKD protocol, Alice and Bob inform each other via an authenticated classical channel, which disobeys the goal of the ASQKD protocols. If Alice and Bob have an authenticated classical channel, then authentication is performed. Therefore, the authenticated classical channel should be changed to a public classical channel in Chang et al.'s ASQKD protocol.

3.2. Reflecting Attack on Chang et al.'s ASQKD Protocol

Although Chang et al. showed that their ASQKD protocol is robust even for an eavesdropper, Eve tries to perform a collective attack, and this study demonstrates that Chang et al.'s ASQKD protocol cannot withstand the reflecting attack. In Chang et al.'s ASQKD protocol, Alice encodes the secret key SK and hash value $H_{K_2}(SK)$ to form $S_A = SK \,||\, H_{K_2}(SK)$, and then generates a binary string, S_D. In Step C2, Alice converts the binary string (S_A and S_D) into a sequence of single photons, Q_A, and then sends Q_A to Bob. In Step C3, Bob can select the measure-resend mode, or the reflecting mode, based on K_1 and then send Q'_A to Alice. In Step C4, Alice checks Q'_A. If the measurement result of Q'_A is equal to the initial state Q_A, the eavesdropping check is passed. Hence, the sent qubits, Q_A, and received qubits, Q'_A, are the same quantum states for Alice. Thus, Eve can intercept the qubits Q_A sent from Alice in Step C2 and then reflect Q_A back to Alice in Step C3. In Step C4, Alice cannot distinguish whether this was sent by Bob or forged by Eve—both scenarios would pass the eavesdropping check. In other words, if Eve performs a reflecting attack, Alice will not notice and continue this protocol, treating Eve as Bob. Although Eve cannot obtain the secret key, she can successfully perform the replay attack.

4. Proposed ASQKD Protocol

In the proposed ASQKD protocol, Alice has full quantum capabilities and Bob has limited quantum capabilities. In the initial phase, Alice and Bob share two secret keys in the protocol, K_1 and K_2, and a pool of universal hash functions. K_1 represents the position of the decoy photons (ternary number system), and K_2 determines the hash function choice from the universal hash function pool. To prevent a reflecting attack, this study utilizes an eavesdropping check using the measurement uncertainty of a single photon. Thus, the proposed protocol can effectively avoid reflecting attacks and does not require classical channels. Figure 1 clearly illustrates the proposed scheme. The steps involved in the proposed ASQKD protocol are as follows:

Step 1. Alice chooses a binary string of length n as the session key SK. Based on the pre-share key K_2, Alice selects a hash function from a pool of universal hash functions. She hashes SK using the selected hash function $H_{K_2}(\cdot)$, and obtains the m-bit hash value, $H_{K_2}(SK)$. Then, Alice concatenates SK and the hashed value $H_{K_2}(SK)$ to form $S_A = SK \,||\, H_{K_2}(SK)$, whose length is $n + m$ bits.

Step 2. Alice generates the binary strings $S_D \in \{0, 1\}^{\frac{n+m}{2}}$ and $S_R \in \{0, 1\}^{\frac{n+m}{2}}$. Based on the pre-shared key K_1, Alice combines S_A, S_D, and S_R into a binary sequence, S_{AB}.

For example, if $K_1^i = 0$, S_A^i is placed in S_{AB}, if $K_1^i = 1$, S_D^i is placed in S_{AB}, and if $K_1^i = 2$, S_R^i is placed in S_{AB}. Thus, Alice obtains a binary sequence, S_{AB}, whose length is $2n + 2m$. Alice converts the binary sequence S_{AB} into a sequence of single photons, Q_A, according to the following rules: (1) binary bits $\{0, 1\}$ in S_A encode into the Z-basis $\{|0\rangle, |1\rangle\}$, and (2) binary bits $\{0, 1\}$ in S_D and S_R encode into the X-basis $\left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$. Then, Alice sends Q_A to Bob one bit at a time through a quantum channel.

Step 3. Bob receives single photons and distinguishes between S_A, S_D, and S_R based on K_1. For each received single photon belonging to S_A or S_R, Bob measures the single photon in the Z-basis and resends the same single photon in the Z-basis based on the measurement result. Otherwise, the received single photon belongs to S_D and Bob reflects a single photon without any interference back to Alice.

Step 4. When Alice receives a sequence of single photons, Q'_A, from Bob, she measures the photons belonging to S'_A in the Z-basis and the photons belonging to S'_D or S'_R in the X-basis. Alice can perform the eavesdropping check as follows: (1) The measurement results of S'_A and S'_D are equal to those of the initial states S_A and S_D. (2) The measurement result of S'_R is not completely equal to that of the initial state S_R (i.e., the measurement result is random). Meanwhile, Bob also calculates $H_{K_2}(SK\prime) = H_{K_2}(SK)\prime$ to identify the secret key sent by Alice. If all the checking steps were passed, the protocol is completed. Otherwise, the communication is aborted.

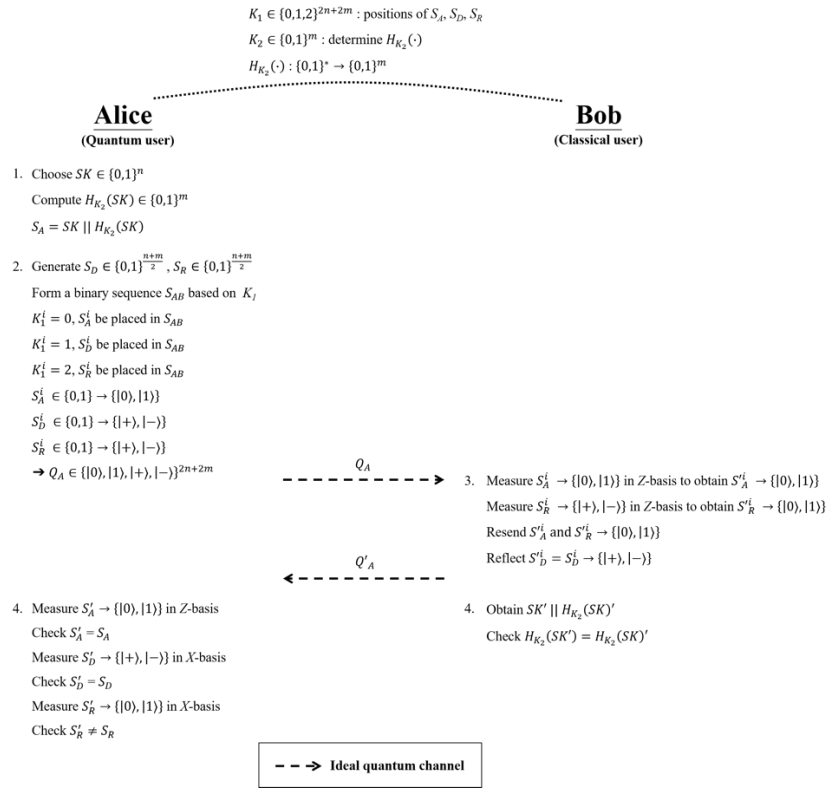

Figure 1. The proposed ASQKD protocol.

In Step 4, Alice performs an eavesdropping check. If the measurement result of S'_R is the same as the original S_R, then a reflecting attack exists during the transmission of the protocol. That is, if $S'_R = S_R$, Alice is aware that Bob did not measure S_R, indicating that the transmission is suffering a reflecting attack. Alice can detect this attack herself without Bob's information. Moreover, Bob authenticates Alice by calculating $H_{K_2}(SK\prime) = H_{K_2}(SK)\prime$. Thus, the proposed ASQKD protocol can effectively avoid reflecting attacks and does not require a classical channel.

5. Security Analysis

In this section, the security analysis of the proposed ASQKD protocol is presented from five perspectives: (1) the reflecting attack and (2) ordinary eavesdropping, (3) collective attack, (4) intercept and resend attack, and (5) measure and resend attack. The security of the proposed protocol is based on Chang et al.'s ASQKD protocol. This has been proven to be robust in a study by Chang et al. [50].

5.1. Security against the Reflecting Attack

If Eve performs the reflecting attack on the proposed ASQKD protocol by directly sending Q_A, as described in Section 3.2, then the attack will be detected in Step 4 because of the use of the measurement uncertainty of the single photon. Eve does not know the positions of S_A, S_D, and S_R when intercepting Q_A in Step 2 and directly resends Q_A to Alice. If S_A, S_D, and S_R can pass the eavesdropping check, Eve can forge Bob's identity. However, without knowing the positions of S_A, S_D, and S_R, Eve can be detected from the eavesdropping check. Therefore, Eve cannot perform a reflective attack to forge Bob's identity.

In the proposed ASQKD protocol, Alice generates a single photon as the checking qubit in the S_R using the X-basis (i.e., $\left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$). When Bob receives the photon, he measures the checking qubit in the S_R using a Z-basis (i.e., $\{|0\rangle, |1\rangle\}$) and resends the same state to Alice. Alice receives and measures the checking qubit in $S\prime_R$ using an X-basis. If the checking qubit is always the same as the initial state, Alice indicates that Bob does not receive and measure-resends the photon based on the measurement uncertainty of the single photon. Thus, the protocol suffers from a reflective attack. Otherwise, Alice would acknowledge that Bob received and measure-resend it. Thus, the proposed protocol can effectively avoid reflecting attacks and does not require a classical channel.

5.2. Security against the Ordinary Eavesdropping

Chang et al.'s ASQKD protocol is resistant to ordinary eavesdropping because Eve cannot measure the S_A and S_D sequences without being detected. To avoid an ordinary eavesdropping attack, the proposed ASQKD protocol uses S_A and S_D (i.e., $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$) in Step 2 to guarantee the correctness of the encoded photons between Alice and Bob. However, based on quantum no-cloning theory [51], we know that the four single-photons $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$ cannot be unambiguously discriminated. For example, without knowing the bases in advance, some errors will later be detected during the eavesdropping check if Eve measures single photons. Hence, regardless of the attack strategy Eve performs, she will be detected in the eavesdropping check (a similar security analysis was proposed in [50]).

5.3. Security against the Collective Attack

This section provides proof that the proposed ASQKD protocol can be secure against the collective attack and does not leak any information if there is no error detected.

In the attack strategy, suppose Eve possesses full quantum abilities with unlimited computational power and controls the quantum channel. Eve tries to eavesdrop on any useful information from Alice and Bob by performing the collective attack. Eve generates a quantum state $|E_1\rangle$ and performs a unitary operation, U_E, on the joint state $|q\rangle \otimes |E_1\rangle$, where $|q\rangle$ represents the transmitting qubit between Alice and Bob in Step 2. After the prepared qubits $|E_1\rangle$ entangle with the qubits sent from Alice in Step 2, Eve can infer the private information based on the measurement result of $|E_1\rangle$.

