scientific reports

OPEN

Encryption chain based on measurement result and its applications on semi-quantum key distribution protocol

Chun-Wei Yang

This study proposes a new encoding method, also known as an encryption chain based on the measurement result. Then, using the encryption chain to propose a unitary-operation-based semi-quantum key distribution protocol (SQKD) protocol. In the existing SQKD protocols, semi-quantum environments adopt a round-trip transmission strategy. In round-trip transmission, the classical participant must resend the received photons to the quantum participant after implementing local operations. Therefore, round-trip transmissions are vulnerable to Trojan horse attacks. Hence, the classical participant must be equipped with a photon number splitter and an optical wavelength filter device against Trojan horse attacks. This is illogical for semi-quantum environments because the burden on the classical participant is significantly increased as it involves the prevention of Trojan horse attacks. The proposed SQKD protocol is congenitally immune to Trojan horse attacks and involves no extra hardware because it is designed based on a one-way transmission as opposed to a round-trip transmission. When compared to the existing SQKD protocols, the proposed SQKD protocol provides the best qubit efficiency, and classical participants only require two quantum capabilities, which enhance its practicability. Moreover, the proposed SQKD protocol is free from collective attacks, Trojan horse attacks, and intercept-resend attacks. Thus, the proposed scheme is more efficient and practical than the existing SQKD protocols.

With the development of information technology, breakthroughs and innovations in the internet of things (IoT), cloud computing, big data, and artificial intelligence (AI) technologies, AI and IoT techniques are used to help solve problems are becoming increasingly popular, especially in the medical field[1–5]. To ensure the data security of these applications, most of them use encryption techniques to protect data security. However, to securely create the secret keys required for encryption, many mainstream applications use public-key cryptographic system to distribute secret keys. In 1994, Shor proposed a quantum algorithm[6] that can break the RSA encryption system in a polynomial time. Therefore, the security framework of the RSA encryption system, which is based on the mathematical difficulty of prime factorization, cannot be guaranteed in the environment of quantum computers. This groundbreaking research result also drives the research energy of quantum cryptography. Therefore, how to design cryptographic techniques that can resist quantum computer attacks has become an important issue in cryptographic research.

Since the rapid development of quantum communication, quantum key distribution (QKD) protocol has become one of the most critical research areas in quantum cryptography. The main principle of the QKD protocol involves distributing a secret key to a receiver via the transmission of qubits. In 1984, Bennett and Brassard[7] developed the first QKD scheme, termed the BB84 protocol, based on the properties of quantum mechanics. In 1992, Bennett et al.[8] put forward a QKD protocol based on the Bell states. In 2002, Long and Liu[9] proposed the QKD protocol by means of a two-step communication strategy. In 2003, Deng et al.[10] also developed a two-step quantum secure direct communication (QSDC) protocol based on Long and Liu's concept. Unlike the QKD protocol, the QSDC protocol allows two participants to transmit information directly over a quantum channel without sharing any secrets in advance. Subsequently, numerous QKD protocols[11–23] and QSDC protocols[24–28] have been proposed using single photons or entangled states. Although QKD protocols provide unconditional security[29–32], it must be assumed that the sender and the receiver possess unlimited quantum capabilities, including generating single photons or entangled states, measuring qubits with any basis, and storing qubits in a

Master Program for Digital Health Innovation, College of Humanities and Sciences, China Medical University, No. 100, Sec. 1, Jingmao Rd., Beitun Dist., Taichung 406040, Taiwan, ROC. email: cwyang@mail.cmu.edu.tw

quantum register. However, most quantum capabilities are difficult to implement, and the devices are expensive. Some researchers focused on designing semi-quantum key distribution (SQKD) protocols that can lead to a more practical QKD protocol.

Boyer et al.[33] developed the first SQKD protocol in 2007. In 2009, Boyer et al.[34] developed two SQKD schemes and defined two semi-quantum environments: the randomization-based environment and measure–resend environment. Based on Boyer et al.'s definition, the term "semi-quantum" implies that the sender, Alice, is a powerful quantum participant, whereas the receiver, Bob, solely possesses classical capabilities. Quantum participants can perform actions such as quantum generation, measurement, and storage. However, the receiver is restricted to implementing the following operations: (1) perform Z-basis $\{|0\rangle, |1\rangle\}$ measurement; (2) generate photons using Z-basis; (3) reflect the photons without any disturbance; and (4) reorder photons using different delay lines. Regarding the limitation of quantum capabilities, the randomization-based SQKD protocol assumes that the receiver possesses three types of quantum capabilities: (1) perform Z-basis measurement; (2) reflect the photons without any disturbance; and (3) reorder photons using different delay lines. The measure–resend SQKD protocol assumes that the receiver possesses three types of quantum capabilities: (1) perform Z-basis measurement; (2) generate photons using Z-basis; and (3) reflect the photons without any disturbance. After the semi-quantum concept was presented, various SQKD protocols[35–47] were proposed for different security scenarios.

Based on a different perspective, Lo et al.[48] developed the first measurement device-independent (MDI) QKD protocol in 2012. MDI-QKD protocols can be free from various eavesdropping attacks on qubit detectors and have been experimentally implemented[49–52]. In MDI-QKD protocols, the communicators send qubits to a third party (TP), which conducts a Bell-state analysis (BSA). Hence, the TP can be untrusted. That is, TP can be completely controlled by an eavesdropper.

Similarly, Zou et al.[53] further restricted the abilities of classical participants. In 2015, Zou et al.[53] proposed an SQKD protocol without invoking the measurement capability of a classical participant and proved it as robust with respect to quantum joint attacks. Regarding the limitation of quantum capabilities, the measurement-free SQKD protocol assumes that the receiver possesses three types of quantum capabilities: (1) generate photons using Z-basis; (2) reflect the photons without any disturbance; and (3) reorder photons using different delay lines. In 2018, Liu and Hwang[54] designed a mediated SQKD (MSQKD) protocol using a measurement-free environment, where the TP should also be equipped with an entangled state generator, an entangled state measurement device, and a quantum register or a quantum delay line.

In contrast to the aforementioned SQKD or MSQKD protocols, Tsai et al.[55,56] proposed lightweight MSQKD protocols, in which the classical participants only possess the capabilities of (1) performing Z-basis measurement and (2) performing the unitary operation. Moreover, Tsai et al.'s lightweight MSQKD protocol[55,56] can reduce the quantum capabilities of the TP. That is, the TP has only two quantum capabilities: (1) generate photons using Z-basis and (2) perform the unitary operation. This implies that TP and communicators are classical in Tsai et al.'s lightweight MSQKD protocol[55,56]. In other words, to implement a semi-quantum cryptographic protocol, the classical participant does not require a quantum-generating device. With respect to the limitation of quantum capabilities, the semi-quantum cryptographic protocols based on a unitary-operation-based environment assume that the receiver possesses two types of quantum capabilities: (1) performing Z-basis measurement and (2) performing the unitary operation. In 2020, Tsai and Yang[57] designed a lightweight authenticated SQKD (ASQKD) protocol using the Bell states. When compared to existing ASQKD protocols[58–63], Tsai and Yang's scheme only requires the classical participant to possess only two quantum capabilities. Thus, Tsai and Yang's scheme is less demanding than existing ASQKD protocols in terms of practical implementation.

Based on the qubit's transmission strategy, the quantum cryptographic protocols presented, to date, can generally be classified into three types: quantum-relay transmission, round-trip transmission, and one-way transmission. Specifically, these semi-quantum environments (i.e., randomization-based, measure-resend, and measurement-free) adopt a round-trip transmission strategy. In round-trip transmission, the classical participant must send back the received qubits to the quantum participant after performing measurements or operations. That is, the qubits are received and sent to the other participants. Hence, round-trip transmissions can suffer from Trojan horse attacks[64–66]. To address the problem of Trojan horse attacks, the classical participant must be equipped with a photon number splitter[67] and an optical wavelength filter device[68] against Trojan horse attacks. This is illogical for semi-quantum environments because the burden on the classical participant is significantly increased by the threat of Trojan horse attacks. Thus, these semi-quantum cryptographic protocols introduce high overheads, which significantly reduce communication efficiency.

