Measure-resend authenticated semi-quantum key distribution with single photons

Chun-Hao Chang · Yu-Chin Lu · Tzonelih Hwang

Abstract

This paper proposes a new measure-resend ASQKD protocol. The proposed ASQKD protocol uses only single photons, needs fewer pre-shared keys and even provides better qubit efficiency than the state-of-the-art ASQKD protocols. The security proof shows the robustness of the proposed protocol under the collective attack.

Keywords Quantum key distribution · Authenticated protocol · Semi-quantum · Measure-resend · Single photon

1 Introduction

The quantum key distribution (QKD) is an important research topic of quantum cryptography, allowing a secret key to be distributed on the quantum channel among participants. The first QKD, proposed in 1984, is called BB84 [1]. BB84 allows two participants, Alice and Bob, to share an unconditionally secure key with a quantum channel and a classical authentication channel. Since BB84, many QKD protocols have been proposed [2–10]. In 2007, Boyer et al. [5] first proposed the idea of semi-quantum key distribution (SQKD), in which Bob is a “classical” participant who can only perform three out of the following four operations: (1) measuring Z-basis qubits, (2) generating Z-basis qubits, (3) reordering qubits, and (4) reflecting qubits. In particular, the measure-resend SQKD proposed in [11] allows the classical user to
perform (1), (2), and (4) operations. All the QKD and SQKD protocols mentioned above have to assume the existence of an ideal classical authentication channel to do the public discussion to detect the existence of an attacker, Eve. In 2014, Yu et al. [12] proposed two authenticated semi-quantum key distribution (ASQKD) protocols using maximally entangled Bell states. The ASQKD uses pre-shared keys to do user authentication as well as key distribution, and hence the assumption of the existence of an ideal classical authentication channel can be removed here. In 2016, Li et al. [13] also proposed two ASQKD protocols using Bell states.

In this paper, a new ASQKD using single qubits instead of Bell states is proposed. The proposed protocol has the following features: First, only single photons are used. Second, the number of pre-shared keys is reduced. Third, the security proof is given, which shows the proposed protocol has robustness under the collective attack. Finally, all the pre-shared keys can be recycled, if there is no detected eavesdropping.

The rest of the paper is organized as follows: Sect. 2 illustrates the proposed ASQKD protocol. Section 3 presents the security analyses and discusses the situation when the quantum channel is noisy. Section 4 compares the proposed protocol with Yu et al.’s and Li et al.’s measure-resend protocols. Section 5 concludes this paper.

2 Proposed measure-resend ASQKD protocol

The proposed protocol (shown in Fig. 1) uses two-step quantum communications. Alice has full quantum capabilities while Bob, the classical user, has only limited quantum capabilities (1), (2), and (4) as described earlier. Assume Alice would like to distribute a key to Bob. In the beginning, Alice and Bob both have pre-shared

![Fig. 1 The proposed ASQKD protocol](image-url)
secret keys $K_1$, $K_2$ and a pool of universal hash functions. The length of $K_1$ is $n + m$ bits while the length of $K_2$ is $m$ bits. $K_1$ is for the position of decoy photons, and $K_2$ is for choosing a hash function from the pool of universal hash functions [14].

**Step 1**: Alice chooses a key, $SK$, which is a binary string of length $n$ as the session key, to be distributed to Bob. She also chooses a hash function from the pool of universal hash functions based on the pre-shared key $K_2$. Then, $SK$ is hashed by the selected hash function to get an $m$-bit hash value. The binary string, $SK$, and the corresponding hash value are concatenated to become $SA$, whose length is $n + m$ bits.

**Step 2**: Alice generates a string $SD \in \{0, 1\}^{n+m}$. $SD$ is inserted into $SA$ based on the pre-shared key $K_1$ (If the $i$-th bit of $K_1$ is 0, then the $i$-th bit of $SD$ is inserted in front of the $i$-th bit of $SA$. Otherwise, it is inserted behind). Thus, a binary string of length $2n + 2m$ bits is produced. Then, according to this binary string, Alice generates a sequence of single photons named $QA$ according to the following rule: For $SA$, 0 is encoded to $|0\rangle$, and 1 is encoded to $|1\rangle$. For $SD$, 0 is encoded to $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$, and 1 is encoded to $|-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$. Finally, she sends $QA$, one bit at a time, to Bob via a public quantum channel.