Theorem 1. *Eve performs the collective attack on the qubit that is sent to Bob. In order to do so, Eve applies a unitary operation, U_E, on the qubit that complies with the theorems of quantum mechanics. However, no unitary operation exists in the collective attack that allows Eve to obtain the information of Alice's secret without being detected.*

Proof of Theorem 1. Suppose Eve uses a unitary operator to attack the transmit qubit from Alice to Bob in Step 2 by U_E, the possibilities can be defined as follows:

$$\begin{aligned}
U_E|000\rangle|E_1\rangle = {} & a_{A1}|000\rangle|i_{A1}\rangle + a_{A2}|001\rangle|i_{A2}\rangle + a_{A3}|010\rangle|i_{A3}\rangle + a_{A4}|011\rangle|i_{A4}\rangle + a_{A5}|100\rangle|i_{A5}\rangle + a_{A6}|101\rangle|i_{A6}\rangle \\
& + a_{A7}|110\rangle|i_{A7}\rangle + a_{A8}|111\rangle|i_{A8}\rangle \\
U_E|001\rangle|E_1\rangle = {} & b_{A1}|000\rangle|j_{A1}\rangle + b_{A2}|001\rangle|j_{A2}\rangle + b_{A3}|010\rangle|j_{A3}\rangle + b_{A4}|011\rangle|j_{A4}\rangle + b_{A5}|100\rangle|j_{A5}\rangle + b_{A6}|101\rangle|j_{A6}\rangle \\
& + b_{A7}|110\rangle|j_{A7}\rangle + b_{A8}|111\rangle|j_{A8}\rangle \\
U_E|010\rangle|E_1\rangle = {} & c_{A1}|000\rangle|k_{A1}\rangle + c_{A2}|001\rangle|k_{A2}\rangle + c_{A3}|010\rangle|k_{A3}\rangle + c_{A4}|011\rangle|k_{A4}\rangle + c_{A5}|100\rangle|k_{A5}\rangle \\
& + c_{A6}|101\rangle|k_{A6}\rangle + c_{A7}|110\rangle|kh_{A7}\rangle + c_{A8}|111\rangle|k_{A8}\rangle \\
U_E|011\rangle|E_1\rangle = {} & d_{A1}|000\rangle|l_{A1}\rangle + d_{A2}|001\rangle|l_{A2}\rangle + d_{A3}|010\rangle|l_{A3}\rangle + d_{A4}|011\rangle|l_{A4}\rangle + d_{A5}|100\rangle|l_{A5}\rangle + d_{A6}|101\rangle|l_{A6}\rangle \\
& + d_{A7}|110\rangle|l_{A7}\rangle + d_{A8}|111\rangle|l_{A8}\rangle \\
U_E|100\rangle|E_1\rangle = {} & e_{A1}|000\rangle|m\rangle + e_{A2}|001\rangle|m_{A2}\rangle + e_{A3}|010\rangle|m_{A3}\rangle + e_{A4}|011\rangle|m_{A4}\rangle + e_{A5}|100\rangle|m_{A5}\rangle \\
& + e_{A6}|101\rangle|m_{A6}\rangle + e_{A7}|110\rangle|m_{A7}\rangle + e_{A8}|111\rangle|m_{A8}\rangle \\
U_E|101\rangle|E_1\rangle = {} & f_{A1}|000\rangle|n_{A1}\rangle + f_{A2}|001\rangle|n_{A2}\rangle + f_{A3}|010\rangle|n_{A3}\rangle + f_{A4}|011\rangle|n_{A4}\rangle + f_{A5}|100\rangle|n_{A5}\rangle \\
& + f_{A6}|101\rangle|n_{A6}\rangle + f_{A7}|110\rangle|n_{A7}\rangle + f_{A8}|111\rangle|n_{A8}\rangle \\
U_E|110\rangle|E_1\rangle = {} & g_{A1}|000\rangle|p_{A1}\rangle + g_{A2}|001\rangle|p_{A2}\rangle + g_{A3}|010\rangle|p_{A3}\rangle + g_{A4}|011\rangle|p_{A4}\rangle + g_{A5}|100\rangle|p_{A5}\rangle \\
& + g_{A6}|101\rangle|p_{A6}\rangle + g_{A7}|110\rangle|p_{A7}\rangle + g_{A8}|111\rangle|p_{A8}\rangle \\
U_E|111\rangle|E_1\rangle = {} & h_{A1}|000\rangle|r_{A1}\rangle + h_{A2}|001\rangle|r_{A2}\rangle + h_{A3}|010\rangle|r_{A3}\rangle + h_{A4}|011\rangle|r_{A4}\rangle + h_{A5}|100\rangle|r_{A5}\rangle \\
& + h_{A6}|101\rangle|r_{A6}\rangle + h_{A7}|110\rangle|r_{A7}\rangle + h_{A8}|111\rangle|r_{A8}\rangle
\end{aligned}$$

$|i_{Ai}\rangle, |j_{Ai}\rangle, |k_{Ai}\rangle, |l_{Ai}\rangle, |m_{Ai}\rangle, |n_{Ai}\rangle, |p_{Ai}\rangle, |r_{Ai}\rangle$ represent Eve's quantum states after the attack.

Alice will send 24 different pairs of qubits as follows: $|0++\rangle, |0+-\rangle, |0-+\rangle, |0--\rangle, |+0+\rangle, |+0-\rangle, |-0+\rangle, |-0-\rangle, |++0\rangle, |+-0\rangle, |-+0\rangle, |--0\rangle, |1++\rangle, |1+-\rangle, |1-+\rangle, |1--\rangle, |+1+\rangle, |+1-\rangle, |-1+\rangle, |-1-\rangle, |++1\rangle, |+-1\rangle, |-+1\rangle, |--1\rangle$. The possibilities can be denoted as follows:

$$\begin{aligned}
U_E|0++\rangle|E_1\rangle = {} & \tfrac{1}{2}(a_{A1}|000\rangle|i_{A1}\rangle + a_{A2}|001\rangle|i_{A2}\rangle + a_{A3}|010\rangle|i_{A3}\rangle \\
& + a_{A4}|011\rangle|i_{A4}\rangle + a_{A5}|100\rangle|i_{A5}\rangle + a_{A6}|101\rangle|i_{A6}\rangle \\
& + a_{A7}|110\rangle|i_{A7}\rangle + a_{A8}|111\rangle|i_{A8}\rangle) \\
& + \tfrac{1}{2}(b_{A1}|000\rangle|j_{A1}\rangle + b_{A2}|001\rangle|j_{A2}\rangle + b_{A3}|010\rangle|j_{A3}\rangle \\
& + b_{A4}|011\rangle|j_{A4}\rangle + b_{A5}|100\rangle|j_{A5}\rangle + b_{A6}|101\rangle|j_{A6}\rangle \\
& + b_{A7}|110\rangle|j_{A7}\rangle + b_{A8}|111\rangle|j_{A8}\rangle) \\
& + \tfrac{1}{2}(c_{A1}|000\rangle|k_{A1}\rangle + c_{A2}|001\rangle|k_{A2}\rangle + c_{A3}|010\rangle|k_{A3}\rangle \\
& + c_{A4}|011\rangle|k_{A4}\rangle + c_{A5}|100\rangle|k_{A5}\rangle + c_{A6}|101\rangle|k_{A6}\rangle \\
& + c_{A7}|110\rangle|kh_{A7}\rangle + c_{A8}|111\rangle|k_{A8}\rangle) + \tfrac{1}{2}(d_{A1}|000\rangle|l_{A1}\rangle \\
& + d_{A2}|001\rangle|l_{A2}\rangle + d_{A3}|010\rangle|l_{A3}\rangle + d_{A4}|011\rangle|l_{A4}\rangle \\
& + d_{A5}|100\rangle|l_{A5}\rangle + d_{A6}|101\rangle|l_{A6}\rangle + d_{A7}|110\rangle|l_{A7}\rangle \\
& + d_{A8}|111\rangle|l_{A8}\rangle) \\
U_E|0+-\rangle|E_1\rangle = {} & \tfrac{1}{2}(a_{A1}|000\rangle|i_{A1}\rangle + a_{A2}|001\rangle|i_{A2}\rangle + a_{A3}|010\rangle|i_{A3}\rangle \\
& + a_{A4}|011\rangle|i_{A4}\rangle + a_{A5}|100\rangle|i_{A5}\rangle + a_{A6}|101\rangle|i_{A6}\rangle \\
& + a_{A7}|110\rangle|i_{A7}\rangle + a_{A8}|111\rangle|i_{A8}\rangle) \\
& - \tfrac{1}{2}(b_{A1}|000\rangle|j_{A1}\rangle + b_{A2}|001\rangle|j_{A2}\rangle + b_{A3}|010\rangle|j_{A3}\rangle \\
& + b_{A4}|011\rangle|j_{A4}\rangle + b_{A5}|100\rangle|j_{A5}\rangle + b_{A6}|101\rangle|j_{A6}\rangle \\
& + b_{A7}|110\rangle|j_{A7}\rangle + b_{A8}|111\rangle|j_{A8}\rangle) \\
& + \tfrac{1}{2}(c_{A1}|000\rangle|k_{A1}\rangle + c_{A2}|001\rangle|k_{A2}\rangle + c_{A3}|010\rangle|k_{A3}\rangle \\
& + c_{A4}|011\rangle|k_{A4}\rangle + c_{A5}|100\rangle|k_{A5}\rangle + c_{A6}|101\rangle|k_{A6}\rangle \\
& + c_{A7}|110\rangle|kh_{A7}\rangle + c_{A8}|111\rangle|k_{A8}\rangle) - \tfrac{1}{2}(d_{A1}|000\rangle|l_{A1}\rangle \\
& + d_{A2}|001\rangle|l_{A2}\rangle + d_{A3}|010\rangle|l_{A3}\rangle + d_{A4}|011\rangle|l_{A4}\rangle \\
& + d_{A5}|100\rangle|l_{A5}\rangle + d_{A6}|101\rangle|l_{A6}\rangle + d_{A7}|110\rangle|l_{A7}\rangle \\
& + d_{A8}|111\rangle|l_{A8}\rangle)
\end{aligned}$$

$$
\begin{aligned}
U_E|0-+\rangle|E_1\rangle = \; & \tfrac{1}{2}(a_{A1}|000\rangle|i_{A1}\rangle + a_{A2}|001\rangle|i_{A2}\rangle + a_{A3}|010\rangle|i_{A3}\rangle \\
& + a_{A4}|011\rangle|i_{A4}\rangle + a_{A5}|100\rangle|i_{A5}\rangle + a_{A6}|101\rangle|i_{A6}\rangle \\
& + a_{A7}|110\rangle|i_{A7}\rangle + a_{A8}|111\rangle|i_{A8}\rangle) \\
& + \tfrac{1}{2}(b_{A1}|000\rangle|j_{A1}\rangle + b_{A2}|001\rangle|j_{A2}\rangle + b_{A3}|010\rangle|j_{A3}\rangle \\
& + b_{A4}|011\rangle|j_{A4}\rangle + b_{A5}|100\rangle|j_{A5}\rangle + b_{A6}|101\rangle|j_{A6}\rangle \\
& + b_{A7}|110\rangle|j_{A7}\rangle + b_{A8}|111\rangle|j_{A8}\rangle) \\
& - \tfrac{1}{2}(c_{A1}|000\rangle|k_{A1}\rangle + c_{A2}|001\rangle|k_{A2}\rangle + c_{A3}|010\rangle|k_{A3}\rangle \\
& + c_{A4}|011\rangle|k_{A4}\rangle + c_{A5}|100\rangle|k_{A5}\rangle + c_{A6}|101\rangle|k_{A6}\rangle \\
& + c_{A7}|110\rangle|kh_{A7}\rangle + c_{A8}|111\rangle|k_{A8}\rangle) - \tfrac{1}{2}(d_{A1}|000\rangle|l_{A1}\rangle \\
& + d_{A2}|001\rangle|l_{A2}\rangle + d_{A3}|010\rangle|l_{A3}\rangle + d_{A4}|011\rangle|l_{A4}\rangle \\
& + d_{A5}|100\rangle|l_{A5}\rangle + d_{A6}|101\rangle|l_{A6}\rangle + d_{A7}|110\rangle|l_{A7}\rangle \\
& + d_{A8}|111\rangle|l_{A8}\rangle)
\end{aligned}
$$

$$
\begin{aligned}
U_E|0--\rangle|E_1\rangle = \; & \tfrac{1}{2}(a_{A1}|000\rangle|i_{A1}\rangle + a_{A2}|001\rangle|i_{A2}\rangle + a_{A3}|010\rangle|i_{A3}\rangle \\
& + a_{A4}|011\rangle|i_{A4}\rangle + a_{A5}|100\rangle|i_{A5}\rangle + a_{A6}|101\rangle|i_{A6}\rangle \\
& + a_{A7}|110\rangle|i_{A7}\rangle + a_{A8}|111\rangle|i_{A8}\rangle) \\
& - \tfrac{1}{2}(b_{A1}|000\rangle|j_{A1}\rangle + b_{A2}|001\rangle|j_{A2}\rangle + b_{A3}|010\rangle|j_{A3}\rangle \\
& + b_{A4}|011\rangle|j_{A4}\rangle + b_{A5}|100\rangle|j_{A5}\rangle + b_{A6}|101\rangle|j_{A6}\rangle \\
& + b_{A7}|110\rangle|j_{A7}\rangle + b_{A8}|111\rangle|j_{A8}\rangle) \\
& - \tfrac{1}{2}(c_{A1}|000\rangle|k_{A1}\rangle + c_{A2}|001\rangle|k_{A2}\rangle + c_{A3}|010\rangle|k_{A3}\rangle \\
& + c_{A4}|011\rangle|k_{A4}\rangle + c_{A5}|100\rangle|k_{A5}\rangle + c_{A6}|101\rangle|k_{A6}\rangle \\
& + c_{A7}|110\rangle|kh_{A7}\rangle + c_{A8}|111\rangle|k_{A8}\rangle) + \tfrac{1}{2}(d_{A1}|000\rangle|l_{A1}\rangle \\
& + d_{A2}|001\rangle|l_{A2}\rangle + d_{A3}|010\rangle|l_{A3}\rangle + d_{A4}|011\rangle|l_{A4}\rangle \\
& + d_{A5}|100\rangle|l_{A5}\rangle + d_{A6}|101\rangle|l_{A6}\rangle + d_{A7}|110\rangle|l_{A7}\rangle \\
& + d_{A8}|111\rangle|l_{A8}\rangle)
\end{aligned}
$$

