Ye et al. *EPJ Quantum Technology* (2023) 10:21
https://doi.org/10.1140/epjqt/s40507-023-00180-3

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

Security and application of semi-quantum key distribution protocol for users with different quantum capabilities

Chong-Qiang Ye[1], Jian Li[2*], Xiu-Bo Chen[2], Yanyan Hou[3] and Zhuo Wang[1]

*Correspondence:
lijian@bupt.edu.cn
[2]Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, 100876, Beijing, China
Full list of author information is available at the end of the article

Abstract

Semi-quantum protocols serve as a bridge between quantum users and "classical" users with limited quantum capabilities, providing support for application scenarios that cannot afford the excessively high cost of quantum resources. In this paper, we present a semi-quantum key distribution (SQKD) protocol based on Bell states and single particles, which is designed for key distribution between different types of users. The protocol enables simultaneous key distribution between quantum and classical users, as well as key establishment between two classical users. The security analysis demonstrates that the protocol can reach the same level of security as the full quantum protocol. Furthermore, we extrapolate the proposed protocol to other semi-quantum protocols, such as semi-quantum key agreement and semi-quantum private comparison protocols. Compared with previous similar ones, our SQKD protocol and its extended versions can fulfill the requirements of their respective counterparts individually. Therefore, our SQKD protocol has the potential for broader applications in practical scenarios.

Keywords: Quantum communication; Semi-quantum key distribution; Different users; Security; Key rate

1 Introduction

Quantum communication [1–3] has experienced significant advancements in recent decades due to its security based on quantum laws rather than computational complexity. Using quantum resources to solve problems in classical communication has become a research hotspot. Quantum key distribution (QKD), a critical branch of quantum communication, is aimed at enabling two quantum users to securely share a secret key, even in the presence of an all-powerful adversary, commonly referred to as Eve. For further investigation on this topic, the reader is referred to the literature cited in references [4–6].

Traditionally, QKD requires all users to possess full quantum capabilities to ensure the security of the protocol. However, given the current technological limitations, not all users may be able to afford the high costs associated with quantum devices. This raises the question of how many quantum resources are necessary to achieve unconditional security, or

whether all users in a communication scheme need to have the ability to generate and measure arbitrary quantum states.

Fortunately, Boyer et al. provided an answer to this question by proposing a semi-quantum key distribution (SQKD) scheme that reduces the quantum capability of one party compared to QKD [7, 8]. In the SQKD protocol, one user, referred to as the "quantum" user, possesses full quantum power, while the other user, known as the "classical" or "semi-quantum" user, has limited quantum capabilities. The classical user is typically only capable of preparing and measuring quantum states in the computational base $\{|0\rangle, |1\rangle\}$, performing direct reflection, and reordering operations. As our society moves towards practical implementation of quantum communication networks, semi-quantum models may offer advantages such as potentially reducing the cost of devices (since fewer "quantum-capable" hardware may be required) or increasing the robustness of devices against hardware failures (by switching to the semi-quantum operation mode in case of device failures). Semi-quantum protocols provide an effective way to reduce the dependence of users on quantum resources, making SQKD an active area of research [9–12]. For example, in 2015, Krawec [9] demonstrated the unconditional security of SQKD protocol and derived the protocol's key rate. Later, Zhang et al. [10] gave a security analysis of single-state based SQKD protocol. By utilizing the error-matching measurement technique, the protocol's noise tolerance [11] can be improved at the expense of efficiency. In addition, other types of semi-quantum cryptography protocols were also investigated, such as semi-quantum secure communication [13–15], semi-quantum secret sharing [16, 17], and semi-quantum private comparison [18–22]. For a comprehensive survey of the literature, the reader is referred to reference [23].

Mediated semi-quantum key distribution (M-SQKD) is a special kind of semi-quantum protocol, which was initially introduced by Krawec [24] in 2015. M-SQKD enables two "classical" users (Alice and Bob) to generate a secure key with the help of a third party (TP), whereas in regular SQKD, the key is shared between quantum and "classical" users. Since its introduction, several M-SQKD protocols have been proposed with various quantum states and transport structures [25–30]. In Ref. [25], Krawec improved the key rate of the original M-SQKD protocol by using an alternative method of proof. After that, Liu et al. [26] presented a new M-SQKD protocol based on entanglement swapping, where the "classical" users do not require quantum measurement capability. Lin et al. [27] presented an M-SQKD protocol with single photons instead of entangled ones to reduce the necessary quantum resources. Recently, Chen et al. [28] designed an M-SQKD protocol using single-particle states. Unlike the previous protocols, this protocol adopts the mode of circular transmission. Guskind et al. [29] improved the M-SQKD protocol's efficiency without requiring users' additional capabilities. Besides, Krawec proposed a multi-party M-SQKD protocol that involves two or more adversarial quantum servers assisting two "classical" users in establishing a secret key [30]. In 2023, Ye et al. [31] implemented the M-SQKD protocol using Bell states and circular transmission, enabling more than two "classical" users to establish a secret key. In addition, there are some variants of the M-SQKD protocol that require attention. Notably, Tsai and Yang [32, 33] introduced two modified versions of the M-SQKD protocol, in which classical users possess the capability of performing lightweight unitary operations. These protocol variations aim to eliminate the need for bidirectional transmission by empowering classical users with enhanced abil-

ities. In this way the impact of Trojan horse attacks on the semi-quantum protocol can be avoided.

In the description above, SQKD realizes the key distribution between the quantum user and classical user, while M-SQKD achieves the key sharing between classical users. SQKD and M-SQKD play a crucial role in semi-quantum communication protocols, especially in multi-party scenarios. Many semi-quantum protocols, such as semi-quantum identification [34] and semi-quantum secure multi-party computation [35, 36], have to rely on them to guarantee the security of the protocol. However, executing SQKD and M-SQKD separately for establishing key relationships between different users can reduce the protocol's efficiency. Currently, there is no known semi-quantum protocol that can achieve simultaneous key distribution among different users.

To address this limitation, in this paper, we present a novel SQKD protocol that utilizes Bell states and single-particle states to establish key distribution between quantum and classical users, as well as between two classical users. This approach effectively reduces the complexity and cost of the secret key distribution process between different users. For the protocol's security, we prove that it is information-theoretically secure under different scenarios. The results show that our protocol may hold similar security to a fully quantum one. Furthermore, we generalize the proposed SQKD protocol to other semi-quantum cryptography protocols, such as the semi-quantum private comparison (SQPC) and semi-quantum key agreement (SQKA), showcasing its versatility and potential for practical applications in other semi-quantum scenarios. In summary, our work provides a promising solution for secure key distribution between different users in semi-quantum environments, and it can be generalized to other types of semi-quantum application scenarios.

The remaining organization of the paper is outlined as follows. Section 2 describes the detailed steps of the proposed SQKD protocol. In Sect. 3, the security of the proposed protocol is analyzed under different conditions, establishing its information-theoretic security. In Sect. 4, the generalization of the SQKD protocol to other semi-quantum protocols, including SQPC and SQKA protocols, is presented. Then, in Sect. 5, we compare the proposed protocols with their respective counterparts separately. Finally, this paper concludes in Sect. 6.

2 The proposed SQKD protocol

There are three users in our protocol, the quantum user TP who has full quantum capability, and the classical users Alice and Bob, whose abilities are limited. The classical users are limited to the following operations: (1) measure: measure the qubit in Z basis $\{|0\rangle, |1\rangle\}$ and regenerate one in the same state (e.g., $|0\rangle \rightarrow |0\rangle, |1\rangle \rightarrow |1\rangle$). (2) reflect: reflect the qubit directly. Note that the reordering operation is not required in this paper, and the classical user only needs to perform the measure or reflect operation.

Next, we introduce the classical channels used in the protocol. In standard practice, the classical channels used in quantum protocols require authentication, so Eve can only access the publicly available classical information and cannot change it [37, 38]. Consequently, all classical channels involved in this protocol, including those used in classical post-processing, adhere to the requirement of authentication.

The detailed protocol steps are as follows (Note that the security for different users will be discussed later in the security analysis).

Step 1: TP prepares $4N$ Bell states all in the state of $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)_{AB}$, and divides them into two sequences:

$$S_A : P_A^1, P_A^2, \ldots, P_A^{4N}, \qquad S_B : P_B^1, P_B^2, \ldots, P_B^{4N}. \tag{1}$$

Then, TP prepares the other two sequences:

$$T_A : P_{TA}^1, P_{TA}^2, \ldots, P_{TA}^{4N}, \qquad T_B : P_{TB}^1, P_{TB}^2, \ldots, P_{TB}^{4N}, \tag{2}$$

where each qubit is randomly from the set $\{|0\rangle, |1\rangle\}$.

Step 2: TP randomly inserts T_A (T_B) into S_A (S_B) to form a new sequence S_A^* (S_B^*). Subsequently, S_A^* and S_B^* will be sent to Alice and Bob, separately.

Step 3: For the arriving qubits, Alice (Bob) randomly chooses the measure or reflect operation. Alice (Bob) will record the measurement result, if she (he) chooses the measure operation.

Step 4: TP receives all the qubits and then divides the qubits of T_A (T_B) from qubits of S_A (S_B) and performs different measurements. In more detail, TP measures the qubits of T_A and T_B in the Z basis, while for qubits of S_A and S_B (i.e., P_A^i and P_B^i, $i \in \{1, 2, \ldots, 4N\}$) she will perform Bell measurements. After that, TP announces her measurement results of S_A and S_B and the positions of these qubits. Note that the measurement results of T_A and T_B are kept in her hands and not leaked to Alice and Bob (They will be discussed later).

Step 5: Alice and Bob discuss eavesdropping and TP's honesty. Depending on Alice and Bob's operations and the information provided by TP, the following three cases will happen (It is expected that there are N qubits in Case 1.):

- *Case 1*: When Alice and Bob choose the measure operation on the qubits P_A^i and P_B^i, they will obtain the same measurement result, and TP will publish the result as either $|\phi^+\rangle$ or $|\phi^-\rangle$. Moreover, TP knows nothing about Alice and Bob's measurements because she performs Bell measurements, not Z-basis measurements, on the qubits P_A^i and P_B^i. Thus, Alice and Bob can establish a raw secret key sequence denoted as $K_{AB} = [k_{AB}^1, k_{AB}^2, \ldots, k_{AB}^N]$.
- *Case 2*: When they choose the reflect operation on the qubits P_A^i and P_B^i, TP should always publish $|\phi^+\rangle$. This case is used for checking the honesty of TP and eavesdropping. If error rate surpasses the threshold, the protocol ends.
- *Case 3*: If they perform different operations, this case will be discarded.