**Step 3**: According to the pre-shared key $K_1$, Bob can distinguish bits in $SA$ from bits in $SD$. For each received photon belonging to $SA$, Bob measures it in Z-basis and resends the single photon in Z-basis based on the result of measurement (i.e., if the result of the measurement is 0 then $|0\rangle$ is resent, else $|1\rangle$ is resent.) If the received photon belongs to $SD$, Bob will reflect it without any disturbance. Since Bob has no delay line to store photons, he has to process one photon at a time and send it back to Alice.

**Step 4**: Upon receiving photons $SA'$ and $SD'$ from Bob, Alice measures these photons as follows. For those photons in $SA'$, Alice measures them in Z-basis. For photons in $SD'$, Alice measures them in X-basis. If the binary strings of $SA'$ and $SD'$ from the measurement result are not the same as the original $SA$ and $SD$, then there must exist some eavesdropping during the process.

**Bob**: In the meantime, while Bob gets $SK'$ and its corresponding hash value $Hash_{K_2}(SK')$ from the measurement result in Step 3, he puts $SK'$ into the hash function selected based on $K_2$ and compares $Hash_{K_2}(SK')$ with $Hash_{K_2}(SK)$. If $Hash_{K_2}(SK')$ is equal to $Hash_{K_2}(SK)$, Bob can assure that he gets the distributed key from Alice. Otherwise, there must be some eavesdropping.

**Step 5**: After the checks in Step 4, Alice and Bob will both send a 1-bit authenticated message to inform each other. If all checks are passed, the pre-shared keys will be recycled. Otherwise, the result will be abandoned, and the pre-shared key $K_2$ should be discarded.

### 3 Security analyses

This section shows the security of the proposed scheme and discusses the situation when the quantum channel is noisy. In Sect. 3.1, we will analyse the security of the proposed protocol and prove that the proposed protocol is robust [5]. By “robust” here, we mean that if the attacker, Eve, attacks the protocol and gets
some useful information, then she will be detected with a non-zero probability. That is, if there is no error being detected, then Eve cannot get any useful information. In Sect. 3.2, we will discuss the situation when the quantum channel is noisy. As we know, there is always some noise (errors) in the quantum channel, which may come from the noisy environment or Eve’s attacks.

3.1 Robustness

We assume Eve can fully control the quantum channel and has unlimited computational power to perform the collective attack [15]. To perform the collective attack, Eve first prepares a quantum state \( |E_i\rangle \), and performs a unitary operator \( U_i \) on the joint state \( |q\rangle \otimes |E_i\rangle \), where \( |q\rangle \) is a qubit transmitted between participants, and \( |E_i\rangle \) is Eve’s prepared quantum state. Eve can apply various quantum state \( |E_i\rangle \) and unitary operators \( U_i \) on the qubits which are originated from Alice or Bob, but she has to use the same \( |E_i\rangle \) and \( U_i \) in every round of attack.

Theorem 1. The proposed protocol is robust under the collective attack, i.e., if there is no error detected, the protocol does not leak any information about the pre-shared key and the newly shared key.

Proof. We denote the unitary operator which Eve uses to attack the qubits sent from Alice to Bob by \( U_1 \). Then we have:

\[
U_1|00\rangle|E_i\rangle = a_{A1}|00\rangle|f_{A1}\rangle + a_{A2}|01\rangle|f_{A2}\rangle + a_{A3}|10\rangle|f_{A3}\rangle + a_{A4}|11\rangle|f_{A4}\rangle
\]

\[
U_1|01\rangle|E_i\rangle = b_{A1}|00\rangle|g_{A1}\rangle + b_{A2}|01\rangle|g_{A2}\rangle + b_{A3}|10\rangle|g_{A3}\rangle + b_{A4}|11\rangle|g_{A4}\rangle
\]

\[
U_1|10\rangle|E_i\rangle = c_{A1}|00\rangle|h_{A1}\rangle + c_{A2}|01\rangle|h_{A2}\rangle + c_{A3}|10\rangle|h_{A3}\rangle + c_{A4}|11\rangle|h_{A4}\rangle
\]

\[
U_1|11\rangle|E_i\rangle = d_{A1}|00\rangle|k_{A1}\rangle + d_{A2}|01\rangle|k_{A2}\rangle + d_{A3}|10\rangle|k_{A3}\rangle + d_{A4}|11\rangle|k_{A4}\rangle
\]

where \( |E_i\rangle \) is Eve’s prepared quantum state and \( |f_{Ai}\rangle, |g_{Ai}\rangle, |h_{Ai}\rangle, |k_{Ai}\rangle \) are Eve’s quantum states after the attack.