$$
\begin{aligned}
U_E|+0+\rangle|E_1\rangle = \; & \tfrac{1}{2}(a_{A1}|000\rangle|i_{A1}\rangle + a_{A2}|001\rangle|i_{A2}\rangle + a_{A3}|010\rangle|i_{A3}\rangle \\
& + a_{A4}|011\rangle|i_{A4}\rangle + a_{A5}|100\rangle|i_{A5}\rangle + a_{A6}|101\rangle|i_{A6}\rangle \\
& + a_{A7}|110\rangle|i_{A7}\rangle + a_{A8}|111\rangle|i_{A8}\rangle) \\
& + \tfrac{1}{2}(b_{A1}|000\rangle|j_{A1}\rangle + b_{A2}|001\rangle|j_{A2}\rangle + b_{A3}|010\rangle|j_{A3}\rangle \\
& + b_{A4}|011\rangle|j_{A4}\rangle + b_{A5}|100\rangle|j_{A5}\rangle + b_{A6}|101\rangle|j_{A6}\rangle \\
& + b_{A7}|110\rangle|j_{A7}\rangle + b_{A8}|111\rangle|j_{A8}\rangle) \\
& + \tfrac{1}{2}(e_{A1}|000\rangle|m\rangle + e_{A2}|001\rangle|m_{A2}\rangle + e_{A3}|010\rangle|m_{A3}\rangle \\
& + e_{A4}|011\rangle|m_{A4}\rangle + e_{A5}|100\rangle|m_{A5}\rangle + e_{A6}|101\rangle|m_{A6}\rangle \\
& + e_{A7}|110\rangle|m_{A7}\rangle + e_{A8}|111\rangle|m_{A8}\rangle) + \tfrac{1}{2}(f_{A1}|000\rangle|n_{A1}\rangle \\
& + f_{A2}|001\rangle|n_{A2}\rangle + f_{A3}|010\rangle|n_{A3}\rangle + f_{A4}|011\rangle|n_{A4}\rangle \\
& + f_{A5}|100\rangle|n_{A5}\rangle + f_{A6}|101\rangle|n_{A6}\rangle + f_{A7}|110\rangle|n_{A7}\rangle \\
& + f_{A8}|111\rangle|n_{A8}\rangle)
\end{aligned}
$$

$$
\begin{aligned}
U_E|+0-\rangle|E_1\rangle = \; & \tfrac{1}{2}(a_{A1}|000\rangle|i_{A1}\rangle + a_{A2}|001\rangle|i_{A2}\rangle + a_{A3}|010\rangle|i_{A3}\rangle \\
& + a_{A4}|011\rangle|i_{A4}\rangle + a_{A5}|100\rangle|i_{A5}\rangle + a_{A6}|101\rangle|i_{A6}\rangle \\
& + a_{A7}|110\rangle|i_{A7}\rangle + a_{A8}|111\rangle|i_{A8}\rangle) \\
& - \tfrac{1}{2}(b_{A1}|000\rangle|j_{A1}\rangle + b_{A2}|001\rangle|j_{A2}\rangle + b_{A3}|010\rangle|j_{A3}\rangle \\
& + b_{A4}|011\rangle|j_{A4}\rangle + b_{A5}|100\rangle|j_{A5}\rangle + b_{A6}|101\rangle|j_{A6}\rangle \\
& + b_{A7}|110\rangle|j_{A7}\rangle + b_{A8}|111\rangle|j_{A8}\rangle) \\
& + \tfrac{1}{2}(e_{A1}|000\rangle|m\rangle + e_{A2}|001\rangle|m_{A2}\rangle + e_{A3}|010\rangle|m_{A3}\rangle \\
& + e_{A4}|011\rangle|m_{A4}\rangle + e_{A5}|100\rangle|m_{A5}\rangle + e_{A6}|101\rangle|m_{A6}\rangle \\
& + e_{A7}|110\rangle|m_{A7}\rangle + e_{A8}|111\rangle|m_{A8}\rangle) - \tfrac{1}{2}(f_{A1}|000\rangle|n_{A1}\rangle \\
& + f_{A2}|001\rangle|n_{A2}\rangle + f_{A3}|010\rangle|n_{A3}\rangle + f_{A4}|011\rangle|n_{A4}\rangle \\
& + f_{A5}|100\rangle|n_{A5}\rangle + f_{A6}|101\rangle|n_{A6}\rangle + f_{A7}|110\rangle|n_{A7}\rangle \\
& + f_{A8}|111\rangle|n_{A8}\rangle)
\end{aligned}
$$