In this work, an SQKD protocol is designed based on Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and one-way transmission. The designed SQKD protocol is developed based on one-way transmission as opposed to round-trip transmission, which enhances its practicability. Specifically, the qubits are directly distributed by the quantum participant to the classical participant via a single path. In addition, this work proposed a new coding function for a unitary-operation-based environment, i.e., the quantum communicator and classical communicator decide to perform the identity operation or Hadamard operation on one of the two-particle quantum entanglement $|\Phi^+\rangle$ based on the previous measurement result. For example, if the previous measurement result is $|0\rangle$ ($|1\rangle$), then the quantum communicator and classical communicator perform the identity operation (the Hadamard operation) on the qubit and measure it using a Z-basis. By using the measurement property of Bell states and Hadamard operation, when the quantum communicator and classical communicator perform the Hadamard operation on first and second qubits from each $|\Phi^+\rangle$, they can obtain the same measurement results using a Z-basis measurement. Based on the measurement results, the quantum and classical communicators can share a secret key. Therefore, the proposed SQKD protocol exhibits the following advantages over existing SQKD protocols.

1. It is simple and efficient because the classical participant only performs Z-basis measurement and Hadamard operation.
2. It is secure with respect to Trojan-horse attack because one-way transmission is adopted.
3. It is immune to various individual eavesdropping attacks.

The remainder of this paper is organized as follows. In "Encryption chain based on the measurement result", a new coding function is presented based on Bell states and Hadamard operations. In "Proposed unitary-operation-based SQKD protocol", a unitary-operation-based SQKD protocol is described. In "Security analysis", an analysis of the security of the proposed SQKD protocol is presented. In "Efficiency analysis", an analysis of the efficiency of the proposed scheme is presented. Finally, the conclusions of the study are stated in "Conclusion".

Encryption chain based on the measurement result

In this section, the relationship between Bell states and Hadamard operations is first introduced. In "Encryption chain for the encoding function" and "Encryption chain for the decoding function", based on the measurement result, an encryption chain for new encoding and decoding functions is proposed. The coding function is useful for constructing a unitary-operation-based SQKD protocol for participants with different abilities.

Relationship between Bell states and Hadamard operations.

The Bell state, as known as the EPR pair, is a two-particle quantum-entangled state. Bell states have the four orthogonal maximal states and can be represented as follows:

$$\begin{aligned} \left|\Phi^{+}\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle) \\ \left|\Phi^{-}\right\rangle &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle) \\ \left|\Psi^{+}\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle) \\ \left|\Psi^{-}\right\rangle &= \frac{1}{\sqrt{2}}(|01\rangle - |10\rangle) \end{aligned} \tag{1}$$

Regarding the limitation of quantum capabilities, the unitary-operation-based environment[35–37] assumes that the receiver possesses two types of quantum capabilities: (1) performing Z-basis measurement and (2) performing identity operator I or Hadamard operator H, where I and H are defined as follows:

$$I = |0\rangle\langle 0| + |1\rangle\langle 1| = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \tag{2}$$

$$H = \frac{1}{\sqrt{2}}(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|) = \frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \tag{3}$$

In Tsai et al.'s schemes[35–37], the communicators can randomly decide to perform the unitary operations I or H on the qubits, and then they measure the qubits using Z-basis, respectively. The relationships between their performed the unitary operations on Bell states and measurement results are calculated in Eqs. (4)–(7) (as shown in Table 1), where MR_A and MR_B represent Alice's and Bob's measurement results, respectively, and $\overline{MR_B}$ denotes the bitwise *NOT* operation on MR_B.

$$\begin{aligned} I \otimes I\left|\Phi^{+}\right\rangle_{AB} &= \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} \\ I \otimes H\left|\Phi^{+}\right\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0+\rangle + |1-\rangle)_{AB} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{AB} \\ H \otimes I\left|\Phi^{+}\right\rangle_{AB} &= \frac{1}{\sqrt{2}}(|+0\rangle + |-1\rangle)_{AB} = \frac{1}{2}(|00\rangle + |01\rangle + |10\rangle - |11\rangle)_{AB} \\ H \otimes H\left|\Phi^{+}\right\rangle_{AB} &= \frac{1}{\sqrt{2}}(|++\rangle + |--\rangle)_{AB} = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB} \end{aligned} \tag{4}$$

$$\begin{aligned} I \otimes I\left|\Phi^{-}\right\rangle_{AB} &= \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)_{AB} \\ I \otimes H\left|\Phi^{-}\right\rangle_{AB} &= \frac{1}{\sqrt{2}}(|0+\rangle - |1-\rangle)_{AB} = \frac{1}{2}(|00\rangle + |01\rangle - |10\rangle + |11\rangle)_{AB} \\ H \otimes I\left|\Phi^{-}\right\rangle_{AB} &= \frac{1}{\sqrt{2}}(|+0\rangle - |-1\rangle)_{AB} = \frac{1}{2}(|00\rangle - |01\rangle + |10\rangle + |11\rangle)_{AB} \\ H \otimes H\left|\Phi^{-}\right\rangle_{AB} &= \frac{1}{\sqrt{2}}(|++\rangle - |--\rangle)_{AB} = \frac{1}{\sqrt{2}}(|01\rangle + |10\rangle)_{AB} \end{aligned} \tag{5}$$

Initial state	Alice's operation	Bob's operation	Quantum state	Relationship of measurement result
$\left\|\Phi^{+}\right\rangle_{AB}$	I	I	$\frac{1}{\sqrt{2}}(\|00\rangle+\|11\rangle)_{AB}$	$MR_A=MR_B$
	I	H	$\frac{1}{2}(\|00\rangle+\|01\rangle+\|10\rangle-\|11\rangle)_{AB}$	Uncertain
	H	I	$\frac{1}{2}(\|00\rangle+\|01\rangle+\|10\rangle-\|11\rangle)_{AB}$	Uncertain
	H	H	$\frac{1}{\sqrt{2}}(\|00\rangle+\|11\rangle)_{AB}$	$MR_A=MR_B$
$\left\|\Phi^{-}\right\rangle_{AB}$	I	I	$\frac{1}{\sqrt{2}}(\|00\rangle-\|11\rangle)_{AB}$	$MR_A=MR_B$
	I	H	$\frac{1}{2}(\|00\rangle+\|01\rangle-\|10\rangle+\|11\rangle)_{AB}$	Uncertain
	H	I	$\frac{1}{2}(\|00\rangle-\|01\rangle+\|10\rangle+\|11\rangle)_{AB}$	Uncertain
	H	H	$\frac{1}{\sqrt{2}}(\|01\rangle+\|10\rangle)_{AB}$	$MR_A=\overline{MR_B}$
$\left\|\Psi^{+}\right\rangle_{AB}$	I	I	$\frac{1}{\sqrt{2}}(\|01\rangle+\|10\rangle)_{AB}$	$MR_A=\overline{MR_B}$
	I	H	$\frac{1}{2}(\|00\rangle-\|01\rangle+\|10\rangle+\|11\rangle)_{AB}$	Uncertain
	H	I	$\frac{1}{2}(\|00\rangle+\|01\rangle-\|10\rangle+\|11\rangle)_{AB}$	Uncertain
	H	H	$\frac{1}{\sqrt{2}}(\|00\rangle-\|11\rangle)_{AB}$	$MR_A=MR_B$
$\left\|\Psi^{-}\right\rangle_{AB}$	I	I	$\frac{1}{\sqrt{2}}(\|01\rangle-\|10\rangle)_{AB}$	$MR_A=\overline{MR_B}$
	I	H	$\frac{1}{2}(\|00\rangle-\|01\rangle-\|10\rangle+\|11\rangle)_{AB}$	Uncertain
	H	I	$\frac{1}{2}(-\|00\rangle+\|01\rangle+\|10\rangle+\|11\rangle)_{AB}$	Uncertain
	H	H	$\frac{-1}{\sqrt{2}}(\|01\rangle-\|10\rangle)_{AB}$	$MR_A=\overline{MR_B}$

Table 1. Relationship between measurement results and unitary operations.