Because Alice will only send eight different qubit pairs: \( |0+\rangle, |+0\rangle, |1+\rangle, |+1\rangle, |0-\rangle, |-0\rangle, |1-\rangle, \) or \( |-1\rangle \) in the protocol, we can denote these situations by:

\[
U_1|0+\rangle|E_i\rangle = \frac{1}{\sqrt{2}}(a_{A1}|00\rangle|f_{A1}\rangle + a_{A2}|01\rangle|f_{A2}\rangle + a_{A3}|10\rangle|f_{A3}\rangle + a_{A4}|11\rangle|f_{A4}\rangle)
\]

\[
+ \frac{1}{\sqrt{2}}(b_{A1}|00\rangle|g_{A1}\rangle + b_{A2}|01\rangle|g_{A2}\rangle + b_{A3}|10\rangle|g_{A3}\rangle + b_{A4}|11\rangle|g_{A4}\rangle)
\]

\[
U_1|+0\rangle|E_i\rangle = \frac{1}{\sqrt{2}}(a_{A1}|00\rangle|f_{A1}\rangle + a_{A2}|01\rangle|f_{A2}\rangle + a_{A3}|10\rangle|f_{A3}\rangle + a_{A4}|11\rangle|f_{A4}\rangle)
\]

\[
+ \frac{1}{\sqrt{2}}(c_{A1}|00\rangle|h_{A1}\rangle + c_{A2}|01\rangle|h_{A2}\rangle + c_{A3}|10\rangle|h_{A3}\rangle + c_{A4}|11\rangle|h_{A4}\rangle)
\]

\[
U_1|0-\rangle|E_i\rangle = \frac{1}{\sqrt{2}}(a_{A1}|00\rangle|f_{A1}\rangle + a_{A2}|01\rangle|f_{A2}\rangle + a_{A3}|10\rangle|f_{A3}\rangle + a_{A4}|11\rangle|f_{A4}\rangle)
\]

\[
+ \frac{1}{\sqrt{2}}(b_{A1}|00\rangle|g_{A1}\rangle + b_{A2}|01\rangle|g_{A2}\rangle + b_{A3}|10\rangle|g_{A3}\rangle + b_{A4}|11\rangle|g_{A4}\rangle)
\]

\[
U_1|+1\rangle|E_i\rangle = \frac{1}{\sqrt{2}}(a_{A1}|00\rangle|f_{A1}\rangle + a_{A2}|01\rangle|f_{A2}\rangle + a_{A3}|10\rangle|f_{A3}\rangle + a_{A4}|11\rangle|f_{A4}\rangle)
\]