$$
\begin{aligned}
U_E|-0+\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(a_{A1}|000\rangle\,|i_{A1}\rangle + a_{A2}|001\rangle\,|i_{A2}\rangle + a_{A3}|010\rangle\,|i_{A3}\rangle \\
&+a_{A4}|011\rangle\,|i_{A4}\rangle + a_{A5}|100\rangle\,|i_{A5}\rangle + a_{A6}|101\rangle\,|i_{A6}\rangle \\
&+a_{A7}|110\rangle\,|i_{A7}\rangle + a_{A8}|111\rangle\,|i_{A8}\rangle\,) \\
&+\tfrac{1}{2}(b_{A1}|000\rangle\,|j_{A1}\rangle + b_{A2}|001\rangle\,|j_{A2}\rangle + b_{A3}|010\rangle\,|j_{A3}\rangle \\
&+b_{A4}|011\rangle\,|j_{A4}\rangle + b_{A5}|100\rangle\,|j_{A5}\rangle + b_{A6}|101\rangle\,|j_{A6}\rangle \\
&+b_{A7}|110\rangle\,|j_{A7}\rangle + b_{A8}|111\rangle\,|j_{A8}\rangle\,) \\
&-\tfrac{1}{2}(e_{A1}|000\rangle\,|m\rangle + e_{A2}|001\rangle\,|m_{A2}\rangle + e_{A3}|010\rangle\,|m_{A3}\rangle \\
&+e_{A4}|011\rangle\,|m_{A4}\rangle + e_{A5}|100\rangle\,|m_{A5}\rangle + e_{A6}|101\rangle\,|m_{A6}\rangle \\
&+e_{A7}|110\rangle\,|m_{A7}\rangle + e_{A8}|111\rangle\,|m_{A8}\rangle\,) - \tfrac{1}{2}(f_{A1}|000\rangle\,|n_{A1}\rangle \\
&+f_{A2}|001\rangle\,|n_{A2}\rangle + f_{A3}|010\rangle\,|n_{A3}\rangle + f_{A4}|011\rangle\,|n_{A4}\rangle \\
&+f_{A5}|100\rangle\,|n_{A5}\rangle + f_{A6}|101\rangle\,|n_{A6}\rangle + f_{A7}|110\rangle\,|n_{A7}\rangle \\
&+f_{A8}|111\rangle\,|n_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|-0-\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(a_{A1}|000\rangle\,|i_{A1}\rangle + a_{A2}|001\rangle\,|i_{A2}\rangle + a_{A3}|010\rangle\,|i_{A3}\rangle \\
&+a_{A4}|011\rangle\,|i_{A4}\rangle + a_{A5}|100\rangle\,|i_{A5}\rangle + a_{A6}|101\rangle\,|i_{A6}\rangle \\
&+a_{A7}|110\rangle\,|i_{A7}\rangle + a_{A8}|111\rangle\,|i_{A8}\rangle\,) \\
&+\tfrac{1}{2}(b_{A1}|000\rangle\,|j_{A1}\rangle + b_{A2}|001\rangle\,|j_{A2}\rangle + b_{A3}|010\rangle\,|j_{A3}\rangle \\
&+b_{A4}|011\rangle\,|j_{A4}\rangle + b_{A5}|100\rangle\,|j_{A5}\rangle + b_{A6}|101\rangle\,|j_{A6}\rangle \\
&+b_{A7}|110\rangle\,|j_{A7}\rangle + b_{A8}|111\rangle\,|j_{A8}\rangle\,) \\
&-\tfrac{1}{2}(e_{A1}|000\rangle\,|m\rangle + e_{A2}|001\rangle\,|m_{A2}\rangle + e_{A3}|010\rangle\,|m_{A3}\rangle \\
&+e_{A4}|011\rangle\,|m_{A4}\rangle + e_{A5}|100\rangle\,|m_{A5}\rangle + e_{A6}|101\rangle\,|m_{A6}\rangle \\
&+e_{A7}|110\rangle\,|m_{A7}\rangle + e_{A8}|111\rangle\,|m_{A8}\rangle\,) + \tfrac{1}{2}(f_{A1}|000\rangle\,|n_{A1}\rangle \\
&+f_{A2}|001\rangle\,|n_{A2}\rangle + f_{A3}|010\rangle\,|n_{A3}\rangle + f_{A4}|011\rangle\,|n_{A4}\rangle \\
&+f_{A5}|100\rangle\,|n_{A5}\rangle + f_{A6}|101\rangle\,|n_{A6}\rangle + f_{A7}|110\rangle\,|n_{A7}\rangle \\
&+f_{A8}|111\rangle\,|n_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|++0\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(a_{A1}|000\rangle\,|i_{A1}\rangle + a_{A2}|001\rangle\,|i_{A2}\rangle + a_{A3}|010\rangle\,|i_{A3}\rangle \\
&+a_{A4}|011\rangle\,|i_{A4}\rangle + a_{A5}|100\rangle\,|i_{A5}\rangle + a_{A6}|101\rangle\,|i_{A6}\rangle \\
&+a_{A7}|110\rangle\,|i_{A7}\rangle + a_{A8}|111\rangle\,|i_{A8}\rangle\,) \\
&+\tfrac{1}{2}(c_{A1}|000\rangle\,|k_{A1}\rangle + c_{A2}|001\rangle\,|k_{A2}\rangle + c_{A3}|010\rangle\,|k_{A3}\rangle \\
&+c_{A4}|011\rangle\,|k_{A4}\rangle + c_{A5}|100\rangle\,|k_{A5}\rangle + c_{A6}|101\rangle\,|k_{A6}\rangle \\
&+c_{A7}|110\rangle\,|kh_{A7}\rangle + c_{A8}|111\rangle\,|k_{A8}\rangle\,) \\
&+\tfrac{1}{2}(e_{A1}|000\rangle\,|m\rangle + e_{A2}|001\rangle\,|m_{A2}\rangle + e_{A3}|010\rangle\,|m_{A3}\rangle \\
&+e_{A4}|011\rangle\,|m_{A4}\rangle + e_{A5}|100\rangle\,|m_{A5}\rangle + e_{A6}|101\rangle\,|m_{A6}\rangle \\
&+e_{A7}|110\rangle\,|m_{A7}\rangle + e_{A8}|111\rangle\,|m_{A8}\rangle\,) + \tfrac{1}{2}(g_{A1}|000\rangle\,|p_{A1}\rangle \\
&+g_{A2}|001\rangle\,|p_{A2}\rangle + g_{A3}|010\rangle\,|p_{A3}\rangle + g_{A4}|011\rangle\,|p_{A4}\rangle \\
&+g_{A5}|100\rangle\,|p_{A5}\rangle + g_{A6}|101\rangle\,|p_{A6}\rangle + g_{A7}|110\rangle\,|p_{A7}\rangle \\
&+g_{A8}|111\rangle\,|p_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|+-0\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(a_{A1}|000\rangle\,|i_{A1}\rangle + a_{A2}|001\rangle\,|i_{A2}\rangle + a_{A3}|010\rangle\,|i_{A3}\rangle \\
&+a_{A4}|011\rangle\,|i_{A4}\rangle + a_{A5}|100\rangle\,|i_{A5}\rangle + a_{A6}|101\rangle\,|i_{A6}\rangle \\
&+a_{A7}|110\rangle\,|i_{A7}\rangle + a_{A8}|111\rangle\,|i_{A8}\rangle\,) \\
&-\tfrac{1}{2}(c_{A1}|000\rangle\,|k_{A1}\rangle + c_{A2}|001\rangle\,|k_{A2}\rangle + c_{A3}|010\rangle\,|k_{A3}\rangle \\
&+c_{A4}|011\rangle\,|k_{A4}\rangle + c_{A5}|100\rangle\,|k_{A5}\rangle + c_{A6}|101\rangle\,|k_{A6}\rangle \\
&+c_{A7}|110\rangle\,|kh_{A7}\rangle + c_{A8}|111\rangle\,|k_{A8}\rangle\,) \\
&+\tfrac{1}{2}(e_{A1}|000\rangle\,|m\rangle + e_{A2}|001\rangle\,|m_{A2}\rangle + e_{A3}|010\rangle\,|m_{A3}\rangle \\
&+e_{A4}|011\rangle\,|m_{A4}\rangle + e_{A5}|100\rangle\,|m_{A5}\rangle + e_{A6}|101\rangle\,|m_{A6}\rangle \\
&+e_{A7}|110\rangle\,|m_{A7}\rangle + e_{A8}|111\rangle\,|m_{A8}\rangle\,) - \tfrac{1}{2}(g_{A1}|000\rangle\,|p_{A1}\rangle \\
&+g_{A2}|001\rangle\,|p_{A2}\rangle + g_{A3}|010\rangle\,|p_{A3}\rangle + g_{A4}|011\rangle\,|p_{A4}\rangle \\
&+g_{A5}|100\rangle\,|p_{A5}\rangle + g_{A6}|101\rangle\,|p_{A6}\rangle + g_{A7}|110\rangle\,|p_{A7}\rangle \\
&+g_{A8}|111\rangle\,|p_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|-+0\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(a_{A1}|000\rangle\,|i_{A1}\rangle + a_{A2}|001\rangle\,|i_{A2}\rangle + a_{A3}|010\rangle\,|i_{A3}\rangle \\
&+a_{A4}|011\rangle\,|i_{A4}\rangle + a_{A5}|100\rangle\,|i_{A5}\rangle + a_{A6}|101\rangle\,|i_{A6}\rangle \\
&+a_{A7}|110\rangle\,|i_{A7}\rangle + a_{A8}|111\rangle\,|i_{A8}\rangle\,) \\
&+\tfrac{1}{2}(c_{A1}|000\rangle\,|k_{A1}\rangle + c_{A2}|001\rangle\,|k_{A2}\rangle + c_{A3}|010\rangle\,|k_{A3}\rangle \\
&+c_{A4}|011\rangle\,|k_{A4}\rangle + c_{A5}|100\rangle\,|k_{A5}\rangle + c_{A6}|101\rangle\,|k_{A6}\rangle \\
&+c_{A7}|110\rangle\,|kh_{A7}\rangle + c_{A8}|111\rangle\,|k_{A8}\rangle\,) \\
&-\tfrac{1}{2}(e_{A1}|000\rangle\,|m\rangle + e_{A2}|001\rangle\,|m_{A2}\rangle + e_{A3}|010\rangle\,|m_{A3}\rangle \\
&+e_{A4}|011\rangle\,|m_{A4}\rangle + e_{A5}|100\rangle\,|m_{A5}\rangle + e_{A6}|101\rangle\,|m_{A6}\rangle \\
&+e_{A7}|110\rangle\,|m_{A7}\rangle + e_{A8}|111\rangle\,|m_{A8}\rangle\,) - \tfrac{1}{2}(g_{A1}|000\rangle\,|p_{A1}\rangle \\
&+g_{A2}|001\rangle\,|p_{A2}\rangle + g_{A3}|010\rangle\,|p_{A3}\rangle + g_{A4}|011\rangle\,|p_{A4}\rangle \\
&+g_{A5}|100\rangle\,|p_{A5}\rangle + g_{A6}|101\rangle\,|p_{A6}\rangle + g_{A7}|110\rangle\,|p_{A7}\rangle \\
&+g_{A8}|111\rangle\,|p_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|--0\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(a_{A1}|000\rangle\,|i_{A1}\rangle + a_{A2}|001\rangle\,|i_{A2}\rangle + a_{A3}|010\rangle\,|i_{A3}\rangle \\
&+a_{A4}|011\rangle\,|i_{A4}\rangle + a_{A5}|100\rangle\,|i_{A5}\rangle + a_{A6}|101\rangle\,|i_{A6}\rangle \\
&+a_{A7}|110\rangle\,|i_{A7}\rangle + a_{A8}|111\rangle\,|i_{A8}\rangle\,) \\
&-\tfrac{1}{2}(c_{A1}|000\rangle\,|k_{A1}\rangle + c_{A2}|001\rangle\,|k_{A2}\rangle + c_{A3}|010\rangle\,|k_{A3}\rangle \\
&+c_{A4}|011\rangle\,|k_{A4}\rangle + c_{A5}|100\rangle\,|k_{A5}\rangle + c_{A6}|101\rangle\,|k_{A6}\rangle \\
&+c_{A7}|110\rangle\,|kh_{A7}\rangle + c_{A8}|111\rangle\,|k_{A8}\rangle\,) \\
&-\tfrac{1}{2}(e_{A1}|000\rangle\,|m\rangle + e_{A2}|001\rangle\,|m_{A2}\rangle + e_{A3}|010\rangle\,|m_{A3}\rangle \\
&+e_{A4}|011\rangle\,|m_{A4}\rangle + e_{A5}|100\rangle\,|m_{A5}\rangle + e_{A6}|101\rangle\,|m_{A6}\rangle \\
&+e_{A7}|110\rangle\,|m_{A7}\rangle + e_{A8}|111\rangle\,|m_{A8}\rangle\,) + \tfrac{1}{2}(g_{A1}|000\rangle\,|p_{A1}\rangle \\
&+g_{A2}|001\rangle\,|p_{A2}\rangle + g_{A3}|010\rangle\,|p_{A3}\rangle + g_{A4}|011\rangle\,|p_{A4}\rangle \\
&+g_{A5}|100\rangle\,|p_{A5}\rangle + g_{A6}|101\rangle\,|p_{A6}\rangle + g_{A7}|110\rangle\,|p_{A7}\rangle \\
&+g_{A8}|111\rangle\,|p_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|1++\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(e_{A1}|000\rangle\,|m\rangle + e_{A2}|001\rangle\,|m_{A2}\rangle + e_{A3}|010\rangle\,|m_{A3}\rangle \\
&+e_{A4}|011\rangle\,|m_{A4}\rangle + e_{A5}|100\rangle\,|m_{A5}\rangle + e_{A6}|101\rangle\,|m_{A6}\rangle \\
&+e_{A7}|110\rangle\,|m_{A7}\rangle + e_{A8}|111\rangle\,|m_{A8}\rangle\,) \\
&+\tfrac{1}{2}(f_{A1}|000\rangle\,|n_{A1}\rangle + f_{A2}|001\rangle\,|n_{A2}\rangle + f_{A3}|010\rangle\,|n_{A3}\rangle \\
&+f_{A4}|011\rangle\,|n_{A4}\rangle + f_{A5}|100\rangle\,|n_{A5}\rangle + f_{A6}|101\rangle\,|n_{A6}\rangle \\
&+f_{A7}|110\rangle\,|n_{A7}\rangle + f_{A8}|111\rangle\,|n_{A8}\rangle\,) \\
&+\tfrac{1}{2}(g_{A1}|000\rangle\,|p_{A1}\rangle + g_{A2}|001\rangle\,|p_{A2}\rangle + g_{A3}|010\rangle\,|p_{A3}\rangle \\
&+g_{A4}|011\rangle\,|p_{A4}\rangle + g_{A5}|100\rangle\,|p_{A5}\rangle + g_{A6}|101\rangle\,|p_{A6}\rangle \\
&+g_{A7}|110\rangle\,|p_{A7}\rangle + g_{A8}|111\rangle\,|p_{A8}\rangle\,) + \tfrac{1}{2}(h_{A1}|000\rangle\,|r_{A1}\rangle \\
&+h_{A2}|001\rangle\,|r_{A2}\rangle + h_{A3}|010\rangle\,|r_{A3}\rangle + h_{A4}|011\rangle\,|r_{A4}\rangle \\
&+h_{A5}|100\rangle\,|r_{A5}\rangle + h_{A6}|101\rangle\,|r_{A6}\rangle + h_{A7}|110\rangle\,|r_{A7}\rangle \\
&+h_{A8}|111\rangle\,|r_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|1+-\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(e_{A1}|000\rangle\,|m\rangle + e_{A2}|001\rangle\,|m_{A2}\rangle + e_{A3}|010\rangle\,|m_{A3}\rangle \\
&+e_{A4}|011\rangle\,|m_{A4}\rangle + e_{A5}|100\rangle\,|m_{A5}\rangle + e_{A6}|101\rangle\,|m_{A6}\rangle \\
&+e_{A7}|110\rangle\,|m_{A7}\rangle + e_{A8}|111\rangle\,|m_{A8}\rangle\,) \\
&-\tfrac{1}{2}(f_{A1}|000\rangle\,|n_{A1}\rangle + f_{A2}|001\rangle\,|n_{A2}\rangle + f_{A3}|010\rangle\,|n_{A3}\rangle \\
&+f_{A4}|011\rangle\,|n_{A4}\rangle + f_{A5}|100\rangle\,|n_{A5}\rangle + f_{A6}|101\rangle\,|n_{A6}\rangle \\
&+f_{A7}|110\rangle\,|n_{A7}\rangle + f_{A8}|111\rangle\,|n_{A8}\rangle\,) \\
&+\tfrac{1}{2}(g_{A1}|000\rangle\,|p_{A1}\rangle + g_{A2}|001\rangle\,|p_{A2}\rangle + g_{A3}|010\rangle\,|p_{A3}\rangle \\
&+g_{A4}|011\rangle\,|p_{A4}\rangle + g_{A5}|100\rangle\,|p_{A5}\rangle + g_{A6}|101\rangle\,|p_{A6}\rangle \\
&+g_{A7}|110\rangle\,|p_{A7}\rangle + g_{A8}|111\rangle\,|p_{A8}\rangle\,) - \tfrac{1}{2}(h_{A1}|000\rangle\,|r_{A1}\rangle \\
&+h_{A2}|001\rangle\,|r_{A2}\rangle + h_{A3}|010\rangle\,|r_{A3}\rangle + h_{A4}|011\rangle\,|r_{A4}\rangle \\
&+h_{A5}|100\rangle\,|r_{A5}\rangle + h_{A6}|101\rangle\,|r_{A6}\rangle + h_{A7}|110\rangle\,|r_{A7}\rangle \\
&+h_{A8}|111\rangle\,|r_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|1-+\rangle|E_1\rangle = \; & \tfrac{1}{2}(e_{A1}|000\rangle|m\rangle + e_{A2}|001\rangle|m_{A2}\rangle + e_{A3}|010\rangle|m_{A3}\rangle \\
& + e_{A4}|011\rangle|m_{A4}\rangle + e_{A5}|100\rangle|m_{A5}\rangle + e_{A6}|101\rangle|m_{A6}\rangle \\
& + e_{A7}|110\rangle|m_{A7}\rangle + e_{A8}|111\rangle|m_{A8}\rangle) \\
& + \tfrac{1}{2}(f_{A1}|000\rangle|n_{A1}\rangle + f_{A2}|001\rangle|n_{A2}\rangle + f_{A3}|010\rangle|n_{A3}\rangle \\
& + f_{A4}|011\rangle|n_{A4}\rangle + f_{A5}|100\rangle|n_{A5}\rangle + f_{A6}|101\rangle|n_{A6}\rangle \\
& + f_{A7}|110\rangle|n_{A7}\rangle + f_{A8}|111\rangle|n_{A8}\rangle) \\
& - \tfrac{1}{2}(g_{A1}|000\rangle|p_{A1}\rangle + g_{A2}|001\rangle|p_{A2}\rangle + g_{A3}|010\rangle|p_{A3}\rangle \\
& + g_{A4}|011\rangle|p_{A4}\rangle + g_{A5}|100\rangle|p_{A5}\rangle + g_{A6}|101\rangle|p_{A6}\rangle \\
& + g_{A7}|110\rangle|p_{A7}\rangle + g_{A8}|111\rangle|p_{A8}\rangle) - \tfrac{1}{2}(h_{A1}|000\rangle|r_{A1}\rangle \\
& + h_{A2}|001\rangle|r_{A2}\rangle + h_{A3}|010\rangle|r_{A3}\rangle + h_{A4}|011\rangle|r_{A4}\rangle \\
& + h_{A5}|100\rangle|r_{A5}\rangle + h_{A6}|101\rangle|r_{A6}\rangle + h_{A7}|110\rangle|r_{A7}\rangle \\
& + h_{A8}|111\rangle|r_{A8}\rangle)
\end{aligned}
$$