Step 6: After the eavesdrop check, Alice and Bob will discuss the operations performed on the sequence T_A (T_B) with TP. They first tell TP their operations on the qubits of T_A and T_B. Note that in the sequence T_A (T_B), there are $2N$ qubits performed the measure operation and $2N$ qubits performed the reflect operation. As a result, three scenarios need to be considered:

- (1) For the qubits performed the reflect operation, TP compares these qubits' initial states and measurement results recorded in step 4. If the error rate is over high, the protocol terminates and restarts.
- (2) For the qubits performed the measure operation (i.e., $2N$ qubits), Alice (Bob) first picks out N qubits and announces the measurement results to TP. Then, TP compares these announcements and her measurement results recorded in step 4. If there is no Eve online, Alice's (Bob's) measurements, TP's measurements, and the initial state of these qubits, all three are the same. These qubits are used for eavesdropping checking.

- (3) For the remaining N qubits that have been performed the measure operation, Alice's (Bob's) measurement results are the same as TP's. Thus, Alice (Bob) and TP can establish a raw secret key sequence. At the same time, Bob (Alice) knows nothing about them. We use $K_{TA} = [k_{TA}^1, k_{TA}^2, \ldots, k_{TA}^N]$ ($K_{TB} = [k_{TB}^1, k_{TB}^2, \ldots, k_{TB}^N]$) to represent the secret key between Alice and TP (Bob and TP).

Step 7: After classical post-processing, different users can obtain the final security key, i.e., TP, Alice, and Bob can respectively establish security keys among themselves.

3 Security analysis

In the above section, we gave the specific steps of the SQKD protocol. Here, we would like to investigate the security of the key distribution between different users. According to [39], security against collective attacks is enough to demonstrate security against arbitrary general attacks. Thereby, we focus on proving security against collective attacks.

3.1 Security of key distribution between the quantum and classical users

In this case, TP is trusted and she wants to establish secure keys with classical users. Alice and Bob play the same role in our protocol, either of whom can establish a secret key with TP. Without loss of generality, we analyze the security of the key distribution between TP and Alice. For the sake of description, both external and internal eavesdroppers will be referred to as Eve. Under collective attacks, the system of TP, Alice, and Eve can be described as

$$\rho'_{TAE} = \sum_{i,j} |i,j\rangle\langle i,j|_{TA} \otimes \rho_E, \tag{3}$$

where ρ_E denotes the state of Eve's ancilla. Let N denote the size of TP and Alice's raw key, $\ell(n)$ denote the length of secure key. Based on [4], our protocol's key rate in the asymptotic scenario is

$$r = \lim_{N\to\infty} \frac{\ell(N)}{N} = \inf\big[S(T|E) - H(T|A)\big], \tag{4}$$

where $S(\cdot)$ denotes the Von Neumann entropy, and $H(\cdot)$ means the Shannon entropy. If $r > 0$, the protocol can obtain a secure secret key. Hence, the goal of the next stage is to analyze Eve's attack strategy and compute the key rate r.

3.1.1 The attack strategy of Eve

Since the semi-quantum protocol is a two-way protocol, the collective attacks can be modeled as two unitaries U_E and U_F (also see Fig. 1). Here, U_E is the attack operator applied on the qubits sent from TP to Alice while U_F is the attack operator applied on the qubits sent from Alice to TP. Note that U_E and U_F have a common probe space with an initial state of $|0\rangle_E$. In this kind of attack, Eve may perform (U_E, U_F) on the target qubit and her probe $|0\rangle_E$ to extract some useful information. According to [9], the effects of U_E and U_F can be described as

$$\begin{aligned} U_E|0,0\rangle_{tE} &= |0,E_0\rangle + |1,E_1\rangle, \\ U_E|1,0\rangle_{tE} &= |0,E_2\rangle + |1,E_3\rangle, \\ U_F|i,E_k\rangle_{tE} &= |0,E_{i,k}^0\rangle + |1,E_{i,k}^1\rangle, \end{aligned} \tag{5}$$

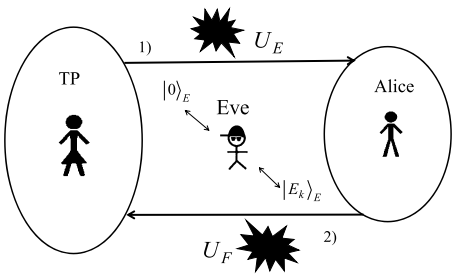

Figure 1 A schematic of Eve's attack. Eve will launch U_E and U_F on the qubits from TP and Alice, respectively, to obtain some helpful information

where t and E represent the target qubit and Eve's probe, respectively. E_k is determined by (U_E, U_F) and $i \in \{0,1\}$, $k \in \{0,1,2,3\}$.

As described in the protocol, the raw key of TP and Alice, K_{TA}, generates in the event that Alice and TP measure the qubits of T_A. After Eve's attack, the system changed as follows.

(1) Eve first launches U_E on the qubit from TP to Alice and her probe $|0\rangle_E$. After that, the density operator describing the system of TP and Eve is

$$\begin{aligned}\rho_1 = {} & \frac{1}{2}|0\rangle\langle 0|_T \otimes \left(|0,E_0\rangle\langle 0,E_0|_{A'E} + |1,E_1\rangle\langle 1,E_1|_{A'E}\right) \\ & + \frac{1}{2}|1\rangle\langle 1|_T \otimes \left(|0,E_2\rangle\langle 0,E_2|_{A'E} + |1,E_3\rangle\langle 1,E_3|_{A'E}\right),\end{aligned} \tag{6}$$

where T denotes the qubit sent by TP, A' represents the qubit after Eve's attack and will be received by Alice.

(2) Alice measures the received qubit and resends a new qubit in the same state to TP. Then, Eve will launch U_F on the qubit from Alice to TP and $|E_k\rangle_E$. After Eve's attack and TP's measurement, the system becomes

$$\begin{aligned}\rho_2 = {} & \frac{1}{2}|0,i,j\rangle\langle 0,i,j|_{TAT'} \otimes \left|E^j_{i,i}\right\rangle\left\langle E^j_{i,i}\right|_E \\ & + \frac{1}{2}|1,i,j\rangle\langle 1,i,j|_{TAT'} \otimes \left|E^j_{i,i+2}\right\rangle\left\langle E^j_{i,i+2}\right|_E,\end{aligned} \tag{7}$$

where A and T' denote Alice's and TP's measurement results, respectively. From (7), it not hard to see that Eve may obtain some secret keys of Alice and TP from her probe.

3.1.2 Key rate derivation

Let $p_{x,i,j}$ represent the probability that the qubit sent by TP is $|x\rangle$, Alice's observation is $|i\rangle$, and TP's measurement result is $|j\rangle$. According to (7), $p_{x,i,j}$ can be estimated as follows.

$$p_{0,i,j} = \left\langle E^j_{i,i}|E^j_{i,i}\right\rangle, \qquad p_{1,i,j} = \left\langle E^j_{i,i+2}|E^j_{i,i+2}\right\rangle. \tag{8}$$

Note that TP and Alice can easily calculate the value of $p_{x,i,j}$. Following the protocol steps, TP accepts the event that the state of the qubit being measured is the same as its initial state (i.e., $x = j$). Thereby, the final generated raw key system becomes

$$\rho_{TAE} = \frac{1}{C}\left(|0,i\rangle\langle 0,i|_{TA} \otimes \left|E^0_{i,i}\right\rangle\left\langle E^0_{i,i}\right|_E + |1,i\rangle\langle 1,i|_{TA} \otimes \left|E^1_{i,i+2}\right\rangle\langle E^1_{i,i+2}|_E\right), \tag{9}$$

where C is the normalization coefficient and $C = \sum_{i=0}^{1}\langle E^0_{i,i}|E^0_{i,i}\rangle + \langle E^1_{i,i+2}|E^1_{i,i+2}\rangle$.

We have now modeled Eve's attack and obtained the density matrix of the collective system. Next, we will derive the protocol's key rate, i.e., $r = S(T|E) - H(T|A)$. Obviously, calculating $H(T|A)$ is simple, so let's start with this part of the calculation.

Let $p_{i,j}$ mean the probability that Alice's raw key is $|i\rangle$ and TP's raw key is $|j\rangle$. Observing (9), we have

$$\begin{aligned} p_{0,0} &= \frac{1}{C}\langle E^0_{0,0}|E^0_{0,0}\rangle, \qquad p_{0,1} = \frac{1}{C}\langle E^1_{0,2}|E^1_{0,2}\rangle, \\ p_{1,0} &= \frac{1}{C}\langle E^0_{1,1}|E^0_{1,1}\rangle, \qquad p_{1,1} = \frac{1}{C}\langle E^1_{1,3}|E^1_{1,3}\rangle. \end{aligned} \tag{10}$$

Thereby, it's easy to obtain $H(T,A) = H(p_{0,0}, p_{0,1}, p_{1,0}, p_{1,1})$. Observing the system of Alice, the probability that Alice obtains $|0\rangle$ is $p_{0,0} + p_{0,1}$, so that we have $H(A) = H(p_{0,0} + p_{0,1}, p_{1,0} + p_{1,1})$. Following this fact, we can calculate:

$$H(T|A) = H(T,A) - H(A). \tag{11}$$

What remains to be calculated is $S(T|E)$. Tracing out A from ρ_{TAE} yields:

$$\begin{aligned} \rho_{TE} = &\frac{1}{C}|0\rangle\langle 0|_T \otimes \left(\left|E^0_{0,0}\right\rangle\left\langle E^0_{0,0}\right|_E + \left|E^0_{1,1}\right\rangle\left\langle E^0_{1,1}\right|_E\right) \\ &+ \frac{1}{C}|1\rangle\langle 1|_T \otimes \left(\left|E^1_{0,2}\right\rangle\left\langle E^1_{0,2}\right|_E + \left|E^1_{1,3}\right\rangle\left\langle E^1_{1,3}\right|_E\right). \end{aligned} \tag{12}$$

According to the theorem from [11]:

Theorem 1 *Given a quantum state ρ'_{TE} of the form*:

$$\rho'_{TE} = \frac{1}{N}\left(|0\rangle\langle 0|_T \otimes \sum_{i=0}^{m}|e_i\rangle\langle e_i| + |1\rangle\langle 1|_T \otimes \sum_{i=0}^{m}|f_i\rangle\langle f_i|\right), \tag{13}$$

where $N > 0$ is a normalization term. Then, we have:

$$S(T|E)_{\rho'} \geq \sum_{i=0}^{m}\left(\frac{\langle e_i|e_i\rangle + \langle f_i|f_i\rangle}{C}\right) \times \left(h\left(\frac{\langle e_i|e_i\rangle}{\langle e_i|e_i\rangle + \langle f_i|f_i\rangle}\right) - h(\lambda_i)\right), \tag{14}$$

$$\lambda_i = \frac{1}{2} + \frac{\sqrt{(\langle e_i|e_i\rangle - \langle f_i|f_i\rangle)^2 + 4\,\mathrm{Re}^2\langle e_i|f_i\rangle}}{2(\langle e_i|e_i\rangle + \langle f_i|f_i\rangle)}, \tag{15}$$

and $h(x) = -x\log_2 x - (1-x)\log_2(1-x)$.