$$\begin{aligned}
I\otimes I\left|\Psi^{+}\right\rangle_{AB}&=\frac{1}{\sqrt{2}}(|01\rangle+|10\rangle)_{AB}\\
I\otimes H\left|\Psi^{+}\right\rangle_{AB}&=\frac{1}{\sqrt{2}}(|0-\rangle+|1+\rangle)_{AB}=\frac{1}{2}(|00\rangle-|01\rangle+|10\rangle+|11\rangle)_{AB}\\
H\otimes I\left|\Psi^{+}\right\rangle_{AB}&=\frac{1}{\sqrt{2}}(|+1\rangle+|-0\rangle)_{AB}=\frac{1}{2}(|00\rangle+|01\rangle-|10\rangle+|11\rangle)_{AB}\\
H\otimes H\left|\Psi^{+}\right\rangle_{AB}&=\frac{1}{\sqrt{2}}(|+-\rangle+|-+\rangle)_{AB}=\frac{1}{\sqrt{2}}(|00\rangle-|11\rangle)_{AB}
\end{aligned} \tag{6}$$

$$\begin{aligned}
I\otimes I\left|\Psi^{-}\right\rangle_{AB}&=\frac{1}{\sqrt{2}}(|01\rangle-|10\rangle)_{AB}\\
I\otimes H\left|\Psi^{-}\right\rangle_{AB}&=\frac{1}{\sqrt{2}}(|0-\rangle-|1+\rangle)_{AB}=\frac{1}{2}(|00\rangle-|01\rangle-|10\rangle+|11\rangle)_{AB}\\
H\otimes I\left|\Psi^{-}\right\rangle_{AB}&=\frac{1}{\sqrt{2}}(|+1\rangle-|-0\rangle)_{AB}=\frac{1}{2}(-|00\rangle+|01\rangle+|10\rangle+|11\rangle)_{AB}\\
H\otimes H\left|\Psi^{-}\right\rangle_{AB}&=\frac{1}{\sqrt{2}}(|+-\rangle-|-+\rangle)_{AB}=\frac{-1}{\sqrt{2}}(|01\rangle-|10\rangle)_{AB}
\end{aligned} \tag{7}$$

Encryption chain for the encoding function. Suppose all the four cases (i.e., $I\otimes I$, $I\otimes H$, $H\otimes I$, $H\otimes H$) are evenly distributed; then only the qubits in $I\otimes I$ and $H\otimes H$ can be used as the secret key bits or checking bits. Based on the relationship mentioned above (see also Table 1), Alice and Bob only have a 50% probability of performing the same unitary operations. Hence, they can use their measurement results as secret key bits or check bits only with 50% of probability.

To improve the qubit efficiency, Alice and Bob decide to perform the unitary operations I or H on q_A and q_B based on their previous measurement results, MR_A^i and MR_B^i, where i represents the i-th time measurement result. The concept of the coding function is illustrated in Fig. 1. We first prepare the Bell state $\left|\Phi^{+}\right\rangle=\frac{1}{\sqrt{2}}(|00\rangle+|11\rangle)_{AB}$ as the quantum carrier, where $|0\rangle$ represents the classical bit "0" and $|1\rangle$ represents the classical bit "1". The encoding function is expressed as follows:

- If $i=0$, then Bob randomly decides to perform the unitary operations I or H on qubit q_B^i to obtain q'^i_B. Then, he measures qubit q'^i_B to obtain the measurement result MR_B^i using Z-basis.
- If $i=1\sim n$, then Bob performs the unitary operations I or H based on the measurement result $MR_B^{i-1}=0/1$. For $MR_B^{i-1}=0$, Bob performs the identity operator I on qubit q_B^i to obtain q'^i_B. Then, he measures the qubit q'^i_B to obtain the measurement result MR_B^i using Z-basis. Otherwise, $MR_B^{i-1}=1$, and Bob performs the Hadamard operator H on qubit q_B^i and measures it.

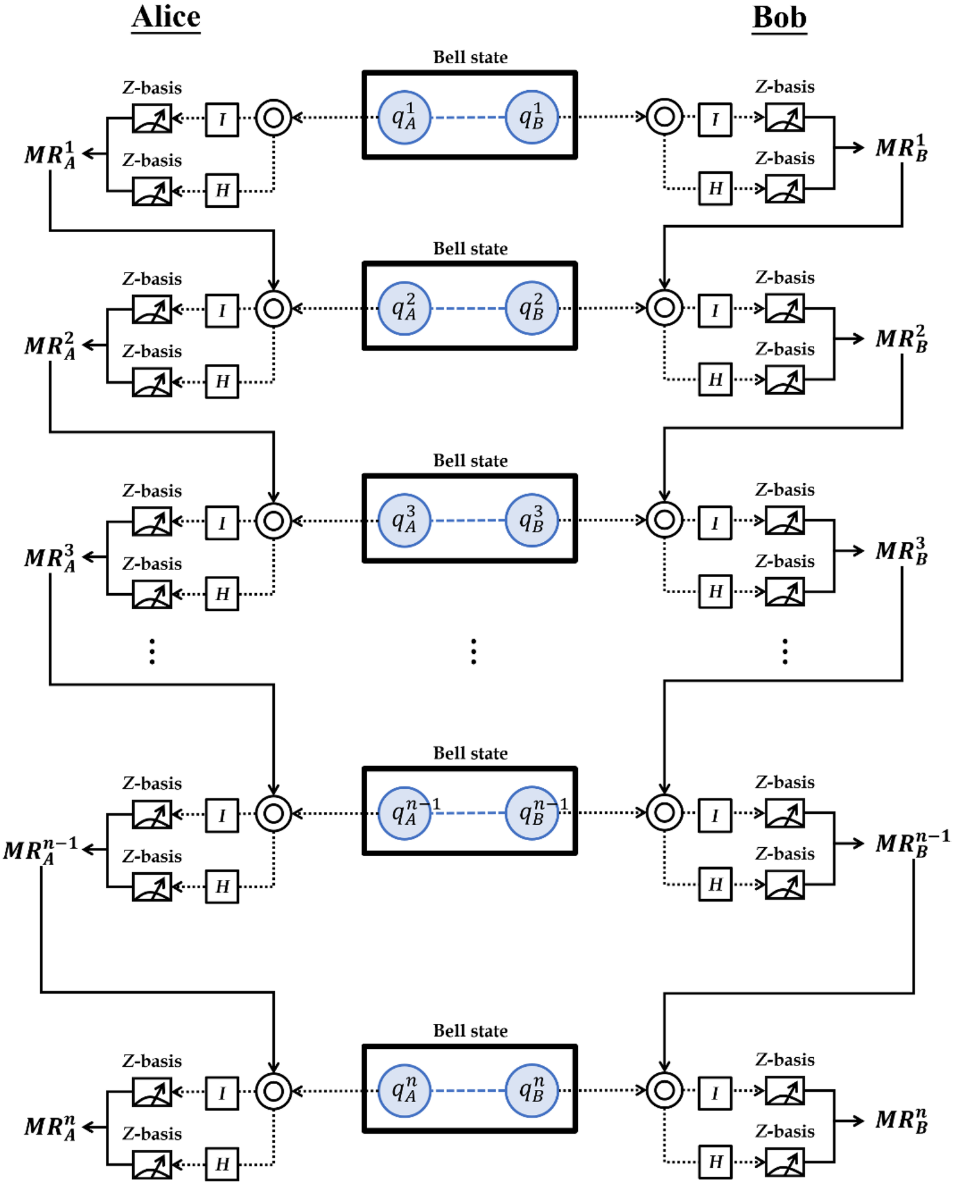

Figure 1. Concept of the coding function.

Encryption chain for the decoding function. In the proposed encoding function, it is guaranteed that Alice and Bob always use the same unitary operations (i.e., $I \otimes I$ or $H \otimes H$), then they will obtain the same measurement results. Hence, based on the Z-basis measurement result of the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$, a decoding table can be constructed (see Table 2). If Alice and Bob perform the same operations (i.e., $I \otimes I$ or $H \otimes H$) on 1st and 2nd qubits in the Bell state $|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$ and also perform the Z-basis measurement on 1st and 2nd qubits, then they can obtain the same measurement result (i.e., "00" or "11"). The concept of a decoding function is described below. Alice's and Bob's measurement results (i.e., "00" or "11") can be used to decide their next operation as either $I \otimes I$ or $H \otimes H$. The decoding function is expressed as follows.

- If $i = 0$, then Bob announces his operation (i.e., I or H). Subsequently, Alice can perform the same operation on q_A^i and measure it to obtain the measurement result MR_A^i using Z-basis.
- If $i = 1 \sim n$, then Alice performs the unitary operations I or H based on the measurement result $MR_A^{i-1} = 0/1$. For $MR_A^{i-1} = 0$, Alice performs the identity operator I on qubit q_A^i to obtain q'^i_A. Subsequently, she measures qubit q'^i_A to obtain the measurement result MR_A^i by using Z-basis. Otherwise, $MR_A^{i-1} = 1$, and Alice performs Hadamard operator H on qubit q_A^i and measures it.

Initial state	Alice's operation	Bob's operation	Quantum state	Relationship between the measurement results	Alice's and Bob's next operation
$\lvert\Phi^+\rangle_{AB}$	I	I	$\frac{1}{\sqrt{2}}(\lvert 00\rangle + \lvert 11\rangle)_{AB}$	$MR_A = MR_B = 0$	I
				$MR_A = MR_B = 1$	H
	H	H	$\frac{1}{\sqrt{2}}(\lvert 00\rangle + \lvert 11\rangle)_{AB}$	$MR_A = MR_B = 0$	I
				$MR_A = MR_B = 1$	H

Table 2. Encoding and decoding table.

Proposed unitary-operation-based SQKD protocol

In this section, a unitary-operation-based SQKD protocol is presented based on the encryption chain proposed in "Encryption chain based on the measurement result". Suppose that the quantum channels are ideal and that the classical channels are authenticated. We assume that a quantum communicator (Alice) wants to distribute a secret key with a classical communicator (Bob), which has two quantum capabilities: (1) performing Z-basis measurement and (2) performing identity operator I or Hadamard operator H. Figure 2 clearly illustrates the proposed unitary-operation-based SQKD protocol. The steps involved in the SQKD protocol are as follows:

Step 1. Alice generates n Bell states in $\left|\Phi^+\right\rangle = \frac{1}{\sqrt{2}}(|00\rangle\ + |11\rangle\ )$. She takes the first and second photons from each Bell state to form the order sequences $S_A = \left\{q_A^i\right\}andS_B = \left\{q_B^i\right\}$, for $i = 1, 2, \ldots, n$. Then, Alice sends $S_B = \left\{q_B^i\right\}$ to Bob one photon at a time.

Step 2. For every received photon q_B^i, Bob randomly selects KEY or CHECK mode. In KEY mode, Bob can perform the following operations:

- If $i = 0$, then Bob randomly decides to perform the unitary operations I or H on the qubit q_B^i to obtain q'^i_B. Then, he measures the qubit q'^i_B to obtain the measurement result K_B^i using Z-basis.
- If $i = 1 \sim n$, then Bob performs the unitary operations I or H based on the measurement result $K_B^{i-1} = 0(1)$. For $K_B^{i-1} = 0(1)$, Bob performs the identity operator I (Hadamard operator H) on qubit q_B^i to obtain q'^i_B. Then, he measures the qubit q'^i_B to obtain the measurement result K_B^i using Z-basis.

In CHECK mode, Bob performs the same operations and records the measurement result C_B^i.

Step 3. After Bob completes his operations, he announces the operations of K_B^0 and C_B^0 (i.e., the operations of the first selection in K_B^i and C_B^i), positions of the CHECK mode, and measurement result of C_B^i to Alice via an authenticated classical channel.

Step 4. When Alice receives information from Bob, she can perform the following operations in KEY mode:

- If $i = 0$, then Alice can perform the same operation with Bob on q_A^i and measure it to obtain the measurement result K_A^i using Z-basis.
- If $i = 1 \sim n$, then Alice performs the unitary operations I or H based on the measurement result $K_A^{i-1} = 0(1)$. For $K_A^{i-1} = 0(1)$, Alice performs the identity operator I (Hadamard operator H) on the qubit q_A^i to obtain q'^i_A. Then, she measures qubit q'^i_A to obtain measurement result K_A^i using Z-basis.

In CHECK mode, Alice performs the same operations and records the measurement result, C_A^i.

Step 5. Based on Table 2, Alice can check $C_A^i = C_B^i$ for the first eavesdropping check. If eavesdropping is not detected, Alice randomly divides the sequence $K_A = \left\{K_A^i | i = 1, 2, \ldots, n\right\}$ into two sequences, namely, K_{AB} and K_{CA}. Further, Alice sends the positions and values of K_{CA} to Bob via an authenticated classical channel. Otherwise, Alice asks Bob to abort the process and start a new process.

Step 6. When Bob receives the information from Alice, he can divide the sequence $K_B = \left\{K_B^i | i = 1, 2, \ldots, n\right\}$ into two sequences, namely K_{AB} and K_{CB}. Then, he/she can check $K_{CA} = K_{CB}$ for the second eavesdropping check. If eavesdropping is not detected, Bob sends an acknowledgment to Alice and shares the raw key K_{AB}. Otherwise, Bob asks Alice to abort the process and start a new process. Eventually, if the quantum transmission between Alice and Bob is secure, then they can distil the secret key using the privacy amplification process[69] on the raw key.

It should be noted that the proposed unitary-operation-based SQKD protocol is secure against Trojan-horse attacks because one-way transmission is adopted. Furthermore, in the proposed SQKD protocol, Alice and Bob can generate the pure-random key because of the property of Z-basis measurements in Bell states. More details of the security and efficiency analyses are provided in "Security analysis" and "Efficiency analysis", respectively.

Security analysis

In this section, the security of the proposed SQKD protocol with respect to the three main attacks is discussed.

Security against collective attack.

Collective attacks[70,71] are a particularly important class of attacks because of their well-known nature such as intercept-and-resend attacks and measure-and-resend attacks. Furthermore, a collective attack is considered as the most general attack[72–75]. Thus, in this study, we prove that the proposed SQKD protocol can be secure against a collective attack to prove the proposed scheme is robust.