$$
\begin{aligned}
U_E|1--\rangle|E_1\rangle = \; & \tfrac{1}{2}(e_{A1}|000\rangle|m\rangle + e_{A2}|001\rangle|m_{A2}\rangle + e_{A3}|010\rangle|m_{A3}\rangle \\
& + e_{A4}|011\rangle|m_{A4}\rangle + e_{A5}|100\rangle|m_{A5}\rangle + e_{A6}|101\rangle|m_{A6}\rangle \\
& + e_{A7}|110\rangle|m_{A7}\rangle + e_{A8}|111\rangle|m_{A8}\rangle) \\
& - \tfrac{1}{2}(f_{A1}|000\rangle|n_{A1}\rangle + f_{A2}|001\rangle|n_{A2}\rangle + f_{A3}|010\rangle|n_{A3}\rangle \\
& + f_{A4}|011\rangle|n_{A4}\rangle + f_{A5}|100\rangle|n_{A5}\rangle + f_{A6}|101\rangle|n_{A6}\rangle \\
& + f_{A7}|110\rangle|n_{A7}\rangle + f_{A8}|111\rangle|n_{A8}\rangle) \\
& - \tfrac{1}{2}(g_{A1}|000\rangle|p_{A1}\rangle + g_{A2}|001\rangle|p_{A2}\rangle + g_{A3}|010\rangle|p_{A3}\rangle \\
& + g_{A4}|011\rangle|p_{A4}\rangle + g_{A5}|100\rangle|p_{A5}\rangle + g_{A6}|101\rangle|p_{A6}\rangle \\
& + g_{A7}|110\rangle|p_{A7}\rangle + g_{A8}|111\rangle|p_{A8}\rangle) + \tfrac{1}{2}(h_{A1}|000\rangle|r_{A1}\rangle \\
& + h_{A2}|001\rangle|r_{A2}\rangle + h_{A3}|010\rangle|r_{A3}\rangle + h_{A4}|011\rangle|r_{A4}\rangle \\
& + h_{A5}|100\rangle|r_{A5}\rangle + h_{A6}|101\rangle|r_{A6}\rangle + h_{A7}|110\rangle|r_{A7}\rangle \\
& + h_{A8}|111\rangle|r_{A8}\rangle)
\end{aligned}
$$

$$
\begin{aligned}
U_E|+1+\rangle|E_1\rangle = \; & \tfrac{1}{2}(c_{A1}|000\rangle|k_{A1}\rangle + c_{A2}|001\rangle|k_{A2}\rangle + c_{A3}|010\rangle|k_{A3}\rangle \\
& + c_{A4}|011\rangle|k_{A4}\rangle + c_{A5}|100\rangle|k_{A5}\rangle + c_{A6}|101\rangle|k_{A6}\rangle \\
& + c_{A7}|110\rangle|kh_{A7}\rangle + c_{A8}|111\rangle|k_{A8}\rangle) \\
& + \tfrac{1}{2}(d_{A1}|000\rangle|l_{A1}\rangle + d_{A2}|001\rangle|l_{A2}\rangle + d_{A3}|010\rangle|l_{A3}\rangle \\
& + d_{A4}|011\rangle|l_{A4}\rangle + d_{A5}|100\rangle|l_{A5}\rangle + d_{A6}|101\rangle|l_{A6}\rangle \\
& + d_{A7}|110\rangle|l_{A7}\rangle + d_{A8}|111\rangle|l_{A8}\rangle) \\
& + \tfrac{1}{2}(g_{A1}|000\rangle|p_{A1}\rangle + g_{A2}|001\rangle|p_{A2}\rangle + g_{A3}|010\rangle|p_{A3}\rangle \\
& + g_{A4}|011\rangle|p_{A4}\rangle + g_{A5}|100\rangle|p_{A5}\rangle + g_{A6}|101\rangle|p_{A6}\rangle \\
& + g_{A7}|110\rangle|p_{A7}\rangle + g_{A8}|111\rangle|p_{A8}\rangle) + \tfrac{1}{2}(h_{A1}|000\rangle|r_{A1}\rangle \\
& + h_{A2}|001\rangle|r_{A2}\rangle + h_{A3}|010\rangle|r_{A3}\rangle + h_{A4}|011\rangle|r_{A4}\rangle \\
& + h_{A5}|100\rangle|r_{A5}\rangle + h_{A6}|101\rangle|r_{A6}\rangle + h_{A7}|110\rangle|r_{A7}\rangle \\
& + h_{A8}|111\rangle|r_{A8}\rangle)
\end{aligned}
$$

$$
\begin{aligned}
U_E|+1-\rangle|E_1\rangle = \; & \tfrac{1}{2}(c_{A1}|000\rangle|k_{A1}\rangle + c_{A2}|001\rangle|k_{A2}\rangle + c_{A3}|010\rangle|k_{A3}\rangle \\
& + c_{A4}|011\rangle|k_{A4}\rangle + c_{A5}|100\rangle|k_{A5}\rangle + c_{A6}|101\rangle|k_{A6}\rangle \\
& + c_{A7}|110\rangle|kh_{A7}\rangle + c_{A8}|111\rangle|k_{A8}\rangle) \\
& - \tfrac{1}{2}(d_{A1}|000\rangle|l_{A1}\rangle + d_{A2}|001\rangle|l_{A2}\rangle + d_{A3}|010\rangle|l_{A3}\rangle \\
& + d_{A4}|011\rangle|l_{A4}\rangle + d_{A5}|100\rangle|l_{A5}\rangle + d_{A6}|101\rangle|l_{A6}\rangle \\
& + d_{A7}|110\rangle|l_{A7}\rangle + d_{A8}|111\rangle|l_{A8}\rangle) \\
& + \tfrac{1}{2}(g_{A1}|000\rangle|p_{A1}\rangle + g_{A2}|001\rangle|p_{A2}\rangle + g_{A3}|010\rangle|p_{A3}\rangle \\
& + g_{A4}|011\rangle|p_{A4}\rangle + g_{A5}|100\rangle|p_{A5}\rangle + g_{A6}|101\rangle|p_{A6}\rangle \\
& + g_{A7}|110\rangle|p_{A7}\rangle + g_{A8}|111\rangle|p_{A8}\rangle) - \tfrac{1}{2}(h_{A1}|000\rangle|r_{A1}\rangle \\
& + h_{A2}|001\rangle|r_{A2}\rangle + h_{A3}|010\rangle|r_{A3}\rangle + h_{A4}|011\rangle|r_{A4}\rangle \\
& + h_{A5}|100\rangle|r_{A5}\rangle + h_{A6}|101\rangle|r_{A6}\rangle + h_{A7}|110\rangle|r_{A7}\rangle \\
& + h_{A8}|111\rangle|r_{A8}\rangle)
\end{aligned}
$$