For the detailed proof process, the reader is referred to [11]. Applying Theorem 1 to (12), we can derive the result:

$$S(T|E) \geq \sum_{i=0}^{1}\frac{\langle \gamma_i|\gamma_i\rangle + \langle \eta_i|\eta_i\rangle}{C} \times \left(h\left(\frac{\langle \gamma_i|\gamma_i\rangle}{\langle \gamma_i|\gamma_i\rangle + \langle \eta_i|\eta_i\rangle)}\right) - h(\lambda_i)\right), \tag{16}$$

$$\lambda_i = \frac{1}{2} + \frac{\sqrt{(\langle \gamma_i|\gamma_i\rangle - \langle \eta_i|\eta_i\rangle)^2 + 4\,\mathrm{Re}^2\langle \gamma_i|\eta_i\rangle}}{2(\langle \gamma_i|\gamma_i\rangle + \langle \eta_i|\eta_i\rangle)}, \tag{17}$$

where

$$\gamma_0 = E^0_{0,0}, \qquad \gamma_1 = E^0_{1,1}, \qquad \eta_0 = E^1_{1,3}, \qquad \eta_1 = E^1_{0,2}. \tag{18}$$

From (16) and (17), it's easy to find that $S(A|T)$ depends on the parameters $\langle\gamma_i|\gamma_i\rangle$, $\langle\eta_i|\eta_i\rangle$, and $\mathrm{Re}\langle\gamma_i|\eta_i\rangle$. According to (8) and (18), the values of $\langle\gamma_i|\gamma_i\rangle$ and $\langle\eta_i|\eta_i\rangle$ can be obtained. Thereby, we need to bound $\mathrm{Re}\langle\gamma_i|\eta_i\rangle$, i.e., $\mathrm{Re}\langle E^0_{0,0}|E^1_{1,3}\rangle$ and $\mathrm{Re}\langle E^0_{1,1}|E^1_{0,2}\rangle$.

In the above analysis, we only focus on the case where the qubits come from the sequence T_A and are measured by Alice. Now let's turn our attention to the case where the qubits come from $|\phi^+\rangle$ and are directly reflected by Alice and Bob. It may provide a way to calculate $\mathrm{Re}\langle\gamma_i|\eta_i\rangle$. Specifically, after Eve's attacks, the Bell state $|\phi^+\rangle$ becomes

$$\begin{aligned} U_F U_E|\phi^+\rangle|0\rangle_E = \frac{1}{2}\big[&|\phi^+\rangle\big(|F_0\rangle + |F_3\rangle\big) + |\phi^-\rangle\big(|F_0\rangle - |F_3\rangle\big) \\ &+ |\psi^-\rangle\big(|F_1\rangle - |F_2\rangle\big) + |\psi^+\rangle\big(|F_1\rangle + |F_2\rangle\big)\big], \end{aligned} \tag{19}$$

where

$$\begin{aligned} |F_0\rangle &= |E^0_{0,0}\rangle + |E^0_{1,1}\rangle, \qquad |F_1\rangle = |E^1_{0,0}\rangle + |E^1_{1,1}\rangle, \\ |F_2\rangle &= |E^0_{0,2}\rangle + |E^0_{1,3}\rangle, \qquad |F_3\rangle = |E^1_{0,2}\rangle + |E^1_{1,3}\rangle. \end{aligned} \tag{20}$$

Then, TP measures the qubits with Bell basis and announces her measurements. If the measurement is not $|\phi^+\rangle$, Alice knows there is an error raised. Here, we use p_{ψ^-}, p_{ψ^+}, and p_{ϕ^-} to represent the probabilities that TP's outcomes are $|\psi^-\rangle$, $|\psi^+\rangle$, and $|\phi^-\rangle$, respectively. According to (19), it's easy to get

$$\begin{aligned} p_{\psi^-} &= \frac{1}{4}\langle F_1|F_1\rangle - \frac{1}{2}\mathrm{Re}\langle F_1|F_2\rangle + \frac{1}{4}\langle F_2|F_2\rangle, \\ p_{\psi^+} &= \frac{1}{4}\langle F_1|F_1\rangle + \frac{1}{2}\mathrm{Re}\langle F_1|F_2\rangle + \frac{1}{4}\langle F_2|F_2\rangle, \\ p_{\phi^-} &= \frac{1}{4}\langle F_0|F_0\rangle - \frac{1}{2}\mathrm{Re}\langle F_0|F_3\rangle + \frac{1}{4}\langle F_3|F_3\rangle. \end{aligned} \tag{21}$$

Note that U_E and U_F are unitary, which mean that $\langle F_0|F_0\rangle + \langle F_1|F_1\rangle = \langle F_2|F_2\rangle + \langle F_3|F_3\rangle = 1$. After some algebra, we have

$$p_{\psi^+} + p_{\psi^-} + p_{\phi^-} = 1 - \frac{1}{2}\mathrm{Re}\langle F_0|F_3\rangle - \frac{1}{4}\langle F_0|F_0\rangle - \frac{1}{4}\langle F_3|F_3\rangle. \tag{22}$$

Using (20) into (22), thus

$$\begin{aligned} &\mathrm{Re}\big\langle E^0_{0,0}|E^1_{1,3}\big\rangle + \mathrm{Re}\big\langle E^0_{1,1}|E^1_{0,2}\big\rangle \\ &\quad = 2 - 2(p_{\psi^+} + p_{\phi^-} + p_{\psi^-}) - \mathrm{Re}\big(\big\langle E^0_{0,0}|E^1_{0,2}\big\rangle + \big\langle E^0_{1,1}|E^1_{1,3}\big\rangle\big) \\ &\qquad - \frac{1}{2}\mathrm{Re}\big(\big\langle E^0_{0,0}|E^0_{0,0}\big\rangle + \big\langle E^0_{1,1}|E^0_{0,0}\big\rangle + \big\langle E^0_{0,0}|E^0_{1,1}\big\rangle + \big\langle E^0_{1,1}|E^0_{1,1}\big\rangle\big) \\ &\qquad - \frac{1}{2}\mathrm{Re}\big(\big\langle E^1_{0,2}|E^1_{0,2}\big\rangle + \big\langle E^1_{1,3}|E^1_{0,2}\big\rangle + \big\langle E^1_{0,2}|E^1_{1,3}\big\rangle + \big\langle E^1_{1,3}|E^1_{1,3}\big\rangle\big). \end{aligned} \tag{23}$$

Then, according to the Cauchy–Schwarz inequality (i.e., $|\mathrm{Re}\langle a|b\rangle| \leq |\langle a|b\rangle| \leq \sqrt{\langle a|a\rangle\langle b|b\rangle}$) and (8), the ranges of $\mathrm{Re}\langle E^0_{0,0}|E^1_{1,3}\rangle$ and $\mathrm{Re}\langle E^0_{1,1}|E^1_{0,2}\rangle$ can be obtained. It is important to point out that the value of $\mathrm{Re}\langle E^0_{1,1}|E^1_{0,2}\rangle$ is generally low, because $\mathrm{Re}\langle E^0_{1,1}|E^1_{0,2}\rangle \leq \sqrt{p_{0,1,0}p_{1,0,1}}$, and $p_{0,1,0}$, $p_{1,0,1}$ represent the probability that TP and Alice measurements do not match, which is very small in the protocol, otherwise the protocol would be terminated due to the high error rate.

Therefore, we concentrate on minimizing the value of $\mathrm{Re}\langle E^0_{0,0}|E^1_{1,3}\rangle$. Let $\mathrm{Re}\langle E^0_{1,1}|E^1_{0,2}\rangle = \sqrt{p_{0,1,0}p_{1,0,1}}$, we have

$$\begin{aligned}\mathrm{Re}\left\langle E^0_{0,0}|E^1_{1,3}\right\rangle \geq\ & 2 - 2(p_{\psi^+} + p_{\phi^-} + p_{\psi^-}) \\ & - (\sqrt{p_{1,0,1}p_{0,0,0}} + \sqrt{p_{0,1,0}p_{1,1,1}} + \sqrt{p_{0,1,0}p_{1,0,1}}) \\ & - \frac{1}{2}(p_{0,0,0} + \sqrt{p_{0,1,0}p_{0,0,0}} + \sqrt{p_{0,0,0}p_{0,1,0}} + p_{0,1,0}) \\ & - \frac{1}{2}(p_{1,0,1} + \sqrt{p_{1,1,1}p_{1,0,1}} + \sqrt{p_{1,0,1}p_{1,1,1}} + p_{1,1,1}).\end{aligned} \tag{24}$$

The parameters in (24) can all be easily obtained by making observations of the channel. Then, following the values of $\mathrm{Re}\langle E^0_{0,0}|E^1_{1,3}\rangle$ and $\mathrm{Re}\langle E^0_{1,1}|E^1_{0,2}\rangle$ we can calculate (15), which in turn gives the value of $S(T|E)$. So far, we have derived the bounds of $H(T|A)$ and $S(T|E)$, thus, the protocol's key rate can be derived.

3.1.3 Key rate evaluation

In this part, we parameterize the errors introduced by Eve's attack to estimate the key rate of the protocol. The following are typical parametric assumptions [9, 11]:

1. The quantum channels of TP to Alice and Alice to TP are the depolarization channel with parameter q:

$$\varepsilon_q(\rho) = (1-q)\rho + \frac{q}{2}I. \tag{25}$$

   Moreover, the quantum channels are independent of each other.
2. Let Q represent the probability that TP (Alice) sents single particle $|i\rangle$ while Alice (TP) observes $|1-i\rangle$.
3. Let Q_R represent the probability that TP announces the wrong result when Alice and Bob reflect the qubits of Bell states. That is, $p_{\psi^+} + p_{\psi^-} + p_{\phi^-} = Q_R$.