\[
+ \frac{1}{\sqrt{2}}(c_{A1}|00\rangle|h_{A1}\rangle + c_{A2}|01\rangle|h_{A2}\rangle + c_{A3}|10\rangle|h_{A3}\rangle + c_{A4}|11\rangle|h_{A4}\rangle)
\]
\[ U_1|1+\rangle|E_1\rangle = \frac{1}{\sqrt{2}} (c_{A1}|00\rangle|h_{A1}\rangle + c_{A2}|01\rangle|h_{A2}\rangle + c_{A3}|10\rangle|h_{A3}\rangle + c_{A4}|11\rangle|h_{A4}\rangle ) \\
\quad + \frac{1}{\sqrt{2}} (d_{A1}|00\rangle|k_{A1}\rangle + d_{A2}|01\rangle|k_{A2}\rangle + d_{A3}|10\rangle|k_{A3}\rangle + d_{A4}|11\rangle|k_{A4}\rangle ) \\
U_1|+1\rangle|E_1\rangle = \frac{1}{\sqrt{2}} (b_{A1}|00\rangle|g_{A1}\rangle + b_{A2}|01\rangle|g_{A2}\rangle + b_{A3}|10\rangle|g_{A3}\rangle + b_{A4}|11\rangle|g_{A4}\rangle ) \\
\quad + \frac{1}{\sqrt{2}} (d_{A1}|00\rangle|k_{A1}\rangle + d_{A2}|01\rangle|k_{A2}\rangle + d_{A3}|10\rangle|k_{A3}\rangle + d_{A4}|11\rangle|k_{A4}\rangle ) \\
U_1|0−\rangle|E_1\rangle = \frac{1}{\sqrt{2}} (a_{A1}|00\rangle|f_{A1}\rangle + a_{A2}|01\rangle|f_{A2}\rangle + a_{A3}|10\rangle|f_{A3}\rangle + a_{A4}|11\rangle|f_{A4}\rangle ) \\
\quad - \frac{1}{\sqrt{2}} (b_{A1}|00\rangle|g_{A1}\rangle + b_{A2}|01\rangle|g_{A2}\rangle + b_{A3}|10\rangle|g_{A3}\rangle + b_{A4}|11\rangle|g_{A4}\rangle ) \\
U_1|−0\rangle|E_1\rangle = \frac{1}{\sqrt{2}} (a_{A1}|00\rangle|f_{A1}\rangle + a_{A2}|01\rangle|f_{A2}\rangle + a_{A3}|10\rangle|f_{A3}\rangle + a_{A4}|11\rangle|f_{A4}\rangle ) \\
\quad - \frac{1}{\sqrt{2}} (c_{A1}|00\rangle|h_{A1}\rangle + c_{A2}|01\rangle|h_{A2}\rangle + c_{A3}|10\rangle|h_{A3}\rangle + c_{A4}|11\rangle|h_{A4}\rangle ) \\
U_1|1−\rangle|E_1\rangle = \frac{1}{\sqrt{2}} (c_{A1}|00\rangle|h_{A1}\rangle + c_{A2}|01\rangle|h_{A2}\rangle + c_{A3}|10\rangle|h_{A3}\rangle + c_{A4}|11\rangle|h_{A4}\rangle ) \\
\quad - \frac{1}{\sqrt{2}} (d_{A1}|00\rangle|k_{A1}\rangle + d_{A2}|01\rangle|k_{A2}\rangle + d_{A3}|10\rangle|k_{A3}\rangle + d_{A4}|11\rangle|k_{A4}\rangle ) \\
U_1|−1\rangle|E_1\rangle = \frac{1}{\sqrt{2}} (b_{A1}|00\rangle|g_{A1}\rangle + b_{A2}|01\rangle|g_{A2}\rangle + b_{A3}|10\rangle|g_{A3}\rangle + b_{A4}|11\rangle|g_{A4}\rangle ) \\
\quad - \frac{1}{\sqrt{2}} (d_{A1}|00\rangle|k_{A1}\rangle + d_{A2}|01\rangle|k_{A2}\rangle + d_{A3}|10\rangle|k_{A3}\rangle + d_{A4}|11\rangle|k_{A4}\rangle ),

Upon receiving the attacked qubits, Bob will measure the qubits in \( S_A \) in Z-basis. And after he receives all qubits from Alice, he will check the hash value. If the attacker changes the Z-basis qubits, the check of the hash value in Step 4 will fail, and then the attacker will be detected. By the definition of robustness, we can assume that the attacker will not change the value of the Z-basis qubits. This gives a limit to the possible \( U_1 \), and we can denote the limited \( U_1 \) by:

\[
U_1|0+\rangle|E_1\rangle = \frac{1}{\sqrt{2}} (|00\rangle|f_{A1}\rangle + |01\rangle|g_{A2}\rangle ) \\
U_1|+0\rangle|E_1\rangle = \frac{1}{\sqrt{2}} (|00\rangle|f_{A1}\rangle + |10\rangle|h_{A3}\rangle )
\]
Eve can use a different unitary operator $U_2$ to attack instead. We denote the unitary operator $U_2$ by:

$$U_2|00\rangle|f_{A1}\rangle = a_{B1}|00\rangle|f_{B1}\rangle + a_{B2}|01\rangle|f_{B2}\rangle + a_{B3}|10\rangle|f_{B3}\rangle + a_{B4}|11\rangle|f_{B4}\rangle$$

$$U_2|01\rangle|g_{A2}\rangle = b_{B1}|00\rangle|g_{B1}\rangle + b_{B2}|01\rangle|g_{B2}\rangle + b_{B3}|10\rangle|g_{B3}\rangle + b_{B4}|11\rangle|g_{B4}\rangle$$