$$
\begin{aligned}
U_E|-1+\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(c_{A1}|000\rangle\,|k_{A1}\rangle + c_{A2}|001\rangle\,|k_{A2}\rangle + c_{A3}|010\rangle\,|k_{A3}\rangle \\
&+c_{A4}|011\rangle\,|k_{A4}\rangle + c_{A5}|100\rangle\,|k_{A5}\rangle + c_{A6}|101\rangle\,|k_{A6}\rangle \\
&+c_{A7}|110\rangle\,|kh_{A7}\rangle + c_{A8}|111\rangle\,|k_{A8}\rangle\,) \\
&+\tfrac{1}{2}(d_{A1}|000\rangle\,|l_{A1}\rangle + d_{A2}|001\rangle\,|l_{A2}\rangle + d_{A3}|010\rangle\,|l_{A3}\rangle \\
&+d_{A4}|011\rangle\,|l_{A4}\rangle + d_{A5}|100\rangle\,|l_{A5}\rangle + d_{A6}|101\rangle\,|l_{A6}\rangle \\
&+d_{A7}|110\rangle\,|l_{A7}\rangle + d_{A8}|111\rangle\,|l_{A8}\rangle\,) \\
&-\tfrac{1}{2}(g_{A1}|000\rangle\,|p_{A1}\rangle + g_{A2}|001\rangle\,|p_{A2}\rangle + g_{A3}|010\rangle\,|p_{A3}\rangle \\
&+g_{A4}|011\rangle\,|p_{A4}\rangle + g_{A5}|100\rangle\,|p_{A5}\rangle + g_{A6}|101\rangle\,|p_{A6}\rangle \\
&+g_{A7}|110\rangle\,|p_{A7}\rangle + g_{A8}|111\rangle\,|p_{A8}\rangle\,) - \tfrac{1}{2}(h_{A1}|000\rangle\,|r_{A1}\rangle \\
&+h_{A2}|001\rangle\,|r_{A2}\rangle + h_{A3}|010\rangle\,|r_{A3}\rangle + h_{A4}|011\rangle\,|r_{A4}\rangle \\
&+h_{A5}|100\rangle\,|r_{A5}\rangle + h_{A6}|101\rangle\,|r_{A6}\rangle + h_{A7}|110\rangle\,|r_{A7}\rangle \\
&+h_{A8}|111\rangle\,|r_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|-1-\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(c_{A1}|000\rangle\,|k_{A1}\rangle + c_{A2}|001\rangle\,|k_{A2}\rangle + c_{A3}|010\rangle\,|k_{A3}\rangle \\
&+c_{A4}|011\rangle\,|k_{A4}\rangle + c_{A5}|100\rangle\,|k_{A5}\rangle + c_{A6}|101\rangle\,|k_{A6}\rangle \\
&+c_{A7}|110\rangle\,|kh_{A7}\rangle + c_{A8}|111\rangle\,|k_{A8}\rangle\,) \\
&-\tfrac{1}{2}(d_{A1}|000\rangle\,|l_{A1}\rangle + d_{A2}|001\rangle\,|l_{A2}\rangle + d_{A3}|010\rangle\,|l_{A3}\rangle \\
&+d_{A4}|011\rangle\,|l_{A4}\rangle + d_{A5}|100\rangle\,|l_{A5}\rangle + d_{A6}|101\rangle\,|l_{A6}\rangle \\
&+d_{A7}|110\rangle\,|l_{A7}\rangle + d_{A8}|111\rangle\,|l_{A8}\rangle\,) \\
&-\tfrac{1}{2}(g_{A1}|000\rangle\,|p_{A1}\rangle + g_{A2}|001\rangle\,|p_{A2}\rangle + g_{A3}|010\rangle\,|p_{A3}\rangle \\
&+g_{A4}|011\rangle\,|p_{A4}\rangle + g_{A5}|100\rangle\,|p_{A5}\rangle + g_{A6}|101\rangle\,|p_{A6}\rangle \\
&+g_{A7}|110\rangle\,|p_{A7}\rangle + g_{A8}|111\rangle\,|p_{A8}\rangle\,) + \tfrac{1}{2}(h_{A1}|000\rangle\,|r_{A1}\rangle \\
&+h_{A2}|001\rangle\,|r_{A2}\rangle + h_{A3}|010\rangle\,|r_{A3}\rangle + h_{A4}|011\rangle\,|r_{A4}\rangle \\
&+h_{A5}|100\rangle\,|r_{A5}\rangle + h_{A6}|101\rangle\,|r_{A6}\rangle + h_{A7}|110\rangle\,|r_{A7}\rangle \\
&+h_{A8}|111\rangle\,|r_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|++1\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(b_{A1}|000\rangle\,|j_{A1}\rangle + b_{A2}|001\rangle\,|j_{A2}\rangle + b_{A3}|010\rangle\,|j_{A3}\rangle \\
&+b_{A4}|011\rangle\,|j_{A4}\rangle + b_{A5}|100\rangle\,|j_{A5}\rangle + b_{A6}|101\rangle\,|j_{A6}\rangle \\
&+b_{A7}|110\rangle\,|j_{A7}\rangle + b_{A8}|111\rangle\,|j_{A8}\rangle\,) \\
&+\tfrac{1}{2}(d_{A1}|000\rangle\,|l_{A1}\rangle + d_{A2}|001\rangle\,|l_{A2}\rangle + d_{A3}|010\rangle\,|l_{A3}\rangle \\
&+d_{A4}|011\rangle\,|l_{A4}\rangle + d_{A5}|100\rangle\,|l_{A5}\rangle + d_{A6}|101\rangle\,|l_{A6}\rangle \\
&+d_{A7}|110\rangle\,|l_{A7}\rangle + d_{A8}|111\rangle\,|l_{A8}\rangle\,) \\
&+\tfrac{1}{2}(f_{A1}|000\rangle\,|n_{A1}\rangle + f_{A2}|001\rangle\,|n_{A2}\rangle + f_{A3}|010\rangle\,|n_{A3}\rangle \\
&+f_{A4}|011\rangle\,|n_{A4}\rangle + f_{A5}|100\rangle\,|n_{A5}\rangle + f_{A6}|101\rangle\,|n_{A6}\rangle \\
&+f_{A7}|110\rangle\,|n_{A7}\rangle + f_{A8}|111\rangle\,|n_{A8}\rangle\,) + \tfrac{1}{2}(h_{A1}|000\rangle\,|r_{A1}\rangle \\
&+h_{A2}|001\rangle\,|r_{A2}\rangle + h_{A3}|010\rangle\,|r_{A3}\rangle + h_{A4}|011\rangle\,|r_{A4}\rangle \\
&+h_{A5}|100\rangle\,|r_{A5}\rangle + h_{A6}|101\rangle\,|r_{A6}\rangle + h_{A7}|110\rangle\,|r_{A7}\rangle \\
&+h_{A8}|111\rangle\,|r_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|+-1\rangle\,|E_1\rangle \;=\;& \tfrac{1}{2}(b_{A1}|000\rangle\,|j_{A1}\rangle + b_{A2}|001\rangle\,|j_{A2}\rangle + b_{A3}|010\rangle\,|j_{A3}\rangle \\
&+b_{A4}|011\rangle\,|j_{A4}\rangle + b_{A5}|100\rangle\,|j_{A5}\rangle + b_{A6}|101\rangle\,|j_{A6}\rangle \\
&+b_{A7}|110\rangle\,|j_{A7}\rangle + b_{A8}|111\rangle\,|j_{A8}\rangle\,) \\
&-\tfrac{1}{2}(d_{A1}|000\rangle\,|l_{A1}\rangle + d_{A2}|001\rangle\,|l_{A2}\rangle + d_{A3}|010\rangle\,|l_{A3}\rangle \\
&+d_{A4}|011\rangle\,|l_{A4}\rangle + d_{A5}|100\rangle\,|l_{A5}\rangle + d_{A6}|101\rangle\,|l_{A6}\rangle \\
&+d_{A7}|110\rangle\,|l_{A7}\rangle + d_{A8}|111\rangle\,|l_{A8}\rangle\,) \\
&+\tfrac{1}{2}(f_{A1}|000\rangle\,|n_{A1}\rangle + f_{A2}|001\rangle\,|n_{A2}\rangle + f_{A3}|010\rangle\,|n_{A3}\rangle \\
&+f_{A4}|011\rangle\,|n_{A4}\rangle + f_{A5}|100\rangle\,|n_{A5}\rangle + f_{A6}|101\rangle\,|n_{A6}\rangle \\
&+f_{A7}|110\rangle\,|n_{A7}\rangle + f_{A8}|111\rangle\,|n_{A8}\rangle\,) - \tfrac{1}{2}(h_{A1}|000\rangle\,|r_{A1}\rangle \\
&+h_{A2}|001\rangle\,|r_{A2}\rangle + h_{A3}|010\rangle\,|r_{A3}\rangle + h_{A4}|011\rangle\,|r_{A4}\rangle \\
&+h_{A5}|100\rangle\,|r_{A5}\rangle + h_{A6}|101\rangle\,|r_{A6}\rangle + h_{A7}|110\rangle\,|r_{A7}\rangle \\
&+h_{A8}|111\rangle\,|r_{A8}\rangle\,)
\end{aligned}
$$

$$
\begin{aligned}
U_E|-+1\rangle|E_1\rangle = \; & \tfrac{1}{2}(b_{A1}|000\rangle|j_{A1}\rangle + b_{A2}|001\rangle|j_{A2}\rangle + b_{A3}|010\rangle|j_{A3}\rangle \\
& + b_{A4}|011\rangle|j_{A4}\rangle + b_{A5}|100\rangle|j_{A5}\rangle + b_{A6}|101\rangle|j_{A6}\rangle \\
& + b_{A7}|110\rangle|j_{A7}\rangle + b_{A8}|111\rangle|j_{A8}\rangle) \\
& + \tfrac{1}{2}(d_{A1}|000\rangle|l_{A1}\rangle + d_{A2}|001\rangle|l_{A2}\rangle + d_{A3}|010\rangle|l_{A3}\rangle \\
& + d_{A4}|011\rangle|l_{A4}\rangle + d_{A5}|100\rangle|l_{A5}\rangle + d_{A6}|101\rangle|l_{A6}\rangle \\
& + d_{A7}|110\rangle|l_{A7}\rangle + d_{A8}|111\rangle|l_{A8}\rangle) \\
& - \tfrac{1}{2}(f_{A1}|000\rangle|n_{A1}\rangle + f_{A2}|001\rangle|n_{A2}\rangle + f_{A3}|010\rangle|n_{A3}\rangle \\
& + f_{A4}|011\rangle|n_{A4}\rangle + f_{A5}|100\rangle|n_{A5}\rangle + f_{A6}|101\rangle|n_{A6}\rangle \\
& + f_{A7}|110\rangle|n_{A7}\rangle + f_{A8}|111\rangle|n_{A8}\rangle) - \tfrac{1}{2}(h_{A1}|000\rangle|r_{A1}\rangle \\
& + h_{A2}|001\rangle|r_{A2}\rangle + h_{A3}|010\rangle|r_{A3}\rangle + h_{A4}|011\rangle|r_{A4}\rangle \\
& + h_{A5}|100\rangle|r_{A5}\rangle + h_{A6}|101\rangle|r_{A6}\rangle + h_{A7}|110\rangle|r_{A7}\rangle \\
& + h_{A8}|111\rangle|r_{A8}\rangle)
\end{aligned}
$$

$$
\begin{aligned}
U_E|--1\rangle|E_1\rangle = \; & \tfrac{1}{2}(b_{A1}|000\rangle|j_{A1}\rangle + b_{A2}|001\rangle|j_{A2}\rangle + b_{A3}|010\rangle|j_{A3}\rangle \\
& + b_{A4}|011\rangle|j_{A4}\rangle + b_{A5}|100\rangle|j_{A5}\rangle + b_{A6}|101\rangle|j_{A6}\rangle \\
& + b_{A7}|110\rangle|j_{A7}\rangle + b_{A8}|111\rangle|i_{A8}\rangle) \\
& - \tfrac{1}{2}(d_{A1}|000\rangle|l_{A1}\rangle + d_{A2}|001\rangle|l_{A2}\rangle + d_{A3}|010\rangle|l_{A3}\rangle \\
& + d_{A4}|011\rangle|l_{A4}\rangle + d_{A5}|100\rangle|l_{A5}\rangle + d_{A6}|101\rangle|l_{A6}\rangle \\
& + d_{A7}|110\rangle|l_{A7}\rangle + d_{A8}|111\rangle|l_{A8}\rangle) \\
& - \tfrac{1}{2}(f_{A1}|000\rangle|n_{A1}\rangle + f_{A2}|001\rangle|n_{A2}\rangle + f_{A3}|010\rangle|n_{A3}\rangle \\
& + f_{A4}|011\rangle|n_{A4}\rangle + f_{A5}|100\rangle|n_{A5}\rangle + f_{A6}|101\rangle|n_{A6}\rangle \\
& + f_{A7}|110\rangle|n_{A7}\rangle + f_{A8}|111\rangle|n_{A8}\rangle) + \tfrac{1}{2}(h_{A1}|000\rangle|r_{A1}\rangle \\
& + h_{A2}|001\rangle|r_{A2}\rangle + h_{A3}|010\rangle|r_{A3}\rangle + h_{A4}|011\rangle|r_{A4}\rangle \\
& + h_{A5}|100\rangle|r_{A5}\rangle + h_{A6}|101\rangle|r_{A6}\rangle + h_{A7}|110\rangle|r_{A7}\rangle \\
& + h_{A8}|111\rangle|r_{A8}\rangle)
\end{aligned}
$$

After the prepared qubits $|E_1\rangle$ entangle with the qubits sent from Alice in Step 2, Eve can infer the information of transmitting qubit $|q\rangle$ by the corresponding measurement result of $|E_1\rangle$. However, after Bob receives the attacked qubits, he will measure S_A in the Z-basis. Bob then abstracts $SK \,||\, H_{K_2}(SK)$ from S_A and calculates $H_{K_2}(SK\prime) = H_{K_2}(SK)\prime$ to identify that the secret key sent by Alice has not been modified. Thus, to pass the detection, Eve will not modify the value of Z-basis qubits, which restricts the possibilities of U_E. The restricted U_E can be defined as follows:

$$U_E|0++\rangle|E_1\rangle = \frac{1}{2}(|000\rangle|i_{A1}\rangle + |001\rangle|j_{A2}\rangle + |010\rangle|k_{A3}\rangle + |011\rangle|l_{A4}\rangle)$$

$$U_E|0+-\rangle|E_1\rangle = \frac{1}{2}(|000\rangle|i_{A1}\rangle - |001\rangle|j_{A2}\rangle + |010\rangle|k_{A3}\rangle - |011\rangle|l_{A4}\rangle)$$

$$U_E|0-+\rangle|E_1\rangle = \frac{1}{2}(|000\rangle|i_{A1}\rangle + |001\rangle|j_{A2}\rangle - |010\rangle|k_{A3}\rangle - |011\rangle|l_{A4}\rangle)$$

$$U_E|0--\rangle|E_1\rangle = \frac{1}{2}(|000\rangle|i_{A1}\rangle - |001\rangle|j_{A2}\rangle - |010\rangle|k_{A3}\rangle + |011\rangle|l_{A4}\rangle)$$

$$U_E|+0+\rangle|E_1\rangle = \frac{1}{2}(|000\rangle|i_{A1}\rangle - |001\rangle|j_{A2}\rangle + |100\rangle|m_{A5}\rangle - |101\rangle|n_{A6}\rangle)$$

$$U_E|+0-\rangle|E_1\rangle = \frac{1}{2}(|000\rangle|i_{A1}\rangle - |001\rangle|j_{A2}\rangle + |100\rangle|m_{A5}\rangle - |101\rangle|n_{A6}\rangle)$$

$$U_E|-0+\rangle|E_1\rangle = \frac{1}{2}(|000\rangle|i_{A1}\rangle + |001\rangle|j_{A2}\rangle - |100\rangle|m_{A5}\rangle - |101\rangle|n_{A6}\rangle)$$

$$U_E|-0-\rangle|E_1\rangle = \frac{1}{2}(|000\rangle|i_{A1}\rangle + |001\rangle|j_{A2}\rangle - |100\rangle|m_{A5}\rangle + |101\rangle|n_{A6}\rangle)$$

$$U_E|++0\rangle|E_1\rangle = \frac{1}{2}(|000\rangle|i_{A1}\rangle + |010\rangle|k_{A3}\rangle + |100\rangle|m_{A5}\rangle + |110\rangle|p_{A7}\rangle)$$