Single particles and Bell states will produce different results through depolarization channels. Through simple calculation, it's not difficult to get: $Q = q/2$ and $Q_R = q(1-q/2) = 2Q(1-Q)$. Note that Q can be easily observed in this protocol. Furthermore (8) can be represented by Q as follows

$$\begin{aligned} &p_{0,0,0} = p_{1,1,1} = (1-Q)^2, \qquad p_{1,0,1} = p_{0,1,0} = Q^2, \\ &p_{1,1,0} = p_{0,0,1} = Q(1-Q), \qquad p_{0,1,1} = p_{1,0,0} = (1-Q)Q. \end{aligned} \tag{26}$$

Then (10) can be rewritten as

$$p_{0,0} = p_{1,1} = \frac{1}{C}(1-Q)^2, \qquad p_{0,1} = p_{1,0} = \frac{1}{C}Q(1-Q), \tag{27}$$

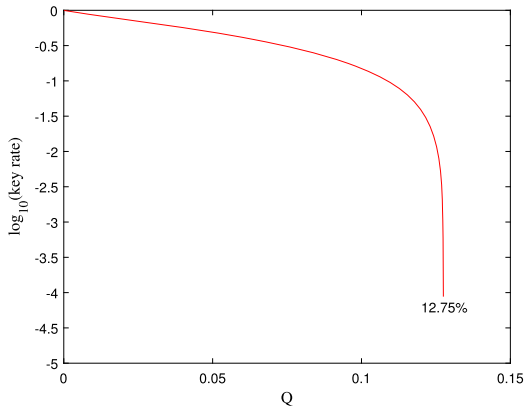

Figure 2 A diagram of the key rate between quantum and classical users

where $C = 2(1-Q)^2 + 2(1-Q)Q$. For $\mathrm{Re}\langle E^0_{0,0}|E^1_{1,3}\rangle$ and $\mathrm{Re}\langle E^0_{1,1}|E^1_{0,2}\rangle$, applying (26) into (24), we have

$$\begin{aligned} &\mathrm{Re}\langle E^0_{0,0}|E^1_{1,3}\rangle \geq 2 - 2Q_R - 4(1-Q)Q - 2Q^2 - (1-Q)^2, \\ &\mathrm{Re}\langle E^0_{1,1}|E^1_{0,2}\rangle = Q^2. \end{aligned} \tag{28}$$

Finally, the bounds of $H(T|A)$ and $S(T|E)$ are all denoted by Q. Thus, put it all together into the (4), the key rate r can be estimated by the variable Q. The relationship between r and Q is shown in Fig. 2. As long as $Q \leq 12.75\%$, we have $r > 0$, that is, a secure key can be obtained by Alice and TP.

3.2 Security of key distribution between two classical users

In the proposed protocol, all quantum resources and complex quantum state measurements can only be accomplished by TP. If TP is adversarial, she will bring the greatest threat to classical users because she can take all possible attacks to steal helpful information, including preparing fake quantum states. Here we consider the worst scenario, where TP is adversarial and wants to steal the secrets of Alice and Bob. Besides, we do not separate natural noise and adversarial noise and briefly hypothesize that all errors are caused by TP's attacks [29].

3.2.1 The attack strategy of TP

TP is adversarial, so she unnecessarily follows the protocol description to prepare Bell state, but instead any arbitrary state $|\Phi\rangle = \sum_{i,j=0}^{1} \zeta_{i,j}|i,j\rangle$. Moreover, TP is allowed to perform any quantum operation, she may entangle her private ancilla with the target qubits. However, according to the protocol steps, she must announce the same message to Alice and Bob in the form of a Bell state, which serves as the basis for Alice and Bob to generate the key.

Following the security proof in [29], TP's attack can be modeled as an isometry operator U (also see Fig. 3). In more detail, the effect of U is mapping the target qubits from Alice and Bob to TP's ancilla and a message state $|m\rangle$:

$$U|i,j\rangle = \sum_{m=0}^{3} |m, f^m_{i,j}\rangle, \tag{29}$$

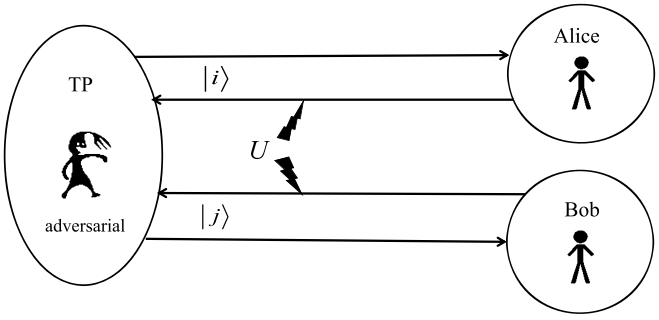

Figure 3 Schematic diagram of TP's attack. Here, TP is adversarial and she may launch U on the qubits from Alice and Bob to obtain helpful information

where $|f_{i,j}^m\rangle$ is arbitrary, not necessarily normalized, belongs to TP's ancilla. Note that $m = 0, 1, 2, 3$ represent that TP publishes messages $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$, respectively.

We first consider the case where Alice and Bob both measure and resend the received qubit. TP first sends the qubits of $|\Phi\rangle = \sum_{i,j=0}^{1} \zeta_{i,j}|i,j\rangle$ to Alice and Bob, respectively. Let $q_{i,j}$ denote the probability that Alice and Bob's observation is $|i,j\rangle$. Then, we have

$$q_{i,j} = \zeta_{i,j}^2. \tag{30}$$

After that, TP performs U on the qubits from Alice and Bob, the system will become

$$\rho'_{ABT} = \sum_{i,j=0,1} \zeta_{i,j}^2 |i,j\rangle\langle i,j|_{AB} \otimes \sum_{0}^{3} \left|m, f_{i,j}^m\right\rangle\left\langle m, f_{i,j}^m\right|_T. \tag{31}$$

TP then advertises the corresponding Bell state depending on the value of m. Alice and Bob can obtain some information based on their measurement results and TP's announcement. Let $q_{m,i,j}$ represent the probability that TP announces message m depending on Alice and Bob observe $|i\rangle$ and $|j\rangle$. Then, we have

$$q_{m,i,j} = \left\langle f_{i,j}^m | f_{i,j}^m \right\rangle. \tag{32}$$

As described in the protocol, the raw key K_{AB} generates in the event that Alice and Bob both choose the measure operation and TP's result is $|\phi^+\rangle$ or $|\phi^-\rangle$. That is, $m = 0, 1$. Conditioning on this event, thus the final generated raw key system is

$$\rho_{ABT} = \frac{1}{N} \sum_{i,j,m=0,1} \zeta_{i,j}^2 |i,j\rangle\langle i,j|_{AB} \otimes \left|m, f_{i,j}^m\right\rangle\left\langle m, f_{i,j}^m\right|_T, \tag{33}$$

where, $N = \sum_{i,j,m=0}^{1} \zeta_{i,j}^2 \langle f_{i,j}^m | f_{i,j}^m \rangle$ is a normalization term. Then, TP may observe her ancilla to obtain some helpful information about K_{AB}.

3.2.2 Key rate derivation

In this part, our goal is to calculate the protocol's key rate r_{AB}. Following the definition of key rate, in this case, it can be expressed as

$$r_{AB} = S(A|T) - H(A|B). \tag{34}$$

If $r_{AB} > 0$, a secure secret key can be obtained.

To locate r_{AB}, we need to determine the values of $S(A|T)$ and $H(A|B)$. Since we have derived the final contributing raw key system ρ_{ABT}, it is not difficult to calculate $S(A|T)$ and $H(A|B)$ according to the derivation process in Sect. 3.1.

Let $q^k_{i,j}$ mean the probability that the raw keys of Alice and Bob are $|i\rangle$ and $|j\rangle$. Observing (33), we have

$$q^k_{i,j} = \frac{1}{N}\zeta^2_{i,j}\sum_{m=0}^{1}\langle f^m_{i,j}|f^m_{i,j}\rangle. \tag{35}$$

Then, it's easy to obtain $H(A,B) = H(\{q^k_{i,j}\}_{i,j})$. Let $q(0)$ be the probability that Bob's raw key is $|0\rangle$, then we have $q(0) = q^k_{1,0} + q^k_{0,0}$. Thereby, $H(B) = h(q(0))$. Following this fact, we can calculate:

$$H(A|B) = H(A,B) - H(B). \tag{36}$$

For $S(T|E)$, it can be derived from the Theorem 1 in Sect. 3.1. Tracing out B from ρ_{ABT} yields:

$$\begin{aligned}\rho_{AT} = &\frac{1}{N}\left(|0\rangle\langle 0|_A \otimes \sum_{j,m=0}^{1}\zeta^2_{0,j}\left|m,f^m_{0,j}\right\rangle\left\langle m,f^m_{0,j}\right|_T\right)\\ &+\frac{1}{N}\left(|1\rangle\langle 1|_A \otimes \sum_{j,m=0}^{1}\zeta^2_{1,j}\left|m,f^m_{1,j}\right\rangle\left\langle m,f^m_{1,j}\right|_T\right).\end{aligned} \tag{37}$$

Applying Theorem 1 to the above state, we can derive the result:

$$\begin{aligned}S(A|T) &\geq \frac{1}{N}\sum_{j,m}\left(\left\langle\zeta^2_{0,j}f^m_{0,j}|f^m_{0,j}\right\rangle + \zeta^2_{1,\bar{j}}\langle f^m_{1,\bar{j}}|f^m_{1,j}|\right)H_{j,m},\\ H_{j,m} &= h\left(\frac{\zeta^2_{0,j}\langle f^m_{0,j}|f^m_{0,j}\rangle}{\zeta^2_{0,j}\langle f^m_{0,j}|f^m_{0,j}\rangle + \zeta^2_{1,\bar{j}}\langle f^m_{1,\bar{j}}|f^m_{1,\bar{j}}\rangle}\right) - h(\lambda_{j,m}),\end{aligned} \tag{38}$$

$$\lambda_{j,m} = \frac{1}{2} + \frac{\sqrt{(\zeta^2_{0,j}\langle f^m_{0,j}|f^m_{0,j}\rangle - \zeta^2_{1,\bar{j}}\langle f^m_{1,\bar{j}}|f^m_{1,\bar{j}}\rangle)^2 + 4\zeta^2_{0,j}\zeta^2_{1,\bar{j}}\mathrm{Re}^2\langle f^m_{0,j}|f^m_{1,\bar{j}}\rangle}}{2(\zeta^2_{0,j}\langle f^m_{0,j}|f^m_{0,j}\rangle + \zeta^2_{1,\bar{j}}\langle f^m_{1,\bar{j}}|f^m_{1,\bar{j}}\rangle)}, \tag{39}$$

where $\bar{j} = 1 - j$.