$$U_2|10\rangle|h_{A3}\rangle = c_{B1}|00\rangle|h_{B1}\rangle + c_{B2}|01\rangle|h_{B2}\rangle + c_{B3}|10\rangle|h_{B3}\rangle + c_{B4}|11\rangle|h_{B4}\rangle$$

$$U_2|11\rangle|k_{A4}\rangle = d_{B1}|00\rangle|k_{B1}\rangle + d_{B2}|01\rangle|k_{B2}\rangle + d_{B3}|10\rangle|k_{B3}\rangle + d_{B4}|11\rangle|k_{B4}\rangle,$$

where $|f_{Bi}\rangle, |g_{Bi}\rangle, |h_{Bi}\rangle, |k_{Bi}\rangle$ are Eve’s quantum states after the attack.

The situations in the protocol are denoted by:

$$U_2 \frac{1}{\sqrt{2}} \left( a_{A1}|f_{A1}\rangle|00\rangle + b_{A2}|g_{A2}\rangle|01\rangle \right)$$

$$= \frac{1}{\sqrt{2}} a_{A1} (a_{B1}|00\rangle|f_{B1}\rangle + a_{B2}|01\rangle|f_{B2}\rangle + a_{B3}|10\rangle|f_{B3}\rangle + a_{B4}|11\rangle|f_{B4}\rangle)$$

$$+ \frac{1}{\sqrt{2}} b_{A2} (b_{B1}|00\rangle|g_{B1}\rangle + b_{B2}|01\rangle|g_{B2}\rangle + b_{B3}|10\rangle|g_{B3}\rangle + b_{B4}|11\rangle|g_{B4}\rangle)$$
\[
U_2 \frac{1}{\sqrt{2}} (a_{A1}\vert f_{A1}\rangle \vert 00\rangle + c_{A3}\vert h_{A3}\rangle \vert 10\rangle )
\]
\[
= \frac{1}{\sqrt{2}} a_{A1} (a_{B1}\vert 00\rangle \vert f_{B1}\rangle + a_{B2}\vert 01\rangle \vert f_{B2}\rangle + a_{B3}\vert 10\rangle \vert f_{B3}\rangle + a_{B4}\vert 11\rangle \vert f_{B4}\rangle )
+ \frac{1}{\sqrt{2}} c_{A3} (c_{B1}\vert 00\rangle \vert h_{B1}\rangle + c_{B2}\vert 01\rangle \vert h_{B2}\rangle + c_{B3}\vert 10\rangle \vert h_{B3}\rangle + c_{B4}\vert 11\rangle \vert h_{B4}\rangle )
\]
\[
U_2 \frac{1}{\sqrt{2}} (c_{A3}\vert h_{A3}\rangle \vert 10\rangle + d_{A4}\vert k_{A4}\rangle \vert 11\rangle )
\]
\[
= \frac{1}{\sqrt{2}} c_{A3} (c_{B1}\vert 00\rangle \vert h_{B1}\rangle + c_{B2}\vert 01\rangle \vert h_{B2}\rangle + c_{B3}\vert 10\rangle \vert h_{B3}\rangle + c_{B4}\vert 11\rangle \vert h_{B4}\rangle )
+ \frac{1}{\sqrt{2}} d_{A4} (d_{B1}\vert 00\rangle \vert k_{B1}\rangle + d_{B2}\vert 01\rangle \vert k_{B2}\rangle + d_{B3}\vert 10\rangle \vert k_{B3}\rangle + d_{B4}\vert 11\rangle \vert k_{B4}\rangle )
\]
\[
U_2 \frac{1}{\sqrt{2}} (b_{A2}\vert g_{A2}\rangle \vert 01\rangle + d_{A4}\vert k_{A4}\rangle \vert 11\rangle )
\]
\[
= \frac{1}{\sqrt{2}} b_{A2} (b_{B1}\vert 00\rangle \vert g_{B1}\rangle + b_{B2}\vert 01\rangle \vert g_{B2}\rangle + b_{B3}\vert 10\rangle \vert g_{B3}\rangle + b_{B4}\vert 11\rangle \vert g_{B4}\rangle )
+ \frac{1}{\sqrt{2}} d_{A4} (d_{B1}\vert 00\rangle \vert k_{B1}\rangle + d_{B2}\vert 01\rangle \vert k_{B2}\rangle + d_{B3}\vert 10\rangle \vert k_{B3}\rangle + d_{B4}\vert 11\rangle \vert k_{B4}\rangle )
\]
\[
U_2 \frac{1}{\sqrt{2}} (a_{A1}\vert f_{A1}\rangle \vert 00\rangle - b_{A2}\vert g_{A2}\rangle \vert 01\rangle )
\]
\[
= \frac{1}{\sqrt{2}} a_{A1} (a_{B1}\vert 00\rangle \vert f_{B1}\rangle + a_{B2}\vert 01\rangle \vert f_{B2}\rangle + a_{B3}\vert 10\rangle \vert f_{B3}\rangle + a_{B4}\vert 11\rangle \vert f_{B4}\rangle )
- \frac{1}{\sqrt{2}} b_{A2} (b_{B1}\vert 00\rangle \vert g_{B1}\rangle + b_{B2}\vert 01\rangle \vert g_{B2}\rangle + b_{B3}\vert 10\rangle \vert g_{B3}\rangle + b_{B4}\vert 11\rangle \vert g_{B4}\rangle )
\]
\[
U_2 \frac{1}{\sqrt{2}} (a_{A1}\vert f_{A1}\rangle \vert 00\rangle - c_{A3}\vert h_{A3}\rangle \vert 10\rangle )
\]
\[
= \frac{1}{\sqrt{2}} a_{A1} (a_{B1}\vert 00\rangle \vert f_{B1}\rangle + a_{B2}\vert 01\rangle \vert f_{B2}\rangle + a_{B3}\vert 10\rangle \vert f_{B3}\rangle + a_{B4}\vert 11\rangle \vert f_{B4}\rangle )
- \frac{1}{\sqrt{2}} c_{A3} (c_{B1}\vert 00\rangle \vert h_{B1}\rangle + c_{B2}\vert 01\rangle \vert h_{B2}\rangle + c_{B3}\vert 10\rangle \vert h_{B3}\rangle + c_{B4}\vert 11\rangle \vert h_{B4}\rangle )
\]
Alice will check all the received qubits. This check gives some limits to the possible $U_1$ and $U_2$. Combining all limits above, we have