$$
\begin{aligned}
U_E|+-0\rangle|E_1\rangle &= \frac{1}{2}(|000\rangle|i_{A1}\rangle - |010\rangle|k_{A3}\rangle + |100\rangle|m_{A5}\rangle - |110\rangle|p_{A7}\rangle)\\
U_E|-+0\rangle|E_1\rangle &= \frac{1}{2}(|000\rangle|i_{A1}\rangle + |010\rangle|k_{A3}\rangle - |100\rangle|m_{A5}\rangle - |110\rangle|p_{A7}\rangle)\\
U_E|--0\rangle|E_1\rangle &= \frac{1}{2}(|000\rangle|i_{A1}\rangle - |010\rangle|k_{A3}\rangle - |100\rangle|m_{A5}\rangle + |110\rangle|p_{A7}\rangle)\\
U_E|1++\rangle|E_1\rangle &= \frac{1}{2}(|100\rangle|m_{A5}\rangle + |101\rangle|n_{A6}\rangle + |110\rangle|p_{A7}\rangle + |111\rangle|r_{A8}\rangle)\\
U_E|1+-\rangle|E_1\rangle &= \frac{1}{2}(|100\rangle|m_{A5}\rangle - |101\rangle|n_{A6}\rangle + |110\rangle|p_{A7}\rangle - |111\rangle|r_{A8}\rangle)\\
U_E|1-+\rangle|E_1\rangle &= \frac{1}{2}(|100\rangle|m_{A5}\rangle + |101\rangle|n_{A6}\rangle - |110\rangle|p_{A7}\rangle - |111\rangle|r_{A8}\rangle)\\
U_E|1--\rangle|E_1\rangle &= \frac{1}{2}(|100\rangle|m_{A5}\rangle - |101\rangle|n_{A6}\rangle - |110\rangle|p_{A7}\rangle + |111\rangle|r_{A8}\rangle)\\
U_E|+1+\rangle|E_1\rangle &= \frac{1}{2}(|010\rangle|k_{A3}\rangle + |011\rangle|l_{A4}\rangle + |110\rangle|p_{A7}\rangle + |111\rangle|r_{A8}\rangle)\\
U_E|+1-\rangle|E_1\rangle &= \frac{1}{2}(|010\rangle|k_{A3}\rangle - |011\rangle|l_{A4}\rangle + |110\rangle|p_{A7}\rangle - |111\rangle|r_{A8}\rangle)\\
U_E|-1+\rangle|E_1\rangle &= \frac{1}{2}(|010\rangle|k_{A3}\rangle + |011\rangle|l_{A4}\rangle - |110\rangle|p_{A7}\rangle - |111\rangle|r_{A8}\rangle)\\
U_E|-1-\rangle|E_1\rangle &= \frac{1}{2}(|010\rangle|k_{A3}\rangle - |011\rangle|l_{A4}\rangle - |110\rangle|p_{A7}\rangle + |111\rangle|r_{A8}\rangle)\\
U_E|++1\rangle|E_1\rangle &= \frac{1}{2}(|001\rangle|j_{A2}\rangle + |011\rangle|l_{A4}\rangle + |101\rangle|n_{A6}\rangle + |111\rangle|r_{A8}\rangle)\\
U_E|+-1\rangle|E_1\rangle &= \frac{1}{2}(|001\rangle|j_{A2}\rangle - |011\rangle|l_{A4}\rangle + |101\rangle|n_{A6}\rangle - |111\rangle|r_{A8}\rangle)\\
U_E|-+1\rangle|E_1\rangle &= \frac{1}{2}(|001\rangle|j_{A2}\rangle + |011\rangle|l_{A4}\rangle - |101\rangle|n_{A6}\rangle - |111\rangle|r_{A8}\rangle)\\
U_E|--1\rangle|E_1\rangle &= \frac{1}{2}(|001\rangle|j_{A2}\rangle - |011\rangle|l_{A4}\rangle - |101\rangle|n_{A6}\rangle + |111\rangle|r_{A8}\rangle)
\end{aligned}
$$

In Step 4, Alice will check all the received qubits, and if the measurement results are not equal to the original states, Alice will detect the eavesdropping. To pass the detection, $|q\rangle$ must be the same as the original states (i.e., $|i_{A1}\rangle \neq |j_{A2}\rangle \neq |k_{A3}\rangle \neq |l_{A4}\rangle \neq |m_{A5}\rangle \neq |n_{A6}\rangle \neq |p_{A7}\rangle \neq |r_{A8}\rangle$), which can be denoted as follows:

$$
\begin{aligned}
U_E|000\rangle|E_1\rangle &= |000\rangle|i_{A1}\rangle \qquad (1)\\
U_E|001\rangle|E_1\rangle &= |001\rangle|j_{A2}\rangle\\
U_E|010\rangle|E_1\rangle &= |010\rangle|k_{A3}\rangle\\
U_E|011\rangle|E_1\rangle &= |011\rangle|l_{A4}\rangle\\
U_E|100\rangle|E_1\rangle &= |100\rangle|m_{A5}\rangle\\
U_E|101\rangle|E_1\rangle &= |101\rangle|n_{A6}\rangle\\
U_E|110\rangle|E_1\rangle &= |110\rangle|p_{A7}\rangle\\
U_E|111\rangle|E_1\rangle &= |111\rangle|r_{A8}\rangle
\end{aligned}
$$

Accordingly, the measurement result of each state $|q\rangle$ has only one possibility in order to pass the detection from Alice. In other words, $|E_1\rangle$ must all be in the same state, which means $|i_{A1}\rangle = |j_{A2}\rangle = |k_{A3}\rangle = |l_{A4}\rangle = |m_{A5}\rangle = |n_{A6}\rangle = |p_{A7}\rangle = |r_{A8}\rangle$. Eventually,

all the $|E_1\rangle$ are identical, which proves that Eve cannot obtain any private information without detection by performing the collective attack. □

5.4. Security against the Intercept and Resend Attack

Assume Eve attempts to perform an intercept and resend attack on the traveling particles in Q_A, to obtain Alice's secret key, SK. To perform the attack, Eve intercepts S_A, S_D, and S_R and resends the fake single photons randomly chosen from four different states (i.e., $|0\rangle, |1\rangle, |+\rangle, |-\rangle$), trying to forge the identity of Alice in Step 2. In Step 4, Bob checks the hash value of SK, which infers that Eve must obtain all the particles' positions to pass the check. However, Eve does not know the corresponding positions of each photon in S_A, S_D, and S_R. Then, Eve has a probability of $\frac{1}{x!}$ to pass the eavesdropping check, where x represents the total number of Q_A (i.e., $x = 2n + 2m$ in the proposed ASQKD protocol). Thus, the probability for Eve to be detected in Step 4 is $1 - \frac{1}{x!}$. If x is large enough, the detection probability would converge to 1, as shown in Figure 2.

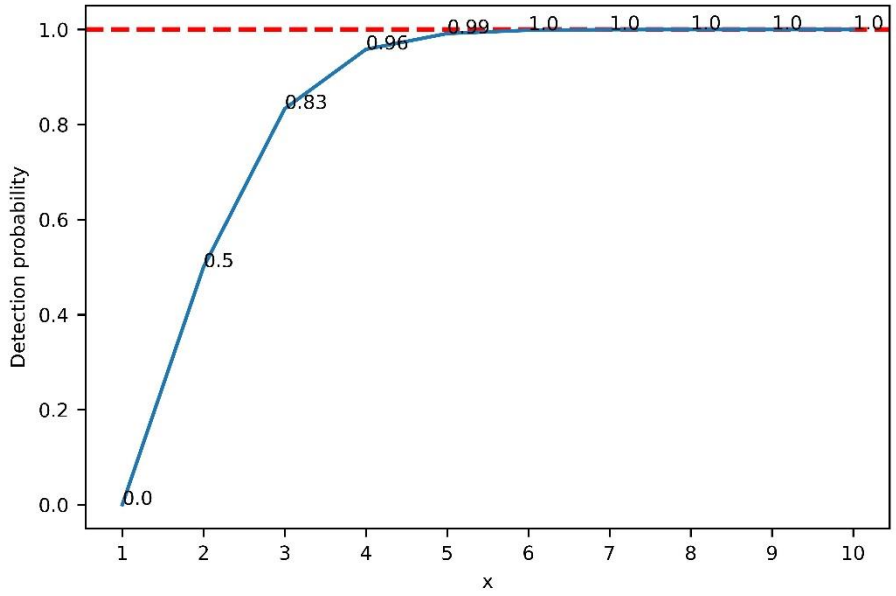

Figure 2. Detection probability of the intercept and resend attack.

5.5. Security against the Measure and Resend Attack

Suppose Eve performs a measure and resend attack on the traveling photons in Q_A, to obtain Alice's secret key, SK. Eve may try to measure Q_A, then resend the measured Q_A photons (or generate new photons based on the measure results) to Bob, hoping to obtain SK without being detected.

In Step 4, Bob checks the hash value of SK, if Eve measures the qubits with the wrong basis, the attack would be detected. Thus, Eve must measure the correct basis on the correct position to pass the eavesdropping check. However, Eve does not obtain the corresponding position of each photon in S_A, S_D, and S_R. Without the information, the probability of randomly measuring the qubits to pass the eavesdropping check in **Step 4** is $\frac{3}{4}$. Hence, the probability to detect the attack in this protocol is $1 - \left(\frac{3}{4}\right)^x$. If x is large enough, the detection rate would converge to 1, as shown in Figure 3.

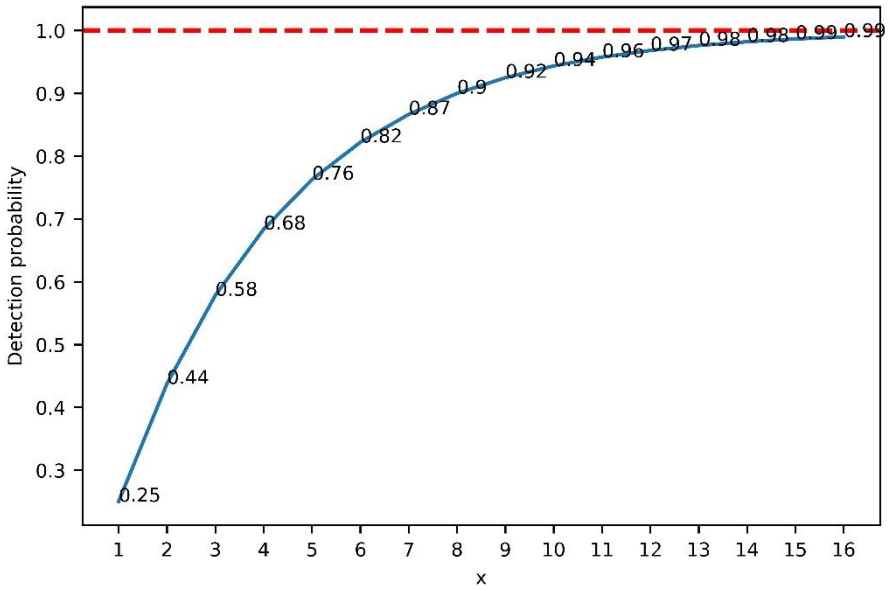

Figure 3. Detection probability of the measure and resend attack.

6. Efficiency Analysis

Table 1 compares several important features of the Yu et al. [45], Li et al. [46], Zebboudj et al. [48], and Chang et al. [50] measure-resend ASQKD protocols with the proposed ASQKD protocol.

Table 1. Comparison of [45,46,48,50] and the proposed ASQKD protocol.