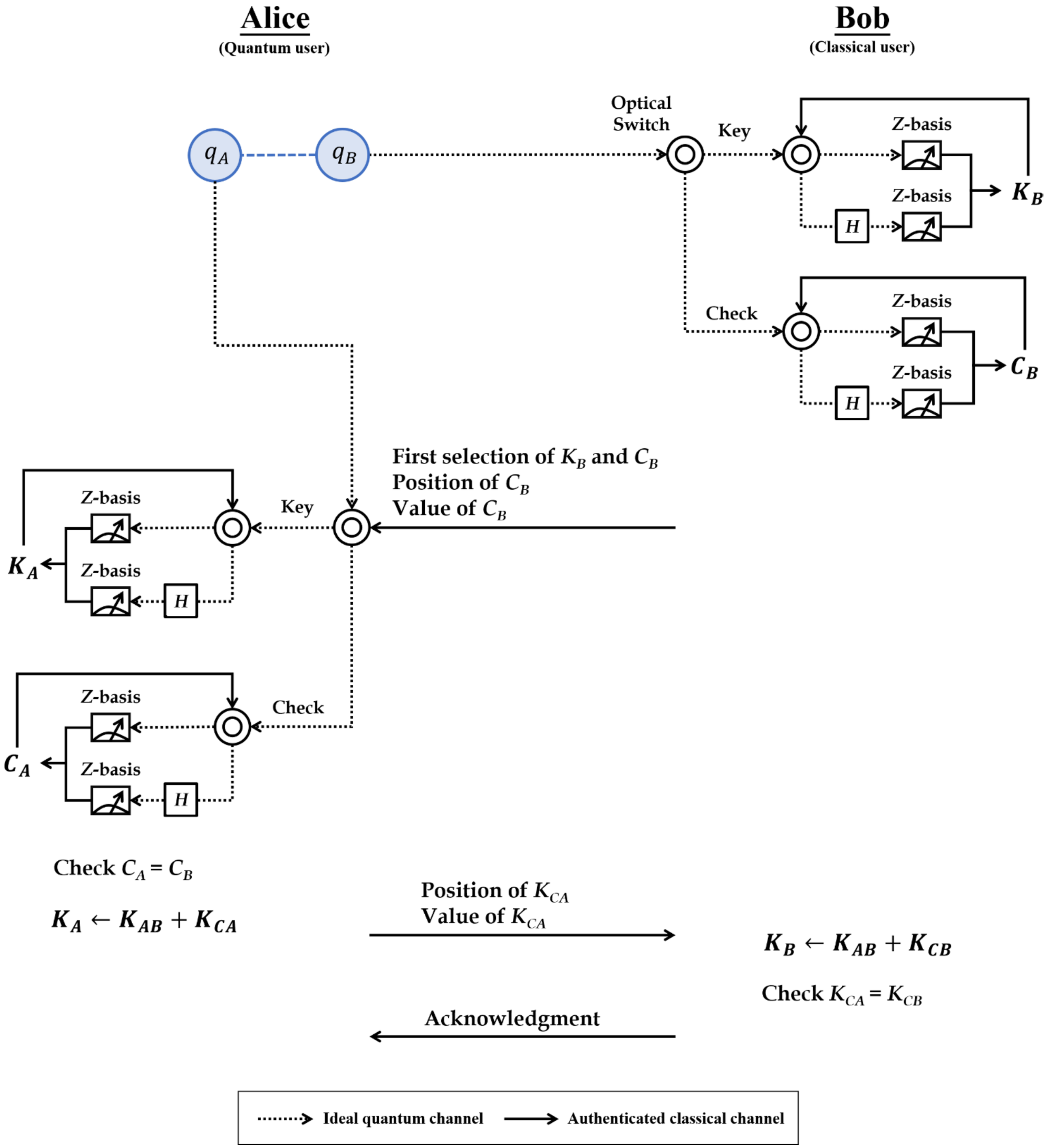

Figure 2. Operational procedure of the proposed SQKD protocol.

Before analyzing the collective attack, we assume an eavesdropper, Eve, who possesses full quantum devices with unlimited computational power and can tamper with the transmitted qubits in the quantum channel. In the collective attack, Eve attempts to eavesdrop on any useful information from Alice and Bob. However, we will prove that Eve cannot reveal any useful information without being detected. In other words, Eve can capture the information, but she will introduce a detectable interruption to the quantum system. Eve performs the collective attack as follows.

In Step 1, Alice sends $S_B = \left\{q_B^i\right\}$ to Bob one photon at a time. Then, Eve generates ancillary qubits $|E\rangle = \{|E_1\rangle, |E_2\rangle, \ldots, |E_n\rangle\}$ and implements a unitary operation, U_E, on the joint states $q_B^i \otimes |E_i\rangle$. In the proposed SQKD protocol, Alice and Bob perform two eavesdropping checks to verify their measurement result in Steps 5 and 6. To pass the eavesdropping check, Eve considers the following two situations: (1) Alice and Bob perform the same unitary operations $I \otimes I$ and (2) they perform the same unitary operations $H \otimes H$. We assume that Eve performs a unitary operation to attack the transmitted qubit from Alice to Bob in Step 1 using U_E. This can be defined as follows:

$$U_E\left(I \otimes I\left|\Phi^{+}\right\rangle \otimes |E_{\mathrm{i}}\rangle\right) = \alpha_0|00\rangle|e_0\rangle + \alpha_1|01\rangle|e_1\rangle + \alpha_2|10\rangle|e_2\rangle + \alpha_3|11\rangle|e_3\rangle \tag{8}$$

$$U_E\left(H \otimes H\left|\Phi^{+}\right\rangle \otimes |E_{\mathrm{i}}\rangle\right) = \frac{1}{2}\begin{bmatrix} |00\rangle \otimes (\alpha_0|e_0\rangle + \alpha_1|e_1\rangle + \alpha_2|e_2\rangle + \alpha_3|e_3\rangle) \\ +|01\rangle \otimes (\alpha_0|e_0\rangle - \alpha_1|e_1\rangle + \alpha_2|e_2\rangle - \alpha_3|e_3\rangle) \\ +|10\rangle \otimes (\alpha_0|e_0\rangle + \alpha_1|e_1\rangle - \alpha_2|e_2\rangle - \alpha_3|e_3\rangle) \\ +|11\rangle \otimes (\alpha_0|e_0\rangle - \alpha_1|e_1\rangle - \alpha_2|e_2\rangle + \alpha_3|e_3\rangle) \end{bmatrix} \tag{9}$$

where $|E_i\rangle$ denotes the initial state of Eve's ancillary qubit; $|e_0\rangle, |e_1\rangle, |e_2\rangle$, and $|e_3\rangle$ are four states that can be distinguished by Eve (i.e., the four states are orthogonal to each other); and $|\alpha_0|^2 + |\alpha_1|^2 + |\alpha_2|^2 + |\alpha_3|^2 = 1$.

In case (1), if Eve passes the eavesdropping check, then she must set $\alpha_1 = \alpha_2 = 0$. However, according to this setting, the quantum system for $U_E\left(I \otimes I\left|\Phi^{+}\right\rangle \otimes |E_{\mathrm{i}}\rangle\right)$ can be expressed as follows:

$$U_E\left(I \otimes I\left|\Phi^{+}\right\rangle \otimes |E_{\mathrm{i}}\rangle\right) = \alpha_0|00\rangle|e_0\rangle + \alpha_3|11\rangle|e_3\rangle \tag{10}$$

In case (2), if Eve passes the eavesdropping check, then she must set $\alpha_0|e_0\rangle - \alpha_1|e_1\rangle + \alpha_2|e_2\rangle - \alpha_3|e_3\rangle = \alpha_0|e_0\rangle + \alpha_1|e_1\rangle - \alpha_2|e_2\rangle - \alpha_3|e_3\rangle = 0$. This implies that $\alpha_0|e_0\rangle - \alpha_3|e_3\rangle = 0$ signifies $\alpha_0|e_0\rangle = \alpha_3|e_3\rangle$. However, according to this setting, the quantum system for $U_E\left(H \otimes H\left|\Phi^{+}\right\rangle \otimes |E_{\mathrm{i}}\rangle\right)$ can be expressed as follows:

$$U_E\left(H \otimes H\left|\Phi^{+}\right\rangle \otimes |E_{\mathrm{i}}\rangle\right) = \frac{1}{2}\begin{bmatrix} |00\rangle \otimes (\alpha_0|e_0\rangle + \alpha_3|e_3\rangle) \\ +|11\rangle \otimes (\alpha_0|e_0\rangle + \alpha_3|e_3\rangle) \end{bmatrix} \tag{11}$$

In conclusion, if Eve wants to pass the eavesdropping check, then she must make $\alpha_0|e_0\rangle = \alpha_3|e_3\rangle$. Eve cannot measure the ancillary qubits $|E\rangle = \{|E_1\rangle, |E_2\rangle, \ldots, |E_n\rangle\}$ to capture the information about Alice's and Bob's measurement results because she cannot distinguish $\alpha_0|e_0\rangle$ from $\alpha_3|e_3\rangle$. Conversely, if Eve wants to reveal the information about Alice's and Bob's measurement results, then she must set $\alpha_0|e_0\rangle \neq \alpha_3|e_3\rangle$ (i.e., Eve must make the auxiliary qubit distinguishable). Based on Eq. (11), Eve will disturb the entanglement of the Bell state and will eventually be detected in the eavesdropping check. Therefore, there is no unitary operation for Eve to capture the information about the secret key without being detected. Thus, the proposed SQKD protocol is free from collective attack.

Security against Trojan horse attack.

Trojan horse attacks[64–66] are common attacks, in which Eve can potentially insert Trojan-horse photons into the transmitted photons sent from Alice. Then, Eve attempts to capture Bob's information in Step 2 using the measurement result of Trojan-horse photons. However, in the proposed SQKD protocol, the semi-quantum environment (i.e., unitary-operation-based) adopts a one-way transmission strategy as opposed to the round-trip transmission (i.e., randomization-based, measure-resend, and measurement-free). Thus, the classical communicator is not required to be equipped with extra hardware (e.g., photon number splitter and optical wavelength filter devices) to be immune to Trojan-horse attacks.

Security against intercept-resend attack.

In this section, we will analyze the security of the proposed SQKD protocol based on the encryption chain, and we assume the existence of an eavesdropper Eve in the middle of the communication between Alice and Bob, and do a probabilistic security analysis based on the attack pattern that Eve can do. Eve wants to obtain the secret key shared by Alice and Bob, and the attack strategy is based on the principle that the maximum chance of getting the secret key and its existence will not be discovered. Therefore, Eve's attack mode is to intercept the sequence $S_B = \left\{q_B^i\right\}$ and guess the unitary operation directly before doing the Z-basis measurement, that is, to do the guessing the unitary operation as identity operator I or Hadamard operator H for each q_B^i and then do the Z-basis measurement. However, if Eve performs a different unitary operation than the original one, the measurement result will be uncertain, with a 50% chance of being "0" or "1", i.e., there is a 50% chance of using the wrong unitary operation to measure the correct result. Therefore, by performing the intercept-resend attack, the eavesdropper can pass the eavesdropping check with a probability of $\left(\frac{3}{4}\right)^n$(assuming that the total number of q_B^i transmitted is n). The probability of $\left(\frac{3}{4}\right)^n$ is the same as that of the BB84 protocol[7]. Thus, the probability to detect the intercept-resend attack in this protocol is $1 - \left(\frac{3}{4}\right)^n$. If n is large enough, the detection rate would converge to 1, as shown in Fig. 3.

Efficiency analysis

Table 3 compares several important parameters of Boyer et al.'s, Wang et al.'s, and Zhou et al.'s SQKD protocols with those of the proposed SQKD protocol. We consider $\eta = \frac{c}{q}$ as the qubit efficiency of a quantum cryptographic protocol[76–78], where c denotes the total number of shared secret bits and q denotes the total number of qubits generated by the protocol. Furthermore, we assume that half of the qubits transmitted in the eavesdropping check of the protocol are used to detect the presence of eavesdroppers and the remaining half of the transmitted qubits are used to check for Trojan horse attacks.

In Boyer et al.'s SQKD protocols, Alice prepares n single photons (i.e., $|0\rangle, |1\rangle, |+\rangle, |-\rangle$), and each single photon can be used to share 1-bit raw key. Bob has a 50% chance of choosing the share mode and a 50% chance of choosing the check mode. In share mode, Bob has a 50% chance of using the right basis and a 50% chance of using the wrong basis. Besides, one round of public discussion was used in the share mode, and half of the transmitted qubits were used to check for Trojan horse attacks. Therefore, the qubit efficiency of Boyer et al.'s SQKD protocols corresponded to $\frac{n}{n} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{16} = 6.25\%$.

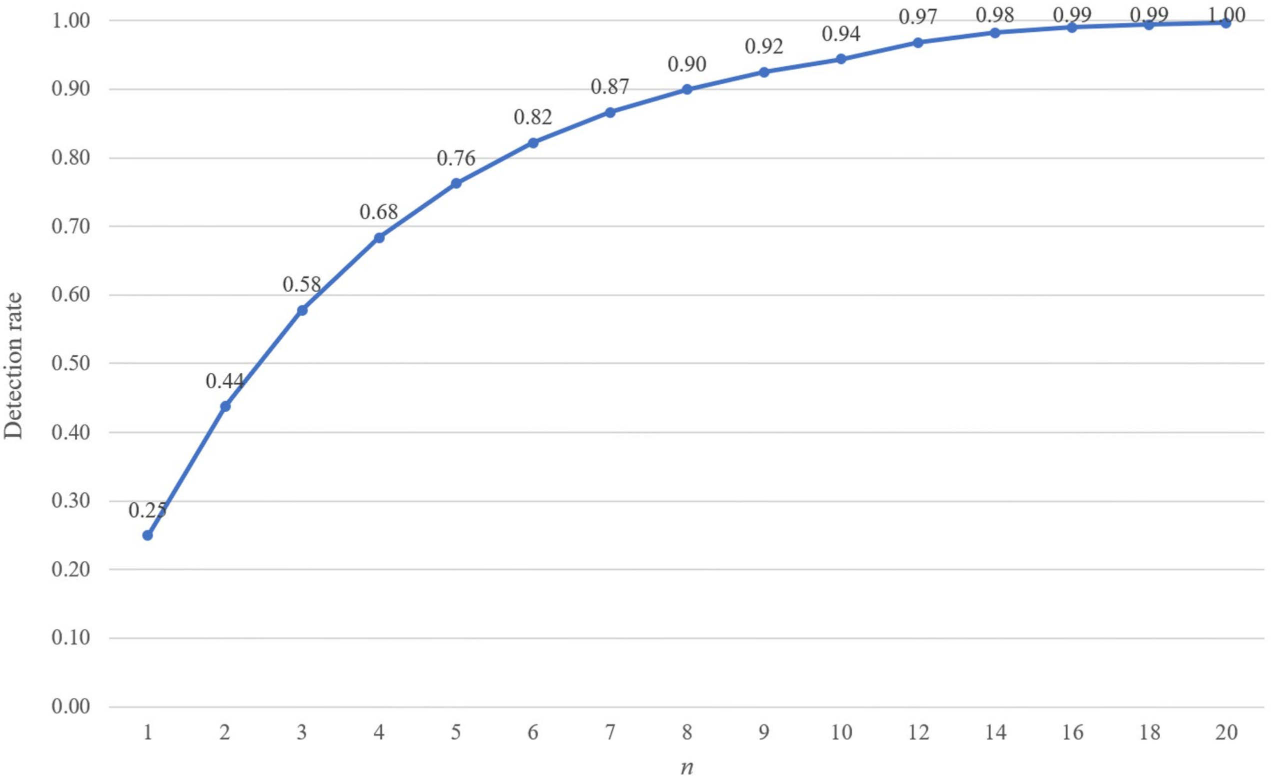

Figure 3. Detection rate of the intercept-resend attack.

	Boyer et al.'s protocol[34]	Boyer et al.'s protocol[34]	Wang et al.'s protocol[36]	Wang et al.'s protocol[36]	Zhou et al.'s protocol[46]	Proposed protocol
Semi-quantum environment	Randomization-based	Measure-resend	Randomization-based	Measure-resend	Measure-resend	Unitary-operation-based
Quantum capability of classical participant	(1) Measurement (2) Reorder photons (3) Reflection	(1) Generation (2) Measurement (3) Reflection	(1) Measurement (2) Reorder photons (3) Reflection	(1) Generation (2) Measurement (3) Reflection	(1) Generation (2) Measurement (3) Reflection	(1) Measurement (2) Operation
Quantum resource	Single photon	Single photon	Bell state	Bell state	Cluster state	Bell state
Qubit efficiency	6.25%	6.25%	6.25%	6.25%	3.125%	12.5%
Qubit measurement for Quantum user	Z-basis measurement X-basis measurement	Z-basis measurement X-basis measurement	Bell measurement Z-basis measurement	Bell measurement Z-basis measurement	Z-basis measurement Bell measurement Cluster-basis measurement	Z-basis measurement
Quantum communication	Round-trip	Round-trip	Round-trip	Round-trip	Round-trip	One-way
Vulnerability to Trojan-horse attacks	No	No	No	No	No	No
Photon number splitter	Yes	Yes	Yes	Yes	Yes	No
Wavelength filter	Yes	Yes	Yes	Yes	Yes	No

Table 3. Comparison of various parameters of Boyer et al.'s, Wang et al.'s, and Zhou et al.'s protocols and the proposed protocol.

In Wang et al.'s SQKD protocols, Alice must generate n Bell states (i.e., $2n$ qubits), and each Bell state can be used to share 1-bit raw key. Two rounds of public discussion were used in Wang et al.'s SQKD protocols, and half of the transmitted qubits were used to check for Trojan horse attacks. Therefore, the qubit efficiency of Wang et al.'s SQKD protocols corresponded to $\frac{n}{2n} \times \frac{1}{2} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{16} = 6.25\%$.

In Zhou et al.'s SQKD protocol, Charlie prepares n Cluster states (i.e., $4n$ qubits), and each Cluster state can be used to share 2-bit raw key. Alice and Bob each have a 50% chance of choosing the share mode and a 50% chance of choosing the check mode. Only when Alice and Bob select share mode at the same time, they can use it for sharing the secret key. The chance of this happening is only 25%. Besides, one round of public discussion was used in the share mode, and half of the transmitted qubits were used to check for Trojan horse attacks. Therefore, the qubit efficiency of Zhou et al.'s SQKD protocol corresponded to $\frac{2n}{4n} \times \frac{1}{4} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{32} = 3.125\%$.

In the proposed SQKD protocol, each Bell state can be used to encode 1-bit raw key. Alice generates *n* Bell states (2*n* qubits). Two rounds of public discussion are conducted in the proposed SQKD protocol. Therefore, the qubit efficiency of the proposed SQKD protocol is $\frac{n}{2n} \times \frac{1}{2} \times \frac{1}{2} = \frac{1}{8} = 12.5\%$. Obviously, the qubit efficiency of the proposed SQKD protocol is twice that of Boyer et al.'s and Wang et al.'s SQKD protocols. The qubit efficiency of the proposed SQKD protocol is four times higher than that of Zhou et al.'s SQKD protocol. The SQKD protocols proposed by Wang et al., Boyer et al., and Zhou et al. are vulnerable to Trojan horse attacks. Furthermore, the qubit efficiency of Wang et al.'s, Boyer et al.'s, and Zhou et al.'s SQKD protocols decrease to 50% if a photon number splitter and wavelength filter are applied to avoid Trojan horse attacks. Moreover, in Wang et al.'s SQKD protocols, the quantum user (Alice) must perform Bell-basis and Z-basis measurements because of the design of the eavesdropping check. In Zhou et al.'s SQKD protocol, the quantum user (Alice) must perform Cluster-basis, Bell-basis, and Z-basis measurements because of the design of the eavesdropping check. Therefore, in the proposed SQKD protocol, Alice is required to solely implement the measurement of single photons, which is simpler than Cluster-basis and Bell-basis measurements.

Conclusion

In this study, a new coding function, also known as an encryption chain based on the measurement result, was proposed. A novel unitary-operation-based SQKD protocol was designed based on this new coding function. The proposed SQKD protocol is more efficient and practical than the existing SQKD protocols because it is designed based on one-way transmission as opposed to round-trip transmission, which is congenitally immune to Trojan horse attacks without the need of any extra hardware. Moreover, security analysis showed that the proposed SQKD protocol can avoid collective attacks. Additionally, the proposed SQKD protocol provides the best qubit efficiency among the existing SQKD protocols, and classical participants are required to possess only two quantum capabilities, which enhances its practicability. Furthermore, the proposed coding function can be useful in applications involving semi-quantum secret sharing protocols and semi-quantum communication protocols for improving qubit efficiency. However, this requires further investigation.

Data availability

All data generated or analysed during this study are included in this published article.

Received: 4 August 2022; Accepted: 25 October 2022
Published online: 01 November 2022

References

1. Allahyari, E. Application of artificial neural network in predicting EI. *Biomedicine* **10**(3), 3 (2020).
2. Ramesh, P., Karuppasamy, R. & Veerappapillai, S. A review on recent advancements in diagnosis and classification of cancers using artificial intelligence. *Biomedicine* **10**(3), 2 (2020).
3. Allahyari, E. & Moshtagh, M. Predicting mental health of prisoners by artificial neural network. *Biomedicine* **11**(1), 3 (2021).
4. Allahyari, E. & Roustaei, N. Applying artificial neural-network model to predict psychiatric symptoms. *Biomedicine* **12**(1), 1 (2021).
5. Cheng, C. F., Huang, E.T.-C., Kuo, J.-T., Liao, K.Y.-K. & Tsai, F. J. Report of clinical bone age assessment using deep learning for an Asian population in Taiwan. *Biomedicine* **11**(3), 8 (2021).
6. Shor, P. W. Algorithms for quantum computation: discrete logarithms and factoring. in *Proceedings of the 35th Annual Symposium on the Foundations of Computer Science, Los Alamitos, CA, USA* (1994).
7. 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* (1984).
8. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.* **68**(5), 557–559 (1992).
9. Long, G. & Liu, X. Theoretically efficient high-capacity quantum-key-distribution scheme. *Phys. Rev. A* **65**(3), 032302 (2002).
10. Deng, F.-G., Long, G. & Liu, X.-S. Two-step quantum direct communication protocol using the Einstein-Podolsky-Rosen pair block. *Phys. Rev. A* **68**(4), 042317 (2003).
11. Kwek, L.-C. *et al.* Chip-based quantum key distribution. *AAPPS Bull.* **31**(1), 15 (2021).
12. Liu, W.-B. *et al.* Homodyne detection quadrature phase shift keying continuous-variable quantum key distribution with high excess noise tolerance. *PRX Quantum* **2**(4), 040334 (2021).
13. Xie, Y.-M. *et al.* Overcoming the rate–distance limit of device-independent quantum key distribution. *Opt Lett* **46**(7), 1632–1635 (2021).
14. Yu-FeiYan, L. Z. & WeiZhong, Y.-B.S. Measurement-device-independent quantum key distribution of multiple degrees of freedom of a single photon. *Front. Phys.* **16**(1), 11501 (2021).
15. Zhang, M., Dou, Y., Huang, Y., Jiang, X.-Q. & Feng, Y. Improved information reconciliation with systematic polar codes for continuous variable quantum key distribution. *Quantum Inf. Process.* **20**(10), 327 (2021).
16. Zhou, C. *et al.* Rate compatible reconciliation for continuous-variable quantum key distribution using Raptor-like LDPC codes. *Sci. China Phys.* **64**(6), 260311 (2021).
17. Aguiar, L. S., Borelli, L. F. M., Roversi, J. A. & Vidiella-Barranco, A. Performance analysis of continuous-variable quantum key distribution using non-Gaussian states. *Quantum Inf. Process.* **21**(8), 304 (2022).
18. Gao, R.-Q. *et al.* Simple security proof of coherent-one-way quantum key distribution. *Opt. Express* **30**(13), 23783–23795 (2022).
19. Liu, B. *et al.* Decoy-state method for quantum-key-distribution-based quantum private query. *Sci. China Phys.* **65**(4), 240312 (2022).
20. Peng, Q., Guo, Y., Liao, Q. & Ruan, X. Satellite-to-submarine quantum communication based on measurement-device-independent continuous-variable quantum key distribution. *Quantum Inf. Process.* **21**(2), 61 (2022).
21. Xie, Y.-M. *et al.* Breaking the rate-loss bound of quantum key distribution with asynchronous two-photon interference. *PRX Quantum* **3**(2), 020315 (2022).
22. Zhao, W. *et al.* Monte Carlo-based security analysis for multi-mode continuous-variable quantum key distribution over underwater channel. *Quantum Inf. Process.* **21**(5), 186 (2022).
23. Zhou, Y.-H., Qin, S.-F., Shi, W.-M. & Yang, Y.-G. Measurement-device-independent continuous variable semi-quantum key distribution protocol. *Quantum Inf. Process.* **21**(8), 303 (2022).
24. Hu, J.-Y. *et al.* Experimental quantum secure direct communication with single photons. *Light Sci. Appl.* **5**(9), e16144 (2016).

25. Zhang, W. *et al.* Quantum secure direct communication with quantum memory. *Phys. Rev. Lett.* **118**(22), 220501 (2017).
26. Qi, Z. *et al.* A 15-user quantum secure direct communication network. *Light Sci. Appl.* **10**(1), 183 (2021).
27. Sheng, Y.-B., Zhou, L. & Long, G.-L. One-step quantum secure direct communication. *Sci. Bull.* **67**(4), 367–374 (2022).
28. Zhou, L. & Sheng, Y.-B. One-step device-independent quantum secure direct communication. *Sci. China Phys.* **65**(5), 250311 (2022).
29. Lo, H. K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**(5410), 2050–2056 (1999).
30. Shor, P. W. & Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**(2), 441–444 (2000).
31. Lo, H. K. A simple proof of the unconditional security of quantum key distribution. *J. Phys. A Math. General* **34**(35), 6957–6967 (2001).
32. Mayers, D. Unconditional security in quantum cryptography. *J Acm* **48**(3), 351–406 (2001).
33. Boyer, M., Kenigsberg, D. & Mor, T. Quantum key distribution with classical bob. *Phys. Rev. Lett.* **99**(14), 140501 (2007).
34. Boyer, M., Gelles, R., Kenigsberg, D. & Mor, T. Semiquantum key distribution. *Phys. Rev. A* **79**(3), 032341 (2009).
35. Zou, X., Qiu, D., Li, L., Wu, L. & Li, L. Semiquantum-key distribution using less than four quantum states. *Phys. Rev. A* **79**(5), 052312 (2009).
36. Wang, J., Zhang, S., Zhang, Q. & Tang, C. J. Semiquantum key distribution using entangled states. *Chin. Phys. Lett.* **28**(10), 100301 (2011).
37. Sun, Z.-W., Du, R.-G. & Long, D.-Y. Quantum key distribution with limited classical bob. *Int. J. Quant. Infor.* **11**(01), 1350005 (2013).
38. Krawec, W. O. Mediated semiquantum key distribution. *Phys. Rev. A* **91**(3), 032323 (2015).
39. Li, Q., Chan, W. H. & Zhang, S. Semiquantum key distribution with secure delegated quantum computation. *Sci. Rep.* **6**, 19898 (2016).
40. Yu, K.-F., Gu, J., Hwang, T. & Gope, P. Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing. *Quantum Inf. Process.* **16**(8), 194 (2017).
41. Tsai, C.-L. & Hwang, T. Semi-quantum key distribution robust against combined collective noise. *Int. J. Theor. Phys.* **57**(11), 3410–3418 (2018).
42. Zhu, K.-N., Zhou, N.-R., Wang, Y.-Q. & Wen, X.-J. Semi-quantum key distribution protocols with GHZ states. *Int. J. Theor. Phys.* **57**(12), 3621–3631 (2018).
43. Amer, O. & Krawec, W. O. Semiquantum key distribution with high quantum noise tolerance. *Phys. Rev. A* **100**(2), 022319 (2019).
44. Tsai, C.-W. & Yang, C.-W. Cryptanalysis and improvement of the semi-quantum key distribution robust against combined collective noise. *Int. J. Theor. Phys.* **58**(7), 2244–2250 (2019).
45. Wang, M.-M., Gong, L.-M. & Shao, L.-H. Efficient semiquantum key distribution without entanglement. *Quantum Inf. Process.* **18**(9), 260 (2019).
46. Zhou, N.-R., Zhu, K.-N. & Zou, X.-F. Multi-party semi-quantum key distribution protocol with four-particle cluster states. *Ann. Phys.* **531**(8), 1800520 (2019).
47. Hajji, H. & El Baz, M. Qutrit-based semi-quantum key distribution protocol. *Quantum Inf. Process.* **20**(1), 4 (2021).
48. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**(13), 130503 (2012).
49. Liu, Y. *et al.* Experimental measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **111**(13), 130502 (2013).
50. Tang, Y.-L. *et al.* Measurement-device-independent quantum key distribution over 200 km. *Phys. Rev. Lett.* **113**(19), 190501 (2014).
51. Tang, Z. *et al.* Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **112**(19), 190503 (2014).
52. Yin, H.-L. *et al.* Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**(19), 190501 (2016).
53. Zou, X., Qiu, D., Zhang, S. & Mateus, P. Semiquantum key distribution without invoking the classical party's measurement capability. *Quantum Inf. Process.* **14**(8), 2981–2996 (2015).
54. Liu, Z.-R. & Hwang, T. Mediated semi-quantum key distribution without invoking quantum measurement. *Ann. Phys.* **530**(4), 1700206 (2018).
55. Tsai, C.-W., Yang, C.-W. & Lee, N.-Y. Lightweight mediated semi-quantum key distribution protocol. *Mod. Phys. Lett. A* **34**(34), 1950281 (2019).
56. Tsai, C.-W. & Yang, C.-W. Lightweight mediated semi-quantum key distribution protocol with a dishonest third party based on Bell states. *Sci. Rep.* **11**(1), 23222 (2021).
57. Tsai, C.-W. & Yang, C.-W. Lightweight authenticated semi-quantum key distribution protocol without trojan horse attack. *Laser Phys. Lett.* **17**(7), 075202 (2020).
58. 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).
59. 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).
60. Meslouhi, A. & Hassouni, Y. Cryptanalysis on authenticated semi-quantum key distribution protocol using Bell states. *Quantum Inf. Process.* **16**(1), 18 (2016).
61. Zebboudj, S., Djoudi, H., Lalaoui, D. & Omar, M. Authenticated semi-quantum key distribution without entanglement. *Quantum Inf. Process.* **19**(3), 77 (2020).
62. Chang, C.-H., Lu, Y.-C. & Hwang, T. Measure-resend authenticated semi-quantum key distribution with single photons. *Quantum Inf. Process.* **20**(8), 272 (2021).
63. 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* **10**(8), 1241 (2022).
64. Deng, F. G., Zhou, P., Li, X. H., Li, C. Y., Zhou, H. Y.: Robustness of two-way quantum communication protocols against trojan horse attack. https://arxiv.org/abs/quant-ph/0508168. (2005) arXiv:quant-ph/0508168v1.
65. Cai, Q. Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. *Phys. Lett. A* **351**(1–2), 23–25 (2006).
66. Yang, Y.-G., Sun, S.-J. & Zhao, Q.-Q. Trojan-horse attacks on quantum key distribution with classical Bob. *Quantum Inf. Process.* **14**(2), 681–686 (2015).
67. Deng, F. G., Li, X. H., Zhou, H. Y. & Zhang, Z. J. Improving the security of multiparty quantum secret sharing against Trojan horse attack. *Phys. Rev. A* **72**(4), 044302 (2005).
68. Li, X. H., Deng, F. G. & Zhou, H. Y. Improving the security of secure direct communication based on the secret transmitting order of particles. *Phys. Rev. A* **74**(5), 054302 (2006).
69. Bennett, C. H., Brassard, G., Crepeau, C. & Maurer, U. M. Generalized privacy amplification. *IEEE Trans. Inf. Theory* **41**(6), 1915–1923 (1995).
70. Biham, E., Boyer, M., Brassard, G., Van de Graaf, J. & Mor, T. Security of quantum key distribution against all collective attacks. *Algorithmica* **34**(4), 372–388 (2002).
71. Scarani, V. *et al.* The security of practical quantum key distribution. *Rev Mod Phys* **81**(3), 1301–1350 (2009).

72. Boyer, M., Gelles, R. & Mor, T. Attacks on fixed-apparatus quantum-key-distribution schemes. *Phys. Rev. A* **90**(1), 012329 (2014).
73. Boyer, M., Katz, M., Liss, R. & Mor, T. Experimentally feasible protocol for semiquantum key distribution. *Phys. Rev. A* **96**(6), 062335 (2017).
74. Boyer, M., Liss, R. & Mor, T. Attacks against a simplified experimentally feasible semiquantum key distribution protocol. *Entropy* **20**(7), 536 (2018).
75. 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* **801**, 96–109 (2020).
76. Yang, C.-W. & Hwang, T. Improved QSDC protocol over a collective-dephasing noise channel. *Int. J. Theor. Phys.* **51**(12), 3941–3950 (2012).
77. Yang, C.-W. & Hwang, T. Quantum dialogue protocols immune to collective noise. *Quantum Inf. Process.* **12**(6), 2131–2142 (2013).
78. Yang, C.-W., Hwang, T. & Luo, Y.-P. Enhancement on "Quantum blind signature based on two-state vector formalism". *Quantum Inf. Process.* **12**(1), 109–117 (2013).

Acknowledgements

This research was partially supported by the National Science and Technology Council, Taiwan, R.O.C. (Grant no. NSTC 111-2221-E-039-014), and China Medical University, Taiwan (Grant no. CMU110-MF-121).

Author contributions

Conceptualization, C.-W.Y.; methodology, C.-W.Y.; investigation, C.-W.Y.; formal analysis, C.-W.Y.; writing—original draft, C.-W.Y.; writing—review & editing, C.-W.Y.; project Administration, C.-W.Y. All authors have read and agreed to the published version of the manuscript.

Competing interests

The author declares no competing interests.

Additional information

Correspondence and requests for materials should be addressed to C.-W.Y.

Reprints and permissions information is available at www.nature.com/reprints.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.