To evaluate the $S(A|T)$, we need to obtain the values of $\zeta_{i,j}$ and the inner-products in the above expressions. Thus, in the following, we will use parameters that Alice and Bob can directly observe to denote $S(A|T)$. Recall (30) and (32), the values of $\zeta_{i,j}$ and the inner-products $\langle f^m_{i,j}|f^m_{i,j}\rangle$ can be easily obtained. what remains is to calculate $\mathrm{Re}^2\langle f^m_{0,j}|f^m_{1,\bar{j}}\rangle$.

Observing the case that Alice and Bob both reflect the qubits, we may bound $\mathrm{Re}\langle f^m_{0,j}|f^m_{1,\bar{j}}\rangle$. Specifically, Alice and Bob both reflect the qubits directly, TP then applies U on the reflected qubits to obtain:

$$\sum_{m=0}^{3}|m\rangle\otimes\sum_{i,j=0,1}\zeta_{i,j}\left|f^m_{i,j}\right\rangle. \tag{40}$$

According the value of m, TP then announces the message in the form of a Bell state. Here, we focus on the events that TP announces $|\phi^+\rangle$ and $|\phi^-\rangle$, i.e., $m=0,1$. Unlike previous protocols [25, 29], we will use the reflection error events and reflection correct events to obtain the range of $\mathrm{Re}\langle f^m_{0,j}|f^m_{1,\bar{j}}\rangle$. We first discuss the case that TP announces $|\phi^-\rangle$, i.e., $m=1$. From (40), the probability that TP announces $|\phi^-\rangle$ is:

$$p_{\phi^-}=\sum_{x,y,i,j=0,1}\zeta_{x,y}\zeta_{i,j}\left\langle f^1_{x,y}|f^1_{i,j}\right\rangle. \tag{41}$$

This provides a way to bound $\mathrm{Re}\langle f^1_{0,0}|f^1_{1,1}\rangle$ and $\mathrm{Re}\langle f^1_{0,1}|f^1_{1,0}\rangle$. After some algebra, we have

$$\left|p_{\phi^-}-\sum_{i,j}\zeta^2_{i,j}\left\langle f^1_{i,j}|f^1_{i,j}\right\rangle\right|=\begin{vmatrix}2\zeta_{0,0}\zeta_{11}\,\mathrm{Re}\left\langle f^1_{0,0}\middle|f^1_{1,1}\right\rangle+2\zeta_{0,0}\zeta_{0,1}\,\mathrm{Re}\left\langle f^1_{0,0}\middle|f^1_{0,1}\right\rangle\\+2\zeta_{0,0}\zeta_{1,0}\,\mathrm{Re}\left\langle f^1_{0,0}\middle|f^1_{1,0}\right\rangle+2\zeta_{1,1}\zeta_{0,1}\,\mathrm{Re}\left\langle f^1_{1,1}\middle|f^1_{0,1}\right\rangle\\+2\zeta_{1,1}\zeta_{1,0}\,\mathrm{Re}\left\langle f^1_{1,1}\middle|f^1_{1,0}\right\rangle+2\zeta_{0,1}\zeta_{1,0}\,\mathrm{Re}\left\langle f^1_{0,1}\middle|f^1_{1,0}\right\rangle\end{vmatrix}. \tag{42}$$

Applying the Cauchy–Schwarz inequality and (32) into $\mathrm{Re}\langle f^1_{0,j}|f^1_{1,\bar{j}}\rangle$, we have

$$\begin{aligned}\mathrm{Re}\left\langle f^1_{0,0}|f^1_{1,1}\right\rangle&\le\sqrt{\left\langle f^1_{0,0}|f^1_{0,0}\right\rangle\left\langle f^1_{1,1}|f^1_{1,1}\right\rangle}=\sqrt{q_{1,0,0}q_{1,1,1}},\\\mathrm{Re}\left\langle f^1_{0,1}|f^1_{1,0}\right\rangle&\le\sqrt{\left\langle f^1_{0,1}|f^1_{0,1}\right\rangle\left\langle f^1_{1,0}|f^1_{1,0}\right\rangle}=\sqrt{q_{1,0,1}q_{1,1,0}}.\end{aligned} \tag{43}$$

Generally speaking, when TP announces $|\phi^-\rangle$, i.e., $m=1$, the probability that Alice and Bob observe different results are small, otherwise it means that there is an error rate too high for the protocol to work properly. That is, the values of $q_{1,1,0}$ and $q_{1,0,1}$ are small, while the values of $q_{1,1,1}$ and $q_{1,0,0}$ are high. Hence, we focus on bounding $\mathrm{Re}\langle f^1_{0,0}|f^1_{1,1}\rangle$.

Let $\mathrm{Re}\langle f^1_{0,1}|f^1_{1,0}\rangle=\sqrt{q_{1,0,1}q_{1,1,0}}$, then applying the Cauchy–Schwarz inequality, Absolute value inequality (i.e., $|a+b|\le|a|+|b|$) and (32) into (42), we can obtain:

$$\begin{aligned}\left|\zeta_{0,0}\zeta_{1,1}\,\mathrm{Re}\left\langle f^1_{0,0}|f^1_{1,1}\right\rangle\right|\ge{}&\left|\frac{1}{2}p_{\phi^-}-\frac{1}{2}\sum_{i,j=0,1}\zeta^2_{i,j}q_{1,i,j}\right|-\zeta_{0,0}\zeta_{0,1}\sqrt{q_{1,0,0}q_{1,0,1}}\\&-\zeta_{0,0}\zeta_{1,0}\sqrt{q_{1,0,0}q_{1,1,0}}-\zeta_{1,1}\zeta_{1,0}\sqrt{q_{1,1,1}q_{1,1,0}}\\&-\zeta_{0,1}\zeta_{1,1}\sqrt{q_{1,0,1}q_{1,1,1}}-\zeta_{0,1}\zeta_{1,0}\sqrt{q_{1,0,1}q_{1,1,0}},\end{aligned} \tag{44}$$

where $\zeta_{i,j}$ can be estimated in (30), and p_{ϕ^-} can be estimated by Alice and Bob when TP announces $|\phi^-\rangle$. Following this fact, we have obtained the bounds of $\mathrm{Re}\langle f^1_{0,0}|f^1_{1,1}\rangle$ and $\mathrm{Re}\langle f^1_{0,1}|f^1_{1,0}\rangle$.

For the case that TP announces $|\phi^+\rangle$, i.e., $m=0$, we can adopt the same method to derive the bounds of $\mathrm{Re}\langle f^0_{0,0}|f^0_{1,1}\rangle$ and $\mathrm{Re}\langle f^0_{0,1}|f^0_{1,0}\rangle$. Let $\mathrm{Re}\langle f^0_{0,1}|f^0_{1,0}\rangle=\sqrt{q_{0,0,1}q_{0,1,0}}$, then it is easy to

obtain

$$\begin{aligned}\left|\zeta_{0,0}\zeta_{1,1}\operatorname{Re}\langle f_{0,0}^{0}|f_{1,1}^{0}\rangle\right| \geq{}& \left|\frac{1}{2}p_{\phi^+}-\frac{1}{2}\sum_{i,j=0,1}\zeta_{i,j}^{2}q_{0,i,j}\right|-\zeta_{0,0}\zeta_{0,1}\sqrt{q_{0,0,0}q_{0,0,1}}\\&-\zeta_{0,0}\zeta_{1,0}\sqrt{q_{0,0,0}q_{0,1,0}}-\zeta_{1,1}\zeta_{1,0}\sqrt{q_{0,1,1}q_{0,1,0}}\\&-\zeta_{0,1}\zeta_{1,1}\sqrt{q_{0,0,1}q_{0,1,1}}-\zeta_{0,1}\zeta_{1,0}\sqrt{q_{0,0,1}q_{0,1,0}}.\end{aligned}\tag{45}$$

Until now, the bound of $\operatorname{Re}\langle f_{0,j}^{m}|f_{1,\bar{j}}^{m}\rangle$ has derived, which depend on the parameters $\zeta_{i,j}$ and $q_{m,i,j}$. Finally, the value of $S(A|T)$ and $H(A|B)$ can be obtained based on the parameters available for Alice and Bob.

3.2.3 Key rate evaluation

Here, we assume that the connections between users are all independent depolarized channels. This also allows us to compare with prior work. The two qubits depolarization channel of TP to Alice and Bob (as well as, Alice and Bob to TP) can be modeled with parameter p:

$$\varepsilon_p(\rho)=(1-p)\rho+\frac{p}{4}I,\tag{46}$$

where I is the identity operator.

To compute the protocol's key rate r_{AB}, we need to obtain $\zeta_{i,j}$, $q_{m,i,j}$, p_{ϕ^+} and p_{ϕ^-}. In the following, the connection between parameter p and $\zeta_{i,j}$, $q_{m,i,j}$, p_{ϕ^+}, p_{ϕ^-} will be build. Let's start with $\zeta_{i,j}$. TP is adversarial, she may prepare arbitrary quantum states and send them to Alice and Bob. In order to comply with the original protocol requirements as much as possible, we assume that the state of TP is $|\phi^+\rangle$. Then passing the depolarization channel, we have

$$\varepsilon_p\left(\left|\phi^+\right\rangle\left\langle\phi^+\right|\right)=(1-p)\left(\left|\phi^+\right\rangle\left\langle\phi^+\right|\right)+\frac{p}{4}I.\tag{47}$$

Thus the probability that Alice and Bob observe $|i\rangle$ and $|j\rangle$:

$$\zeta_{0,0}^{2}=\frac{2-p}{4}=\zeta_{1,1}^{2},\qquad \zeta_{0,1}^{2}=\frac{p}{4}=\zeta_{1,0}^{2}.\tag{48}$$

Then, we calculate $q_{m,i,j}$, (i.e., the probability that TP announces message m depending on Alice and Bob observe $|i,j\rangle$). If Alice and Bob observe $|0,0\rangle$, then passing the depolarization channel, the state will be

$$\varepsilon_p\left(|00\rangle\langle 00|\right)=(1-p)|00\rangle\langle 00|+\frac{p}{4}\sum_{i,j=0,1}|i,j\rangle\langle i,j|.\tag{49}$$

According to the original protocol, TP will perform Bell-based measurement and announce the result. In order to minimize the error of TP's attacks (i.e., incorporate the error into the channel noise), the effect of U should be consistent with the role of TP performing Bell-based measurement on the qubits. Thus, the probability that TP announce $|\phi^-\rangle$, i.e., $m=1$ conditioning on Alice and Bob observe $|0,0\rangle$ is $\frac{1-p}{2}+\frac{p}{4}=\frac{2-p}{4}$. Using the similar

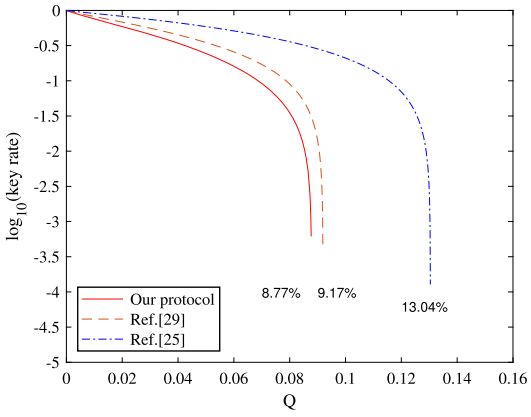

Figure 4 A diagram of the key rate for two classical users to achieve key distribution. Observe that the protocol can work with noise less than 8.77%. Since we only adopt Alice and Bob both measure or both reflect events to calculate the critical parameters without exploiting the mismatched event, resulting in a lower key rate for our protocol than in [25] and [29]. If the same approach as in [25] and [29] is used, a key rate similar to that of [25, 29] can be achieved

process, the other cases will be obtained. Therefore, we have

$$\begin{aligned} q_{0,0,0} &= \frac{2-p}{4} = q_{0,1,1}, \qquad q_{0,0,1} = \frac{p}{4} = q_{0,1,0}, \\ q_{1,0,0} &= \frac{2-p}{4} = q_{1,1,1}, \qquad q_{1,0,1} = \frac{p}{4} = q_{1,1,0}. \end{aligned} \tag{50}$$

For p_{ϕ^+} and p_{ϕ^-}, (i.e., the probabilities that TP announces message $m = 0$ and $m = 1$ when Alice and Bob both reflect the qubits), we also can use p to represent. In more detail, the system of this case can be described as $\varepsilon_p(\varepsilon_p(|\phi^+\rangle\langle\phi^+|))$. Thus, we can derive p_{ϕ^+} and p_{ϕ^-}:

$$p_{\phi^+} = (1-p)^2 + (1-p)\frac{p}{4} + \frac{p}{4}, \qquad p_{\phi^-} = \frac{p}{4}(1-p) + \frac{p}{4}. \tag{51}$$

Note that the above settings for probabilities $\zeta_{i,j}^2$, $q_{m,i,j}$, p_{ϕ^+}, and p_{ϕ^-} are consistent with previous work [25, 29]. Furthermore, we also use Q here as a variable to describe them, which is the probability that Alice and Bob observe different results. It's not difficult to see that $Q = \zeta_{0,1}^2 + \zeta_{1,0}^2 = \frac{p}{2}$. Putting everything together, the key rate r_{AB} can be computed by the variable Q. The relationship between r_{AB} and Q is shown in Fig. 4. As long as $Q \leq 8.77\%$, we have $r > 0$, that is, a secure key can be obtained by Alice and Bob.

4 Generalization to other semi-quantum protocols

In our protocol, Alice, Bob, and TP can establish the secure key sequence with each other. In more detail, Alice and Bob share a key sequence $K_{AB} = [k_{AB}^1, k_{AB}^2, \ldots, k_{AB}^n]$; Alice and TP share a key sequence $K_{TA} = [k_{TA}^1, k_{TA}^2, \ldots, k_{TA}^n]$; Bob and TP have a key sequence $K_{TB} = [k_{TB}^1, k_{TB}^2, \ldots, k_{TB}^n]$. Following this fact, our protocol can be applied to other semi-quantum cryptography protocols, such as semi-quantum private comparison and semi-quantum key agreement protocols.

4.1 Semi-quantum private comparison protocol

Semi-quantum private comparison (SQPC) [18–22] is one of the essential applications of quantum cryptography, whose goal is to allow two classical users, Alice and Bob, to compare whether their private data are the same with the help of TP who has the full quantum capability and may be adversarial. According to the definition of the SQPC protocol, it should follow the rules given below:

1. *Correctness:* The comparison result should be correct.
2. *Security:* Any attackers cannot steal users' data without being detected.
3. *Privacy:* Each user's private data should be kept secret from others.

4.1.1 The detailed steps of SQPC protocol

Same as the SQKD protocol setting, Alice and Bob have the limited quantum capability, while TP has full quantum power and may be adversarial. Alice and Bob have the private binary strings $M_A = [m_A^1, m_A^2, \ldots, m_A^n]$ and $M_B = [m_B^1, m_B^2, \ldots, m_B^n]$, respectively. The detailed steps are shown below.

Step 1$^{\text{SQPC}} \sim$ *Step 6*$^{\text{SQPC}}$*:* These steps are the same as the SQKD protocol described in Sect. 2. After that, Alice, Bob, and TP can establish the secure key sequences with each other, denoted as

$$\begin{aligned} K_{AB} &= \left[k_{AB}^1, k_{AB}^2, \ldots, k_{AB}^n\right], \\ K_{TA} &= \left[k_{TA}^1, k_{TA}^2, \ldots, k_{TA}^n\right], \\ K_{TB} &= \left[k_{TB}^1, k_{TB}^2, \ldots, k_{TB}^n\right]. \end{aligned} \tag{52}$$

Step 7$^{\text{SQPC}}$*:* Alice and Bob calculate $Q_A^j = k_{AB}^j \oplus k_{TA}^j \oplus m_A^j$ and $Q_B^j = k_{AB}^j \oplus k_{TB}^j \oplus m_B^j$, respectively, where $\oplus$ is the modulo 2 summation, and $j \in \{1, 2, \ldots, n\}$. Afterwards, Alice and Bob send $Q_A = [Q_A^1, Q_A^2, \ldots, Q_A^n]$ and $Q_B = [Q_B^1, Q_B^2, \ldots, Q_B^n]$ to TP.

Step 8$^{\text{SQPC}}$*:* TP calculates $R^j = Q_A^j \oplus Q_B^j \oplus k_{TA}^j \oplus k_{TB}^j$. If $R^j = 0$ for $j = 1, 2, \ldots, n$, it means that Alice and Bob have the same secrets. Otherwise, their secrets are not equal.

4.1.2 Analysis of SQPC protocol

It is easy to see that our protocol satisfies the requirements of the SQPC protocol.

Correctness: In our protocol, Alice and Bob can share $K_{AB} = [k_{AB}^1, k_{AB}^2, \ldots, k_{AB}^n]$ based on S_A and S_B. Then, TP can establish the secure key sequence $K_{TA} = [k_{TA}^1, k_{TA}^2, \ldots, k_{TA}^n]$ ($K_{TB} = [k_{TB}^1, k_{TB}^2, \ldots, k_{TB}^n]$) with Alice (Bob) based on the measurement result of T_A (T_B). Afterwards, Alice uses K_{AB}^j and K_{TA}^j to encrypt her secret information m_A^j as

$$Q_A^j = k_{AB}^j \oplus k_{TA}^j \oplus m_A^j. \tag{53}$$

Bob also uses K_{AB}^j and K_{TB}^j to encrypt his secret information m_B^j as

$$Q_B^j = k_{AB}^j \oplus k_{TB}^j \oplus m_B^j. \tag{54}$$

Finally, TP calculates $R^j = Q_A^j \oplus Q_B^j \oplus k_{TA}^j \oplus k_{TB}^j$. It is easy to obtain that

$$\begin{aligned} R^j &= Q_A^j \oplus Q_B^j \oplus k_{TA}^j \oplus k_{TB}^j \\ &= k_{AB}^j \oplus k_{TA}^j \oplus m_A^j \oplus k_{AB}^j \oplus k_{TB}^j \oplus m_B^j \oplus k_{TA}^j \oplus k_{TB}^j \\ &= m_A^j \oplus m_B^j. \end{aligned} \tag{55}$$

The results show that our SQPC protocol can guarantee the correctness of the output.

Security: The security of this SQPC protocol is based on the fact that a secure key relationship can be established between Alice, Bob, and TP. In the previous security analysis, we have shown that Alice, bob, and TP can establish a secure key relationship. Therefore, our protocol is secure. That is, users' private data will not be leaked out to others, and attackers cannot steal users' data without being detected.

Privacy: The user's secret information is encrypted with K_{AB} and K_{TA} (K_{TB}). Any eavesdropper has access to at most a portion of the encryption key. Therefore, each user's private data is kept secret from others.

4.2 Semi-quantum key agreement protocol

The goal of semi-quantum key agreement (SQKA) [40–43] is to achieve the same contribution of all participants to the final shared key, where the capabilities of the participants are different and only one user is fully quantum capable, while other users' quantum capabilities are limited.

In our SQKA protocol, TP has full quantum capability, while Alice and Bob are two classical users with limited quantum power. They have a secret bit strings m_A, m_B and m_T, respectively. That is

$$\begin{aligned} m_A &= \left\{m_A^1, m_A^2, \ldots, m_A^n\right\}, \\ m_B &= \left\{m_B^1, m_B^2, \ldots, m_B^n\right\}, \\ m_T &= \left\{m_T^1, m_T^2, \ldots, m_T^n\right\}. \end{aligned} \tag{56}$$

TP, Alice and Bob want to establish a secret key $K = m_A \oplus m_B \oplus m_T$, where all three parties contribute equally to construct the key.

4.2.1 The detailed steps of SQKA protocol

In the following, we describe the SQKA protocol based on the previously proposed SQKD protocol. For simplicity, we would only like to introduce necessary steps that differ from the SQKD protocol above, while others are the same as those described in Sect. 2.

Step 1$^{\text{SQKA}}$ $\sim$ *Step 6*$^{\text{SQKA}}$*:* These steps are the same as the SQKD protocol described in Sect. 2. After that, Alice, Bob, and TP can establish the secure key sequences with each other, denoted as K_{AB}, K_{TA} and K_{TB}, respectively.