	Yu et al.'s ASQKD Protocol [45]	**Li et al.'s ASQKD Protocol [46]**	**Zebboudj et al.'s ASQKD Protocol [48]**	**Chang et al.' ASQKD Protocol [50]**	**The Proposed ASQKD Protocol**
Semi-quantum environment	Measure-resend	Measure-resend	Measure-resend	Measure-resend	Measure-resend
Quantum capability of classical participant	(1) Generation (2) Measurement (3) Reflection	(1) Generation (2) Measurement (3) Reflection	(1) Generation (2) Measurement (3) Reflection	(1) Generation (2) Measurement (3) Reflection	(1) Generation (2) Measurement (3) Reflection
Quantum resource	Bell states	Bell states, single photons	Single photons	Single photons	Single photons
Quantum storage	Yes	Yes	No	No	No
Bell measurement	Yes	Yes	No	No	No
Communication efficiency	10%	11%	14%	17%	14%
Required pre-shared keys (in bits)	$3n + 3m$	$2n + 2m$	$2n + 2m$	$n + 2m$	$n + 2m$
Hash function	No	Public hash	Public hash	Secret hash	Secret hash
Vulnerability to reflecting attack	No	No	No	Yes	No
Required the classical channel	Yes	Yes	Yes	Yes	No

In the schemes of Yu et al. [45] and Li et al. [46], Alice shares the second qubit of Bell states to Bob. Alice then restores the qubit from Bob to perform Bell measurement, which requires the quantum storage to store the first qubit of Bell states and the hardware to perform the Bell measurement. Moreover, generating a pair of Bell states increases the need for advanced quantum hardware compared to a single photon. Therefore, the proposed protocol based on single photons does not require quantum storage and hardware of Bell measurement, significantly reducing the demand for advanced quantum hardware.

The communication efficiency of a quantum cryptographic protocol is defined as $\eta = \frac{c}{q}$, where c represents the sum of the shared classical secret bits and q denotes the sum of the generated photons in the protocol. Assume Alice chooses a binary string of length n

as the secret key. The length m of the hash value is assumed to be equal to that of the secret key (i.e., $n = m$).

In Yu et al.'s measure-resend ASQKD protocol, Alice prepares $2n + 2m$ Bell states (i.e., $2(2n + 2m)$ qubits). In share mode, Bob measures the second qubit in the Bell state and generates $n + m$ single photons. Therefore, the communication efficiency is $\frac{n}{2(2n+2m)+(n+m)} = 10\%$.

In Li et al.'s measure-resend ASQKD protocol, Alice prepares $n + m$ single photons and $n + m$ Bell states (i.e., $2(n + m)$ qubits). In measurement mode, Bob measures $n + m$ single photons and generates $n + m$ single photons. In addition, Bob measures the second qubit in the Bell state and generates $\frac{(n+m)}{2}$ single photons. Therefore, the communication efficiency is $\frac{n}{(n+m)+2(n+m)+(n+m)+\frac{(n+m)}{2}} = 11\%$.

In Zebboudj et al.'s measure-resend ASQKD protocol, Alice prepares $2n + 2m$ single photons. Bob measures and generates $\frac{3(2n+2m)}{4}$ single photons. Thus, the qubit efficiency of the proposed protocol is $\frac{n}{(2n+2m)+\frac{3(2n+2m)}{4}} = 14\%$.

In Chang et al.'s measure-resend ASQKD protocol, Alice prepares $2n + 2m$ single photons. In measurement mode, Bob generates $n + m$ single photons. Therefore, the communication efficiency is $\frac{n}{(2n+2m)+(n+m)} = 17\%$.

In the proposed measure-resend ASQKD protocol, Alice prepares $2n + 2m$ single photons. In measurement mode, Bob generates $n + m$ single photons in S'_A and $\frac{(n+m)}{2}$ single photons in S'_R. Thus, the communication efficiency of the proposed protocol is $\frac{n}{(2n+2m)+(n+m)+\frac{(n+m)}{2}} = 14\%$.

Compared with Yu et al. [45], Li et al. [46], and Zebboudj et al. [48], the proposed ASQKD protocol not only reduces the length of required pre-shared keys but also possesses an advantage in communication efficiency and applies the secret hash to strengthen the security. Compared with Chang et al. [50], although the communication efficiency of the proposed protocol is slightly lower, the proposed ASQKD protocol is not vulnerable to the reflecting attack and removes the need for the classical channel, elevating security and convenience.

7. Conclusions

This study discovered the possibility of a reflective attack in Chang et al.'s ASQKD protocol and proposed an efficient and secure ASQKD protocol. An eavesdropper can perform a reflecting attack to successfully forge the receiver's identity. Moreover, Chang et al.'s ASQKD protocol requires an authenticated classical channel between the sender and the receiver. It is considered illogical to have an authenticated channel required in the ASQKD protocol. Thus, the proposed ASQKD protocol revised the flaw of impersonation and illogical use of the authenticated classical channel. Accordingly, the proposed ASQKD protocol was shown to be secure under reflecting attacks, collective attacks, as well as several other well-known attacks. According to the comparative study, the proposed ASQKD protocol possesses multiple advantages, as follows: based on a single photon, it demands less advanced quantum devices, the communication efficiency is higher than most protocols, it reduces the length of the required pre-shared keys, endures reflecting attacks, collective attacks, and there is no need for the classical channel. Although the communication efficiency of the proposed ASQKD protocol was slightly lower than that of Chang et al.'s ASQKD protocol, a future challenge is the construction of an ASQKD protocol with a higher communication efficiency that can still remain immune to the reflecting attack in experimental tests.

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 Y.-Y.H.; formal analysis, C.-W.Y.; writing—original draft, H.-W.W. and J.L.; 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, MOST 110-2218-E-005-007-MBK, and MOST 110-2218-E-005-008-MBK), and China Medical University, Taiwan (Grant No. CMU110-S-21).

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. 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.
2. Bruß, D. Optimal Eavesdropping in Quantum Cryptography with Six States. *Phys. Rev. Lett.* **1998**, *81*, 3018–3021. [CrossRef]
3. Cerf, N.J.; Bourennane, M.; Karlsson, A.; Gisin, N. Security of Quantum Key Distribution Using d-Level Systems. *Phys. Rev. Lett.* **2002**, *88*, 127902. [CrossRef] [PubMed]
4. Long, G.; Liu, X. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **2002**, *65*, 032302. [CrossRef]
5. Grosshans, F.; Van Assche, G.; Wenger, J.; Brouri, R.; Cerf, N.J.; Grangier, P. Quantum key distribution using gaussian-modulated coherent states. *Nature* **2003**, *421*, 238. [CrossRef] [PubMed]
6. Hwang, W.-Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
7. Scarani, V.; Acín, A.; Ribordy, G.; Gisin, N. Quantum Cryptography Protocols Robust against Photon Number Splitting Attacks for Weak Laser Pulse Implementations. *Phys. Rev. Lett.* **2004**, *92*, 057901. [CrossRef]
8. Lo, H.K.; Ma, X.F.; Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **2005**, *94*, 4. [CrossRef]
9. Zhang, Z.J.; Man, Z.X.; Shi, S.H. An efficient multiparty quantum key distribution scheme. *Int. J. Quant. Infor.* **2005**, *3*, 555–560. [CrossRef]
10. 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]
11. Li, X.H.; Deng, F.G.; Zhou, H.Y. Efficient quantum key distribution over a collective noise channel. *Phys. Rev. A* **2008**, *78*, 022321. [CrossRef]
12. Lo, H.-K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef] [PubMed]
13. Lucamarini, M.; Patel, K.A.; Dynes, J.F.; Fröhlich, B.; Sharpe, A.W.; Dixon, A.R.; Yuan, Z.L.; Penty, R.V.; Shields, A.J. Efficient decoy-state quantum key distribution with quantified security. *Opt. Express* **2013**, *21*, 24550–24565. [CrossRef] [PubMed]
14. Boyer, M.; Kenigsberg, D.; Mor, T. Quantum Key Distribution with Classical Bob. *Phys. Rev. Lett.* **2007**, *99*, 140501. [CrossRef] [PubMed]
15. Boyer, M.; Gelles, R.; Kenigsberg, D.; Mor, T. Semiquantum key distribution. *Phys. Rev. A* **2009**, *79*, 032341. [CrossRef]
16. 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]
17. Wang, J.; Zhang, S.; Zhang, Q.; Tang, C.J. Semiquantum Key Distribution Using Entangled States. *Chinese Phys. Lett.* **2011**, *28*, 100301. [CrossRef]
18. Boyer, M.; Gelles, R.; Mor, T. Attacks on fixed-apparatus quantum-key-distribution schemes. *Phys. Rev. A* **2014**, *90*, 012329. [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. 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]
22. Krawec, W.O. Security of a semi-quantum protocol where reflections contribute to the secret key. *Quantum Inf. Process.* **2016**, *15*, 2067–2090. [CrossRef]
23. Li, Q.; Chan, W.H.; Zhang, S. Semiquantum key distribution with secure delegated quantum computation. *Sci. Rep.* **2016**, *6*, 19898. [CrossRef] [PubMed]
24. Boyer, M.; Katz, M.; Liss, R.; Mor, T. Experimentally feasible protocol for semiquantum key distribution. *Phys. Rev. A* **2017**, *96*, 062335. [CrossRef]
25. Boyer, M.; Liss, R.; Mor, T. Attacks against a Simplified Experimentally Feasible Semiquantum Key Distribution Protocol. *Entropy* **2018**, *20*, 536. [CrossRef]

26. Liu, Z.-R.; Hwang, T. Mediated Semi-Quantum Key Distribution Without Invoking Quantum Measurement. *Ann. Phys.* **2018**, *530*, 1700206. [CrossRef]
27. Zhang, W.; Qiu, D.; Mateus, P. Security of a single-state semi-quantum key distribution protocol. *Quantum Inf. Process.* **2018**, *17*, 135. [CrossRef]
28. 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]
29. Amer, O.; Krawec, W.O. Semiquantum key distribution with high quantum noise tolerance. *Phys. Rev. A* **2019**, *100*, 022319. [CrossRef]
30. Wang, M.-M.; Gong, L.-M.; Shao, L.-H. Efficient semiquantum key distribution without entanglement. *Quantum Inf. Process.* **2019**, *18*, 260. [CrossRef]
31. 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]
32. Boyer, M.; Liss, R.; Mor, T. Composable security against collective attacks of a modified BB84 QKD protocol with information only in one basis. *Theor. Comput. Sci.* **2020**, *801*, 96–109. [CrossRef]
33. Hajji, H.; El Baz, M. Qutrit-based semi-quantum key distribution protocol. *Quantum Inf. Process.* **2021**, *20*, 4. [CrossRef]
34. 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]
35. 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]
36. He, Q.; Yang, W.; Chen, B.; Huang, L. Cryptanalysis and improvement of the novel semi-quantum secret sharing scheme using entangled states. *Mod. Phys. Lett. B* **2019**, *32*, 1950045. [CrossRef]
37. 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]
38. Tsai, C.-W.; Chang, Y.-C.; Lai, Y.-H.; Yang, C.-W. Cryptanalysis of limited resource semi-quantum secret sharing. *Quantum Inf. Process.* **2020**, *19*, 224. [CrossRef]
39. 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]
40. Yang, C.-W.; Tsai, C.-W. Intercept-and-resend attack and improvement of semiquantum secure direct communication using EPR pairs. *Quantum Inf. Process.* **2019**, *18*, 306. [CrossRef]
41. Rong, Z.; Qiu, D.; Zou, X. Two single-state semi-quantum secure direct communication protocols based on single photons. *Int. J. Mod. Phys. B* **2020**, *34*, 2050106. [CrossRef]
42. Rong, Z.; Qiu, D.; Zou, X. Semi-Quantum Secure Direct Communication Using Entanglement. *Int. J. Theor. Phys.* **2020**, *59*, 1807–1819. [CrossRef]
43. Yang, C.-W. Efficient and secure semi-quantum secure direct communication protocol against double CNOT attack. *Quantum Inf. Process.* **2020**, *19*, 50. [CrossRef]
44. 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]
45. 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]
46. 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]
47. Meslouhi, A.; Hassouni, Y. Cryptanalysis on authenticated semi-quantum key distribution protocol using Bell states. *Quantum Inf. Process.* **2016**, *16*, 18. [CrossRef]
48. Zebboudj, S.; Djoudi, H.; Lalaoui, D.; Omar, M. Authenticated semi-quantum key distribution without entanglement. *Quantum Inf. Process.* **2020**, *19*, 77. [CrossRef]
49. Tsai, C.-W.; Yang, C.-W. Lightweight authenticated semi-quantum key distribution protocol without trojan horse attack. *Laser Phys. Lett.* **2020**, *17*, 075202. [CrossRef]
50. 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]
51. Wootters, W.K.; Zurek, W.H. A Single Quantum Cannot Be Cloned. *Nature* **1982**, *299*, 802–803. [CrossRef]