$$
U_2 \frac{1}{\sqrt{2}} (c_{A3} |h_{A3}\rangle |10\rangle - d_{A4} |k_{A4}\rangle |11\rangle) 
= \frac{1}{\sqrt{2}} c_{A3} (c_{B1} |00\rangle |h_{B1}\rangle + c_{B2} |01\rangle |h_{B2}\rangle + c_{B3} |10\rangle |h_{B3}\rangle + c_{B4} |11\rangle |h_{B4}\rangle) 
- \frac{1}{\sqrt{2}} d_{A4} (d_{B1} |00\rangle |k_{B1}\rangle + d_{B2} |01\rangle |k_{B2}\rangle + d_{B3} |10\rangle |k_{B3}\rangle + d_{B4} |11\rangle |k_{B4}\rangle)
$$

$$
U_2 \frac{1}{\sqrt{2}} (b_{A2} |g_{A2}\rangle |01\rangle - d_{A4} |k_{A4}\rangle |11\rangle) 
= \frac{1}{\sqrt{2}} b_{A2} (b_{B1} |00\rangle |g_{B1}\rangle + b_{B2} |01\rangle |g_{B2}\rangle + b_{B3} |10\rangle |g_{B3}\rangle + b_{B4} |11\rangle |g_{B4}\rangle) 
- \frac{1}{\sqrt{2}} d_{A4} (d_{B1} |00\rangle |k_{B1}\rangle + d_{B2} |01\rangle |k_{B2}\rangle + d_{B3} |10\rangle |k_{B3}\rangle + d_{B4} |11\rangle |k_{B4}\rangle).
$$

And

$$
|f_{A1}\rangle = |g_{A2}\rangle = |h_{A3}\rangle = |k_{A4}\rangle, \quad |f_{B1}\rangle = |g_{B2}\rangle = |h_{B3}\rangle = |k_{B4}\rangle.
$$

We hence prove that no unitary operator can be used by Eve to get useful information about the pre-shared key and the newly shared key without being detected.