Step 7$^{\text{SQKA}}$*:* Alice, Bob and TP encrypt their secret bit stings m_A, m_B and m_T with K_{AB}, K_{TA} and K_{TB}. More exactly, Alice uses K_{AB} and K_{TA} to encrypt m_A as:

$$\begin{aligned} Q_{A\to B} &= \left[m_A^1 \oplus K_{AB}^1, m_A^2 \oplus K_{AB}^2, \ldots, m_A^n \oplus K_{AB}^n\right], \\ Q_{A\to T} &= \left[m_A^1 \oplus K_{TA}^1, m_A^2 \oplus K_{TA}^2, \ldots, m_A^n \oplus K_{TA}^n\right], \end{aligned} \tag{57}$$

Bob uses K_{AB} and K_{TB} to encrypt m_B as:

$$\begin{aligned} Q_{B\to A} &= \left[m_B^1 \oplus K_{AB}^1, m_B^2 \oplus K_{AB}^2, \ldots, m_B^n \oplus K_{AB}^n\right], \\ Q_{B\to T} &= \left[m_B^1 \oplus K_{TB}^1, m_B^2 \oplus K_{TB}^2, \ldots, m_B^n \oplus K_{TB}^n\right], \end{aligned} \tag{58}$$

TP uses K_{TA} and K_{TB} to encrypt m_T as:

$$\begin{aligned} Q_{T\to A} &= \left[m_T^1 \oplus K_{TA}^1, m_T^2 \oplus K_{TA}^2, \ldots, m_T^n \oplus K_{TA}^n\right], \\ Q_{T\to B} &= \left[m_T^1 \oplus K_{TB}^1, m_T^2 \oplus K_{TB}^2, \ldots, m_T^n \oplus K_{TB}^n\right]. \end{aligned} \tag{59}$$

Step 8^{SQKA}*:* Alice, Bob and TP each calculates the hash values of the corresponding encrypted messages and announces the results to other two parties. For example, Alice will send the hash values $h(Q_{A\to B})$ and $h(Q_{A\to T})$ to Bob and TP, respectively (Bob and TP will do similar operations). Here $h(\cdot)$ is some one-way hash function. Note that this step is used to avoid information leaking and tampering due to the asynchronous release of information.

Step 9^{SQKA}*:* After that, Alice, Bob, and TP publish their encrypted messages to the other two parties. Alice calculates the hash values of $Q_{B\to A}$ and $Q_{T\to A}$ to obtain the results $h'(Q_{B\to A})$ and $h'(Q_{T\to A})$. If $h'(Q_{B\to A}) = h(Q_{B\to A})$ and $h'(Q_{T\to A}) = h(Q_{T\to A})$, Alice will accept them. Then, Alice can decrypt $Q_{B\to A}$ and $Q_{T\to A}$ with K_{AB} and K_{TA} to obtain the secret keys m_B and m_T. Using the same procedure, Bob and TP can also obtain m_A, m_T and m_A, m_B, respectively.

Step 10^{SQKA}*:* Each of Alice, Bob, and TP has the secret keys m_A, m_B and m_T. Thus, they can calculate the final key as $K = m_A \oplus m_B \oplus m_T$.

4.2.2 Fairness of the proposed SQKA protocol

In Sect. 3, we provide a detailed security analysis of the SQKD protocol, and since our proposed SQKA protocol is based on the SQKD protocol, the security analysis is similar. That is, Alice, Bob, and TP can establish the secure key sequences with each other. Unlike SQKD protocol, SQKA requires all parties equally contribute to the final key. Therefore, we focus on analyzing the fairness of each party's contribution to the key.

Without loss of generality, we assume that Alice wants to determine the shared key to be $K_A^* = [m_A^{*1}, m_A^{*2}, \ldots, m_A^{*n}]$ alone. To achieve this goal, Alice needs to obtain m_B and m_T. In our protocol, Alice has the opportunity to obtain m_B and m_T from Bob and TP announcing $Q_{B\to A}$ and $Q_{T\to A}$ only in step 9. After that, Alice calculates

$$\begin{aligned} Q_{A\to B}^* &= K_A^* \oplus m_B \oplus m_T \oplus K_{AB}, \\ Q_{A\to T}^* &= K_A^* \oplus m_B \oplus m_T \oplus K_{TA}, \end{aligned} \tag{60}$$

and Alice then publishes $Q_{A\to B}^*$ and $Q_{A\to T}^*$ to Bob and TP, respectively. As a result, Bob and TP can obtain the final key K_A^* by computing $(K_A^* \oplus m_B \oplus m_T) \oplus m_B \oplus m_T = K_A^*$. Unfortunately, Alice's behavior will be detected by Bob and TP. Because $Q_{A\to B}^*$ and $Q_{A\to T}^*$ can be accepted by Bob and TP only if they satisfy: $h'(Q_{A\to B}^*) = h(Q_{A\to B})$ and $h'(Q_{A\to T}^*) = h(Q_{A\to T})$. Obviously, they are not equal, so Alice's cheating behavior cannot succeed.

If two dishonest parties conspire to perform deceptions similar to those described above, third parties will inevitably discover their shows due to the use of hash functions.

The results show that our protocol can guarantee all parties equally contribute to the final key.

5 Discussion

In this paper, we propose several different types of semi-quantum protocols. Specifically, we focus on semi-quantum cryptography protocols, including SQKD, SQPC, and SQKA, which all rely on two-way communication and are susceptible to Trojan attacks. The analysis of Trojan horse attacks is also one of the focuses. Therefore, in this part, we first investigate the resistance of several protocols proposed in this paper to Trojan attacks.

Trojan horse attacks in quantum systems include the invisible photon attack [44] and the delay-photon attack [45]. To mitigate the risks posed by these Trojan attacks, it is essential to incorporate specific devices like wavelength filters and photon number separators for each user [46]. The wavelength filter enables the signal receiver to counteract the former attack, while the photon number separator offers protection against the latter attack. Despite the potential impact on protocol efficiency, the above devices are necessary for quantum protocols involving two-way communication to effectively mitigate Trojan attacks. Therefore, our protocols can resist Trojan attacks by equipping the necessary devices.

Additionally, it is worth mentioning that some variants of semi-quantum key distribution protocols, as described in references [32, 33], address the issue of Trojan attacks by improving capabilities for classical users, effectively transforming the protocol into a one-way communication scheme. This alternative approach can also be considered, particularly if classical users possess the ability to perform lightweight unitary operations, as demonstrated in literature [33].

In the following, we conduct separate comparisons between the proposed protocols and their respective counterparts, to emphasize the unique features of each protocol.

5.1 Comparison of SQKD protocol

Noise tolerance is a critical indicator of the SQKD protocol, and we have analyzed the protocol's noise tolerance (i.e., key rate) under different conditions. Specifically, our proposed protocol demonstrates a noise tolerance of 12.75% for establishing secure keys between quantum and classical users, and a noise tolerance of 8.77% for establishing secure keys between two classical users. These results show that our SQKD protocol exhibits similar security to traditional QKD protocols, such as the BB84 protocol with a noise tolerance of 11%.

To provide a clear comparison of noise tolerance and applicable scenarios, we have compared our protocol with similar SQKD protocols in Table 1. The comparison reveals that our protocol is suitable not only for establishing key relationships between quantum and classical users, but also between two classical users. In contrast, previous SQKD protocols are limited to only one scenario, either between quantum and classical users or between two classical users, which significantly restricts their practical applications.

In order to compare the noise tolerance of our proposed semi-quantum key distribution (SQKD) protocol with existing protocols, we analyze the noise tolerance from two perspectives. Firstly, in the scenario of key establishment between quantum and classical users, our protocol outperforms previous similar protocols [9–12] in terms of noise tolerance. Secondly, in the scenario of key establishment between two classical users, our

Table 1 Comparisons among similar SQKD protocols

	Noise tolerance under quantum and classical users	Noise tolerance under two classical users	Suitable for quantum and classical users	Suitable for two classical users
Ref. [9]	5.34%	–	✓	✗
Ref. [10]	9.65%	–	✓	✗
Ref. [11]	11%	–	✓	✗
Ref. [12]	11.8%	–	✓	✗
Ref. [25]	–	13.04%	✗	✓
Ref. [26]	–	–	✗	✓
Ref. [27]	–	–	✗	✓
Ref. [28]	–	–	✗	✓
Ref. [29]	–	9.17%	✗	✓
Our protocol	12.75%	8.77%	✓	✓

Table 2 Comparison between our SQPC protocol and previous ones

	Qubit efficiency	Need pre-shared keys	Transmission mode
Ref. [18]	$\frac{n}{102n+1}$	Yes	Distributed
Ref. [19]	$\frac{n}{60n+1}$	Yes	Distributed
Ref. [20]	$\frac{n}{52n+1}$	No	Distributed
Ref. [21]	$\frac{n}{53n+1}$	Yes	Distributed
Ref. [22]	$\frac{n}{18n+1}$	No	Circular
Our protocol	$\frac{n}{26n+1}$	No	Distributed

protocol exhibits lower noise tolerance compared to similar protocols [25, 29], primarily due to the fact that we only utilize events where Alice and Bob both measure or both reflect, without exploiting mismatched events. If the same approach as in [25] and [29] is employed, a noise tolerance similar to that of [25, 29] can be achieved. Nonetheless, our protocol still achieves a noise tolerance comparable to previous protocols. It is important to note that Refs. [26–28] only provide security analysis under specific attacks, and no noise tolerance is calculated for these protocols.

5.2 Comparison of extension protocols

The performance of the proposed semi-quantum key agreement (SQKA) and semi-quantum private comparison (SQPC) protocols can be evaluated using the metric of qubit efficiency, as defined in [40]. Qubit efficiency is defined as $\eta = \frac{c}{q+b}$, where c, q, and b are the number of shared classical bits, the number of consumed qubits, and the number of classical bits needed, respectively.

We first calculate the qubit efficiency of the proposed SQPC protocol. In our protocol, Alice and Bob have n secret bits, respectively, which means $c = n$. To implement the protocol, TP needs to generate $4n$ Bell states, and $8n$ single particles, while Alice and Bob need to prepare $4n$ qubits, respectively as a replacement for their measured particles. Thus, the number of consumed qubits is $24n$. Then, Alice and Bob need $2n$ bits to publish their encrypted messages, and TP needs 1 bit to publish the comparison result. That is, $b = 2n + 1$. Putting everything together, the qubit efficiency of our protocol is $\frac{n}{26n+1}$. The qubit efficiencies of Refs. [18–22] are also listed in Table 2. It is evident from the table that our protocol has a higher qubit efficiency compared to protocols using distributed transmission. However, the protocol in [22] which uses circular transmission exhibits higher efficiency compared to our protocol.

Table 3 Comparison of our SQKA protocol with similar ones

	Qubit efficiency	Number of users	Quantum resources
Ref. [40]	$\frac{1}{10}$	Two	Bell states
Ref. [41]	$\frac{1}{15}$	Two	Bell states
Ref. [42]	$\frac{1}{48}$	Three	Cluster states
Ref. [43]	$\frac{1}{38}$	Three	GHZ states
Our protocol	$\frac{1}{36}$	Three	Bell states and single-particles

Next, we calculate the qubit efficiency of the proposed SQKA protocol. In this SQKA protocol, $24n$ qubits are consumed in order to implement the key negotiation of three users and finally generate a shared key of n bits. As for the consumed classical bits, each of user needs to publish n-bits encrypted messages to the other users, along with the hash of the encrypted message (suppose the length of the hash value is n-bits). Thus, the total classical bits is $3 * 2n + 3 * 2n = 12n$. Combining all these values, our protocol's qubit efficiency is $\frac{1}{36}$. Table 3 provides detailed comparison results of our protocol with similar protocols. One can easily observe that the qubit efficiency of three-party schemes is less than that of two-party schemes. It is obvious that as the number of classical users increases, the quantum resources required will also increase. Our protocol is more efficient for scenarios where three users contribute to the secret key.

6 Conclusion

In this work, we propose a novel semi-quantum key distribution (SQKD) protocol that utilizes entangled Bell states and single particles to enable secure key sharing among users of different types. Our protocol can serve as both SQKD and M-SQKD. This effectively reduces the complexity and cost of semi-quantum protocols that require SQKD and M-SQKD between different users to protect the users' private data, respectively.

To prove this SQKD protocol's security, we first analyze the attack strategies of attackers who want to obtain keys in different scenarios. Then the density matrix of the joint system that eventually contributes to the secure key is constructed. Finally, the noise tolerance of the protocol is derived by using the parameters observed in the channel. The results show that the noise tolerance of our protocol can reach the same level as that of the QKD protocol.

In addition to the proposed SQKD protocol, we also generalize our approach to other semi-quantum protocols such as SQPC and SQKA. We conduct comparative analyses of these protocols with similar existing protocols, highlighting the advantages of our proposed protocols in meeting the requirements of their respective use cases.

Several intriguing research questions remain to be addressed in future studies. Firstly, while we have generalized our protocols to SQKA and SQPC, there may be other unexplored application scenarios that could benefit from our approach. Secondly, our analysis has been limited to ideal environments, and practical implementations of devices in semi-quantum environments are still in the nascent stages [47, 48]. Investigating the application of our protocols in real-world scenarios with practical devices would be a promising direction for future research.

Funding

This work was supported by the National Natural Science Foundation of China under Grant 62271070, the BUPT Excellent Ph.D Students Foundation under Grant CX2021117, and the China Scholarship Council under Grant 202206470006.

Abbreviations
QKD, Quantum key distribution; SQKD, Semi-quantum key distribution; M-SQKD, Mediated Semi-quantum key distribution; TP, Third party; SOPC, Semi-quantum private comparison; SQKA, Semi-quantum key agreement.

Availability of data and materials
The data that support the findings of this study are available from the corresponding author upon reasonable request.

Declarations

Ethics approval and consent to participate
Not applicable.

Consent for publication
Not applicable.

Competing interests
The authors declare no competing interests.

Author contributions
Chong-Qiang Ye designed the protocol, conducted the security analysis, and wrote the manuscript; Yanyan Hou and Zhuo Wang checked the writing; Jian Li and Xiu-Bo Chen reviewed the manuscript. All authors read and approved the final manuscript

Author details
[1]School of Artificial Intelligence, Beijing University of Posts and Telecommunications, 100876, Beijing, China. [2]Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, 100876, Beijing, China. [3]College of Information Science and Engineering, ZaoZhuang University, 277160, ZaoZhuang Shandong, China.

Received: 21 April 2023 Accepted: 9 June 2023 Published online: 20 June 2023

References

1. Bennet CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proc. IEEE int. conf. Comput., syst. Signal process. Bangalore, India. 1984. p. 175–9.
2. Ekert AK. Quantum cryptography based on Bell's theorem. Phys Rev Lett. 1991;67(6):661.
3. Bennett CH. Quantum cryptography using any two nonorthogonal states. Phys Rev Lett. 1992;68:3121.
4. Renner R, Gisin N, Kraus B. Information-theoretic security proof for quantum-key-distribution protocols. Phys Rev A. 2005;72(1):012332.
5. Lo HK, Curty M, Tamaki K. Secure quantum key distribution. Nat Photonics. 2014;8(8):595–604.
6. Scarani V, Bechmann-Pasquinucci H, Cerf NJ et al. The security of practical quantum key distribution. Rev Mod Phys. 2009;81(3):1301.
7. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. Phys Rev Lett. 2007;99(14):140501.
8. Boyer M, Gelles R, Kenigsberg D, Mor T. Semiquantum key distribution. Phys Rev A. 2009;79(3):032341.
9. Krawec WO. Security proof of a semi-quantum key distribution protocol. In: 2015 IEEE international symposium on information theory (ISIT). New York: IEEE Press; 2015. p. 686–90.
10. Zhang W, Qiu DW, Mateus P. Security of a single-state semi-quantum key distribution protocol. Quantum Inf Process. 2018;17(6):1–21.
11. Krawec WO. Quantum key distribution with mismatched measurements over arbitrary channels. Quantum Inf Comput. 2017;17(3–4):209–41.
12. Ye CQ, Li J, Chen XB et al. An efficient semi-quantum key distribution protocol and its security proof. IEEE Commun Lett. 2022;26(6):1226–30.
13. Zou XF, Qiu QW. Three-step semiquantum secure direct communication protocol. Sci China, Phys Mech Astron. 2014;57(9):1696–702.
14. Luo Y-P, Hwang T. Authenticated semi-quantum direct communication protocols using bell states. Quantum Inf Process. 2016;15(2):947–58.
15. Ye TY, Ye CQ. Semi-quantum dialogue based on single photons. Int J Theor Phys. 2018;57:1440–54.
16. Li Q, Chan WH, Long DY. Semiquantum secret sharing using entangled states. Phys Rev A. 2010;82(2):022303.
17. Li LZ, Qiu DW, Paulo M. Quantum secret sharing with classical bobs. J Phys A, Math Theor. 2013;46(4):045304.
18. Thapliyala K, Sharmab RD, Pathak A. Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment. Int J Quantum Inf. 2018;16:1850047
19. Ye TY, Ye CQ. Measure-resend semi-quantum private comparison without entanglement. Int J Theor Phys. 2018;57(12):3819–34.
20. Lin P-H, Hwang T, Tsai C-W. Efficient semi-quantum private comparison using single photons. Quantum Inf Process. 2019;18(7):1–14.
21. Yan LL, Zhang SB, Chang Y et al. Semi-quantum private comparison protocol with three-particle G-like states. Quantum Inf Process. 2021;20(1):1–16.
22. Ye CQ, Li J, Chen XB, Tian Y. Efficient semi-quantum private comparison without using entanglement resource and pre-shared key. Quantum Inf Process. 2021;20(8):1–19.
23. Iqbal H, Krawec WO. Semi-quantum cryptography. Quantum Inf Process. 2020;19(3):1–52.
24. Krawec WO. Mediated semiquantum key distribution. Phys Rev A. 2015;91:032323.

25. Krawec WO. An improved asymptotic key rate bound for a mediated semi-quantum key distribution protocol. Quantum Inf Comput. 2016;16(9–10):813–34.
26. Liu Z-R, Hwang T. Mediated semi-quantum key distribution without invoking quantum measurement. Ann Phys. 2018;530(4):1700206.
27. Lin P-H, Tsai C-W, Hwang T. Mediated semi-quantum key distribution using single photons. Ann Phys. 2019;531(8):1800347.
28. Chen LL, Li Q, Liu CD, Peng Y, Yu F. Efficient mediated semi-quantum key distribution. Phys A, Stat Mech Appl. 2021;582:126265.
29. Guskind J, Krawec W. Mediated semi-quantum key distribution with improved efficiency. Quantum Sci Technol. 2022;7(3):035019.
30. Krawec WO. Multi-mediated semi-quantum key distribution. In: 2019 IEEE globecom workshops (GC wkshps). New York: IEEE Press; 2019. p. 1–6.
31. Ye CQ, Li J, Chen XB et al. Circular mediated semi-quantum key distribution. Quantum Inf Process. 2023;22(4):170.
32. Tsai CW, Yang CW, Lee NY. Lightweight mediated semi-quantum key distribution protocol. Mod Phys Lett A. 2019;34(34):1950281.
33. Tsai CW, Yang CW. Lightweight mediated semi-quantum key distribution protocol with a dishonest third party based on Bell states. Sci Rep. 2021;11(1):23222.
34. Zhou NR, Zhu KN, Bi W et al. Semi-quantum identification. Quantum Inf Process. 2019;18(6):1–17.
35. Ye TY, Xu TJ, Geng MJ et al. Two-party secure semiquantum summation against the collective-dephasing noise. Quantum Inf Process. 2022;21(3):1–14.
36. Geng MJ, Chen Y, Xu TJ, Ye TY. Single-state semiquantum private comparison based on Bell states. EPJ Quantum Technol. 2022;9(1):1.
37. Gottesman D, Lo HK. Proof of security of quantum key distribution with two-way classical communications. IEEE Trans Inf Theory. 2003;49(2):457–75.
38. Renner R. Security of quantum key distribution. Int J Quantum Inf. 2008;6(01):1–127.
39. Christandl M, König R, Renner R. Postselection technique for quantum channels with applications to quantum cryptography. Phys Rev Lett. 2009;102(2):020504.
40. Shukla C, Thapliyal K, Pathak A. Semi-quantum communication: protocols for key agreement, controlled secure direct communication and dialogue. Quantum Inf Process. 2017;16(12):1–19.
41. Yan LL, Zhang SB, Chang Y et al. Semi-quantum key agreement and private comparison protocols using Bell states. Int J Theor Phys. 2019;58(11):3852–62.
42. Zhou NR, Zhu KN, Wang YQ. Three-party semi-quantum key agreement protocol. Int J Theor Phys. 2020;59(3):663–76.
43. Xu TJ, Chen Y, Geng MJ et al. Single-state multi-party semiquantum key agreement protocol based on multi-particle GHZ entangled states. Quantum Inf Process. 2022;21(7):1–18.
44. Cai QY. Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys Lett A. 2006;351(1–2):23–5.
45. Gisin N, Fasel S, Kraus B, Zbinden H, Ribordy G. Trojan-horse attacks on quantum-key distribution systems. Phys Rev A. 2006;73:022320
46. Deng FG, Zhou P, Li XH, et al. Robustness of two-way quantum communication protocols against Trojan horse attack. arXiv:quant-ph/0508168.
47. Boyer M, Katz M, Liss R et al. Experimentally feasible protocol for semiquantum key distribution. Phys Rev A. 2017;96(6):062335.
48. Han S, Huang Y, Mi S et al. Proof-of-principle demonstration of semi-quantum key distribution based on the Mirror protocol. EPJ Quantum Technol. 2021;8(1):1.

Publisher's Note