### 3.2 On the noisy quantum channel

When the quantum channel is noisy, the proposed protocol cannot be used to distribute keys between Alice and Bob because they will always detect errors. Consequently, the results and the used pre-shared keys will always be abandoned.

To overcome this problem, Error Correction Code (ECC) [16, 17] can be applied on $S_A$ to correct the errors, and then privacy amplification [18] is applied to the results to
guarantee the security of newly shared key. To do this, we modify Steps 1 and 4 of the proposed protocol:

We assume the error rate of the quantum channel is $r$. In this situation, Alice and Bob both need to have an extra pre-shared secret key $K_3$, and a systematic $r$-error correction code is used to generate the redundant bits to correct errors in a binary string.

1’. Alice uses the error correction code to generate the redundant bits of $SK$ and the corresponding hash value. Alice then encrypt the redundant bits by the pre-shared key $K_3$, Alice concatenates $SK$, the hash value, and the redundant bits to generate $S_A$.

4’. Before Bob check the hash value of $SK$, he will decrypt the redundant bits by $K_3$ and use the redundant bits to correct the errors in $SK$ and hash value.

If the error rate in the quantum channel is less than $r$, the errors in $S_A$ will be corrected, and Bob’s check will be successful. Alice will also check the error rate of the resend qubits (both in Z-basis and X-basis). If the error rate is also less than $r$, then the proposed protocol will be successful.

Though we can use ECC to correct the errors (noise) in the quantum channel, the ECC will also hide Eve’s attacks and make the newly shared key insecure. For example, Eve can replace the noisy quantum channel with an ideal one and attack the communication. If the errors caused by Eve’s attack are not over $r$, Bob will correct the errors using the redundant bits, and hence Eve’s attack will not be detected. Eve then can get some information about the newly shared key without being detected. To guarantee the security of the shared key, however, Alice and Bob can use privacy amplification to extract a secret key from $SK$ based on the error rate (which could destroy the information Eve can obtain). Privacy amplification will shorten the length of the newly shared secret key but can keep the security of the shared key.

On the other hand, the pre-shared key $K_1$ can still be totally recycled securely. Since there is no way to know the basis of any qubit in the $Q_A$ and $Q'_A$ if $S_A$ is totally random, and the attacker doesn’t know the value of $S_A$ [19], i.e., Eve cannot perform the know-plaintext attack. $S_A$ is first produced by Alice in Step 1 of the proposed protocol, it should be in secret. In Step 4, if the protocol fails, $S_A$ is abandoned, and no one can get it; if the protocol is successful, Eve cannot get any information about $S_A$ according to the security analysis above. To keep $S_A$ random, the pre-shared key $K_2$ and $K_3$ cannot be recycled. It should be changed every time when the quantum channel is noisy.

Table 1 shows the comparison of the proposed protocols with and without noise tolerance. The use of an extra pre-shared key $K_3$ for the noisy quantum channel, which cannot be recycled, as well as the privacy amplification definitely lowers the
efficiency of the protocol, but if the error rate is not too high, the proposed protocol can still distribute keys on a noisy quantum channel.

### 4 Comparison

The proposed protocol is compared with Yu et al.’s and Li et al.’s measure-resend protocols on the following features: (1) classical participants’ quantum capabilities, (2) quantum resource, (3) qubit efficiency, (4) bit number of pre-shared keys, (5) classical channels required during key distribution, (6) hash function, and (7) security proof as given in Table 2 above.

The qubit efficiency is defined as the number of distributed key bits divided by the total number of generated qubits [13]. If we set $n = m$, then the qubit efficiency of the proposed protocol is $\frac{n}{2n+2m+(n+m)} = \frac{1}{6}$, where $2n + 2m$ is for $Q_A$ sent from Alice, and $n + m$ is for photons belonging to $S_A$ resent from Bob.

### 5 Conclusions

The proposed ASQKD protocol uses only single photons to efficiently distribute keys from Alice to Bob. The proposed protocol is shown to be robust under collective attacks, and the pre-shared keys can be recycled securely. We also analyse the situation when the quantum channel is noisy. If the noise in the quantum channel is not too high, the proposed protocol can still be able to distribute secret keys with the cost of qubit efficiency and an extra shared key. How to design a more efficient protocol to distribute keys with a noisy channel is an important question for future research.
|                           | Yu et al.’s measure-resend ASQKD | Li et al.’s measure-resend ASQKD | The proposed measure-resend ASQKD |
|---------------------------|----------------------------------|----------------------------------|----------------------------------|
| **Classical participants’ quantum capabilities** | Generate | Generate | Reflect |
|                           | Reflect | Reflect | Reflect |
|                           | Measure | Measure | Measure |
| **Quantum resource**      | Bell state | Bell state, single photons | Single photons |
| **Qubit efficiency**      | $1/10$ | $1/9$ | $1/6$ |
| **Required pre-shared keys (in bits)** | $3n + 3m$ | $2n + 2m$ | $n + 2m$ |
| **Required classical channel** | Public discussion | 1-bit authenticated message | 1-bit authenticated message (2 times) |
| **Hash function**         | No | Public hash | Secret hash |
| **Proven security**       | No | No | Yes |
Acknowledgements This research was partially supported by the Ministry of Science and Technology, Taiwan, R.O.C. (MOST 107-2627-E-006-001 and 109-2221-E-006-168).

References

1. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. Theor. Comput. Sci. 560(12), 7–11 (2014)
2. Bennett, C.H.: Quantum cryptography using any two nonorthogonal states. Phys. Rev. Lett. 68(21), 3121 (1992)
3. Lo, H.-K., Chau, H.F., Ardehali, M.: Efficient quantum key distribution scheme and a proof of its unconditional security. J. Cryptol. 18(2), 133–165 (2005)
4. Ekert, A.K.: Quantum cryptography based on Bell’s theorem. Phys. Rev. Lett. 67(6), 661 (1991)
5. Boyer, M., Kenigsberg, D., Mor, T.: Quantum key distribution with classical Bob. In: 2007 First International Conference on Quantum, Nano, and Micro Technologies (ICQNM’07), pp. 10–10. IEEE (2007)
6. Lo, H.-K., Ma, X., Chen, K.: Decoy state quantum key distribution. Phys. Rev. Lett. 94(23), 230504 (2005)
7. Lo, H.-K., Curty, M., Qi, B.: Measurement-device-independent quantum key distribution. Phys. Rev. Lett. 108(13), 130503 (2012)
8. Grosshans, F., Van Assche, G., Wenger, J., Broui, R., Cerf, N.J., Grangier, P.: Quantum key distribution using gaussian-modulated coherent states. Nature 421(6920), 238–241 (2003)
9. Long, G.-L., Liu, X.-S.: Theoretically efficient high-capacity quantum-key-distribution scheme. Phys. Rev. A 65(3), 032302 (2002)
10. Cerf, N.J., Bourennane, M., Karlsson, A., Gisin, N.: Security of quantum key distribution using d-level systems. Phys. Rev. Lett. 88(12), 127902 (2002)
11. Boyer, M., Gelles, R., Kenigsberg, D., Mor, T.: Semiquantum key distribution. Physical Review A 79(3), 032341 (2009)
12. Yu, K.-F., Yang, C.-W., Liao, C.-H., Hwang, T.: Authenticated semi-quantum key distribution protocol using Bell states. Quantum Inf. Process. 13(6), 1457–1465 (2014)
13. Li, C.-M., Yu, K.-F., Kao, S.-H., Hwang, T.: Authenticated semi-quantum key distributions without classical channel. Quantum Inf. Process. 15(7), 2881–2893 (2016)
14. Carter, J.L., Wegman, M.N.: Universal classes of hash functions. J. Comput. Syst. Sci. 18(2), 143–154 (1979)
15. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The security of practical quantum key distribution. Rev. Mod. Phys. 81(3), 1301–1350 (2009). https://doi.org/10.1103/revmodphys.81.1301
16. Reed, I.S., Solomon, G.: Polynomial codes over certain finite fields. J. Soc. Ind. Appl. Math. 8(2), 300–304 (1960)
17. Gallager, R.: Low-density parity-check codes. IRE Trans. Inf. Theory 8(1), 21–28 (1962)
18. Renner, R., König, R.: Universally composably disposable privacy amplification against quantum adversaries. Paper presented at the Theory of Cryptography Conference,
19. Yu-Chin Lu, C.-W.T., Tzonelih Hwang: Quantum Key Recycling with optimal key recycling rate based on a noise level. arXiv pre-print server (2020). 2004.11596

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations