Scalable Mediated Semi-quantum Key Distribution

Chong-Qiang Ye 1,3, Jian Li∗2,3, Xiu-Bo Chen2, and Yan-Yan Hou1

1 School of Artificial Intelligence, Beijing University of Posts Telecommunications, Beijing 100876, China.
2 Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China
3 Key Laboratory of Cryptography of Zhejiang Province, Hangzhou Normal University, Hangzhou 311121, China

September 7, 2022

Abstract

Mediated semi-quantum key distribution (M-SQKD) permits two limited “semi-quantum” or “classical” users to establish a secret key with the help of a third party (TP), in which TP has fully quantum power and may be untrusted. Several protocols have been studied recently for two-party scenarios, but no one has considered M-SQKD for multi-party scenarios. In this paper, we design a circular M-SQKD protocol based on Bell states, which offers an approach to realizing multiple ‘classical’ users’ key distribution. Then, we prove the protocol is unconditional security in the asymptotic scenario. The protocol’s key rate and noise tolerance can be derived by utilizing the parameters observed in the channel. The results show that our protocol may hold similar security to a fully quantum one. We also compare the proposed protocol with other similar protocols in terms of noise tolerance, qubit efficiency, communication cost and scalability. Finally, the security proof method of this paper may contribute to studying the security of other circular semi-quantum cryptography protocols.

Keywords: Quantum cryptography, Semi-quantum key distribution, Security proof, Scalability

1 Introduction

Quantum key distribution (QKD) [1] enables both parties to generate a shared key according to quantum mechanics laws, securely countering the computationally unbounded adversary. Since the first QKD protocol was investigated by Bennett and Brassard, theoretical and experimental studies on QKD have increased significantly [2,3]. Nevertheless, both parties, Alice and Bob, are equipped with complete quantum resources, leading to high overhead for the quantum devices.

Semi-quantum key distribution (SQKD) was first investigated by Boyer et al. [4], which cut down the quantum capability of one party compared with QKD. In more detail, the SQKD has two parties, one of whom is fully quantum capable of doing anything quantum mechanics allows, while the other is limited to doing the below operations: (1) Measure and resend. Measuring the qubit in the basis {\[0\], \[1\]} (i.e., Z basis) and then resending an identical qubit to the next recipient; (2) Reflect. Reflecting the qubit directly (i.e., learning nothing about its state); (3) Permute. Reorder the qubits without disturbing them. The limited party is usually called “classical” or “semi-quantum”. Obviously, the classical party can only work on the Z basis, which may alleviate the burden of quantum resources. Since then, SQKD has attracted the extensive attention of researchers, and many SQKD protocols and security analysis methods have been proposed [5–13]. For example, in 2015, Krawec [6] demonstrated the unconditional security of SQKD protocol and derived the protocol’s key rate. After that, many researchers began to study the security of different SQKD protocols. Meanwhile, other types of semi-quantum cryptography protocols were also investigated, such as semi-quantum secure communication [14–16], semi-quantum secret

∗Corresponding author: lijian@bupt.edu.cn
sharing [17–19], and semi-quantum private comparison [20–22]. The reader is referred to [23] for a survey, which gave a detailed review of semi-quantum cryptography.

Mediated semi-quantum key distribution (M-SQKD) was first investigated in 2015 by Krawec [24], which is an essential research focus of SQKD. The primary different between SQKD and M-SQKD is that M-SQKD enables two “classical” users (Alice and Bob) to generate a secure key with the help of a third party (TP), while SQKD allows the keys to be shared between quantum and “classical” users. M-SQKD can be regarded as a basic protocol in the field of semi-quantum cryptography. So far, several M-SQKD protocols have been proposed with various quantum states and transport structures [25–32]. 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 (i.e., the qubits travel from TP to Alice, to Bob, then back to TP). In 2019, Krawec proposed a multi-party M-SQKD protocol where two (or more) adversarial quantum servers are used to help two “classical” users establish a secret key [29]. In 2022, Guskind et al. [30] improved the M-SQKD protocol’s efficiency without requiring additional users’ additional capabilities. In the above mentioned, only a few M-SQKD protocols provided security proof [24,25,30], while others only analyzed that protocols can resist certain types of attacks. In particular, no one has yet to consider how to implement key distribution for multiple “classical” users.

In this paper, we attempt to design an M-SQKD protocol that works for multiple “classical” users to establish the secret keys. Due to the scalability of circular transmission, this provides a way to implement key distribution for multiple classical users. Naturally, we propose a circular M-SQKD protocol based on Bell states, which is suitable for multi-party scenarios. To prove security, we figure out a lower bound of the protocol’s key rate and noise tolerance (i.e., error tolerance), by utilizing the specific parameters Alice and Bob may estimate. Indeed, if TP is semi-honest (i.e., TP fully complies with the requirements of the protocol, but otherwise, she can do anything she likes), using the key rate bound in this paper, Alice and Bob can obtain a secret key when the noise is smaller than 16.02%. If TP is untrusted (TP can do anything she wants, including preparing fake particles and publishing fake results), they can obtain a secret key when the noise is less than 13.19%. The results show that our protocol’s noise tolerance is close to previous protocols [24,25,30]. Even in the worst case (i.e., TP is untrusted), the noise tolerance is also better than previous M-SQKD protocols. Furthermore, we evaluate the performance of the protocol in terms of noise tolerance, qubit efficiency, communication cost and scalability. Compared with similar protocols, our protocol has comparable advantages in the above four aspects.

In summary, the contributions of this work are as follows. First, we propose a circular M-SQKD protocol with good scalability, which offers an approach to realizing multiple “classical” users’ key distribution. Second, we give a detailed security proof of this circular M-SQKD protocol. The results show that the proposed protocol has similar security as the full quantum protocol.

## 2 The Proposed M-SQKD Protocol

Let’s use two-party scenarios as an example for illustration (the multi-party scenarios will be discuss later). The “classical” users, Alice and Bob, are only allowed to reflect the qubits to the next recipient; or measure and resend the qubits to the next recipient on $Z$ basis. They desire to generate a secure key with a quantum TP’s help, who may be untrusted. The detailed process is given in the following.

**Step 1:** TP prepares $8(N + \delta)$ Bell states where each state is $|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$ and $\delta$ is a fixed parameter. Subsequently, she sends the second qubit of each Bell state to Alice.

**Step 2:** Upon receiving the qubit, Alice randomly decides to reflect it to Bob or measure and resend it to Bob.

**Step 3:** Similarly, Bob randomly decides to reflect or to measure and resend the received qubit to TP.

**Step 4:** TP uses the Bell basis to measure the received qubit and the corresponding qubit in her hand. Then, TP announces her measurements to Alice and Bob.
Step 5: After TP releases her measurements, Alice and Bob divulge their choices through the authenticated classical channels. According to their choices, the following three cases are available.

- **Case 1**: When Alice and Bob reflect the received qubit, 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 2**: When they measure and resend the received qubit, TP will publish the result as either $|\phi^+\rangle$ or $|\phi^-\rangle$. If the result of TP is not $|\phi^+\rangle$ or $|\phi^-\rangle$, they will discard this case.

- **Case 3**: When they perform different operations on the received qubit, this case will be discarded.

Step 6: Alice and Bob select a small subset of Case 2 and divulge their measurements for eavesdropping detection. Once the error rate is over the threshold, the protocol terminates. If not, the protocol continues.

Step 7: After the classical post-processing (e.g., privacy amplification), two “classical” users can obtain the final secure key.

3 Security

In this section, we will give a detailed proof of security. Here we only consider the threat posed by an adversarial TP instead of outside eavesdroppers because outside eavesdroppers’ attacks can be absorbed into the TP’s attacks. Besides, according to [33] and [34], security against collective attacks is enough to demonstrate security against arbitrary general attacks. Thereby, we focus on proving security against collective attacks.

In our protocol, the raw keys are only established in the event that Alice and Bob choose to measure, and that TP announces $|\phi^-\rangle$. Under collective attacks, the system of Alice, Bob, and TP can be described as

$$\rho_{ABT} = \sum_{i,j} |i,j\rangle\langle i,j|_{AB} \otimes \rho_T,$$

where $\rho_T$ denotes the state of TP’s ancilla. Let $N$ denote the size of Alice and Bob’s raw key, $\ell(n)$ denote the length of secure key. Based on [2], our protocol’s key rate in the asymptotic scenario is

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

where $S(\cdot)$ denotes the Von Neumann entropy, and $H(\cdot)$ means the Shannon entropy. Observing the system’s parameters, the conditional entropy of $S(A|T)$ and $H(A|B)$ can be derived. If $r > 0$, the protocol can obtain a secure secret key. Hence, the goal of the next stage is to analyze TP’s attack strategy and compute the key rate $r$.

3.1 The scenario of semi-honest TP

We first consider a particular scenario where TP is semi-honest. In this scenario, TP follows the protocol description thoroughly, but otherwise, she can do anything she likes. As for channel noise, we assume that its effects can be incorporated into the errors caused by TP attacks [6].

3.1.1 The attack strategy of semi-honest TP

To catch Alice and Bob’s raw key, the attack strategy of TP can be modeled as follows (Also see Fig. 1). Here, we first consider Alice and Bob both measure and resend the received qubit.

1) According to the protocol’s description, TP first sends the second qubit of $|\phi^+\rangle$ to Alice. After that, Alice measures and resends the received qubit. Thus, the density operator describing the system of Alice and TP is

$$\rho_1 = \frac{1}{2} |00\rangle\langle 00|_{HA} + \frac{1}{2} |11\rangle\langle 11|_{HA}$$

where $H$ denotes the qubit left in TP’s hands, and $A$ denotes Alice’s measurement result.
2) TP launches her first attack on the qubits from Alice. Specifically, she performs the $U_1$ operation on the Alice’s qubit and her auxiliary state $|0\rangle_T$. The effect of $U_1$ is

$$U_1 |0, 0\rangle = |0, E_0\rangle + |1, E_1\rangle,$$
$$U_1 |1, 0\rangle = |1, E_3\rangle + |0, E_2\rangle.$$  \hspace{1cm} (4) (5)

After TP’s attack, the system becomes

$$\rho_2 = \frac{1}{2}|0\rangle_H \otimes (|0, E_0\rangle_0, E_0\rangle \langle 0, E_0| + |1, E_1\rangle_1, E_1\rangle_T + |1, E_2\rangle_2, E_2\rangle + |1, E_3\rangle_3, E_3\rangle_A'),$$

$$+ \frac{1}{2}|1\rangle_H \otimes (|0, E_0\rangle_0, E_0\rangle \langle 0, E_0| + |1, E_2\rangle_2, E_2\rangle + |1, E_3\rangle_3, E_3\rangle_A')$$ \hspace{1cm} (6)

Here, $|E_0\rangle, |E_1\rangle, |E_2\rangle,$ and $|E_3\rangle$ are pure states determined by $U_1$. $A'$ means the qubit of Alice after TP’s attack and it will be received by Bob.

3) Bob measures and resends the received qubit. The system transforms to

$$\rho_3 = \frac{1}{2}|00\rangle_{HA} \otimes (|0, E_0\rangle_0, E_0\rangle \langle 0, E_0| + |1, E_1\rangle_1, E_1\rangle_B + |1, E_2\rangle_2, E_2\rangle + |1, E_3\rangle_3, E_3\rangle_B),$$

$$+ \frac{1}{2}|11\rangle_{HA} \otimes (|0, E_0\rangle_0, E_0\rangle \langle 0, E_0| + |1, E_2\rangle_2, E_2\rangle + |1, E_3\rangle_3, E_3\rangle_B),$$ \hspace{1cm} (7)

where $B$ denotes Bob’s measurement result. Then, TP launches her second attack. Specifically, she performs the $U_2$ operation on the Bob’s qubit and her auxiliary state $|E_k\rangle$. The effect of $U_2$ is as follows:

$$U_2 i, E_k = \sum_{j=0}^{1} |j, E_{i,k}\rangle,$$ \hspace{1cm} (8)

where $i, j \in \{0, 1\}$ and $k \in \{0, 1, 2, 3\}$. Thus, the system of Alice, Bob, and TP becomes

$$\rho_4 = \frac{1}{2} (|0000\rangle_{HABB'} \otimes |E_0^0\rangle \langle E_0^0|_T + |0001\rangle_{HABB'} \otimes |E_0^1\rangle \langle E_0^1|_T + + |0010\rangle_{HABB'} \otimes |E_1^0\rangle \langle E_1^0|_T + |0011\rangle_{HABB'} \otimes |E_1^1\rangle \langle E_1^1|_T + |1100\rangle_{HABB'} \otimes |E_0^0\rangle \langle E_0^0|_T + |1101\rangle_{HABB'} \otimes |E_0^1\rangle \langle E_0^1|_T + + |1110\rangle_{HABB'} \otimes |E_1^0\rangle \langle E_1^0|_T + |1111\rangle_{HABB'} \otimes |E_1^1\rangle \langle E_1^1|_T + + |1111\rangle_{HABB'} \otimes |E_1^1\rangle \langle E_1^1|_T),$$ \hspace{1cm} (9)
where $B'$ means the qubit received by TP.

4) TP uses the Bell basis to measure the received qubit $B'$ and qubit $H$ in her hand, and publishes the outcomes to Alice and Bob. Subsequently, according to the statement of TP and the qubits observed by Alice and Bob, it will get:

$$
\begin{align*}
p_{i,0} &= \langle E_{0,0}^i | E_{0,0}^0 \rangle, \quad p_{i,1} = \langle E_{0,1}^i | E_{0,1}^0 \rangle, \\
p_{0,i} &= \langle E_{0,0}^0 | E_{0,1}^i \rangle, \quad p_{1,i} = \langle E_{0,2}^0 | E_{0,1}^i \rangle, \\
p_{i,2} &= \langle E_{0,2}^i | E_{0,2}^0 \rangle, \quad p_{i,3} = \langle E_{0,2}^i | E_{0,1}^0 \rangle,
\end{align*}
$$

(10)

where $p_{i,j}$ means the probability that the qubits $B'$ and $H$ are consistent (i.e., TP’s statement is $|\phi^+\rangle$ or $|\phi^-\rangle$), and the qubits observed by Alice and Bob are $|i\rangle$ and $|j\rangle$, while $p_{i,j}'$ represents the probability that the qubits $B'$ and $H$ are inconsistent, and the qubits observed by Alice and Bob are $|i\rangle$ and $|j\rangle$.

However, Alice and Bob only accept the event where TP announces $|\phi^+\rangle$ or $|\phi^-\rangle$. Conditioning on this event and tracing out $B'$ and $H$, the final contributing raw key system is

$$
\rho_{ABT} = \frac{1}{N} (|00\rangle_{AB} \otimes |E_{0,0}^0 \rangle_{TF} \langle E_{0,0}^0 \rangle_{T} \\
+ |01\rangle_{AB} \otimes |E_{0,1}^0 \rangle_{TF} \langle E_{0,1}^0 \rangle_{T} \\
+ |10\rangle_{AB} \otimes |E_{0,2}^0 \rangle_{TF} \langle E_{0,2}^0 \rangle_{T} \\
+ |11\rangle_{AB} \otimes |E_{0,3}^0 \rangle_{TF} \langle E_{0,3}^0 \rangle_{T}),
$$

(11)

where $N$ is the normalization term: $N = \langle E_{0,0}^0 | E_{0,0}^0 \rangle + \langle E_{0,1}^0 | E_{0,1}^0 \rangle + \langle E_{0,2}^0 | E_{0,2}^0 \rangle + \langle E_{0,3}^0 | E_{0,3}^0 \rangle$. Let $p_{i,j}$ denote the probability that Alice and Bob’s raw keys are $i$ and $j$. From (11), we have

$$
\begin{align*}
p_{0,0} &= \frac{1}{N} \langle E_{0,0}^0 | E_{0,0}^0 \rangle, \quad p_{0,1} = \frac{1}{N} \langle E_{0,1}^0 | E_{0,1}^0 \rangle, \\
p_{1,0} &= \frac{1}{N} \langle E_{0,2}^0 | E_{0,2}^0 \rangle, \quad p_{1,1} = \frac{1}{N} \langle E_{0,3}^0 | E_{0,3}^0 \rangle.
\end{align*}
$$

(12)

TP may obtain the raw keys by observing the states of her auxiliary state. Recall the definition of the key rate, as long as $r = S(A|T) - H(A|B) > 0$, a secure secret key can be distilled. Thus, in the next step, we have to calculate the range of $r$.

### 3.1.2 Key rate derivation

Obviously, the calculation of $H(A|B)$ is simple. According to the (12), $H(A|B)$ is calculated:

$$
H(A|B) = H(A, B) - H(B) = H(p_{0,0}, p_{0,1}, p_{1,0}, p_{1,1}) - H(p_{0,0} + p_{1,0}, p_{1,1} + p_{0,1}).
$$

(13)

To bound $S(A|T)$, we introduce a new auxiliary system $F$ to simplify the calculation process. According to the strong sub additivity, we have $S(A|T) \geq S(A|TF)$. Thereby, we can obtain a lower bound of $r$

$$
r = S(A|T) - H(A|B) \geq S(A|TF) - H(A|B).
$$

(14)

The new system $F$ is spanned by $\{|C\rangle, |W\rangle\}$, where $|C\rangle$ means the raw key of Alice and Bob is consistent, while $|W\rangle$ represents their raw key is not consistent. Then the new mixed system is:

$$
\rho_{ABTF} = \frac{1}{N} (|00\rangle_{AB} \otimes |E_{0,0}^0 \rangle_{TF} \langle E_{0,0}^0 \rangle_{T} \otimes |C\rangle \langle C|_F \\
+ |01\rangle_{AB} \otimes |E_{0,1}^0 \rangle_{TF} \langle E_{0,1}^0 \rangle_{T} \otimes |W\rangle \langle W|_F \\
+ |10\rangle_{AB} \otimes |E_{0,2}^0 \rangle_{TF} \langle E_{0,2}^0 \rangle_{T} \otimes |W\rangle \langle W|_F \\
+ |11\rangle_{AB} \otimes |E_{0,3}^0 \rangle_{TF} \langle E_{0,3}^0 \rangle_{T} \otimes |C\rangle \langle C|_F),
$$

(15)

Tracing out $B$ from $\rho_{ABTF}$, $\rho_{ATF}$ can be written as a diagonal matrix, where the elements are $p_{i,j}$. Thereby:

$$
S(ATF) = S(\rho_{ATF}) = H(p_{0,0}, p_{0,1}, p_{1,0}, p_{1,1}).
$$

(16)
Next, we calculate $S(TF)$. Tracing out $A$ and $B$ from $\rho_{ABTF}$ yields:

$$
\rho_{TF} = \frac{1}{N}(|E^0_{0,0}\rangle\langle E^0_{0,0}| + |E^1_{1,3}\rangle\langle E^1_{1,3}|) \otimes |C\rangle\langle C|_{F}
+ \frac{1}{N}(|E^0_{1,1}\rangle\langle E^0_{1,1}| + |E^0_{0,2}\rangle\langle E^0_{0,2}|) \otimes |W\rangle\langle W|_{F}.
$$

(17)

Let $\xi_1 = \frac{1}{N}(|E^0_{0,0}\rangle \langle E^0_{0,0}| + |E^1_{1,3}\rangle \langle E^1_{1,3}|) = p_{0,0} + p_{1,1}$, $\xi_2 = \frac{1}{N}(|E^0_{1,1}\rangle \langle E^1_{1,1}| + |E^0_{0,2}\rangle \langle E^0_{0,2}|) = p_{0,1} + p_{1,0}$. Then (17) can be rewritten as

$$
\rho_{TF} = \xi_1 |C\rangle\langle C|_{F} + \xi_2 |W\rangle\langle W|_{F},
$$

(18)

where

$$
\sigma_1 = \frac{|E^0_{0,0}\rangle\langle E^0_{0,0}| + |E^1_{1,3}\rangle\langle E^1_{1,3}|}{|E^0_{0,0}\rangle\langle E^0_{0,0}| + |E^1_{1,3}\rangle\langle E^1_{1,3}|}, \quad \sigma_2 = \frac{|E^0_{1,1}\rangle\langle E^1_{1,1}| + |E^0_{0,2}\rangle\langle E^0_{0,2}|}{|E^1_{1,1}\rangle\langle E^1_{1,1}| + |E^0_{0,2}\rangle\langle E^0_{0,2}|}.
$$

(19)

According to the joint entropy theorem of Von Neumann entropy (For detailed proof, see [6]), $S(\rho_{TF})$ can be derived as

$$
S(TF) = S(\rho_{TF}) = H(p_{0,0} + p_{1,1}, p_{0,1} + p_{1,0}) + (p_{0,0} + p_{1,1})S(\sigma_1) + (p_{0,1} + p_{1,0})S(\sigma_2).
$$

(20)

Since $\sigma_1$ and $\sigma_2$ are two-dimensional systems, we have $S(\sigma_1) \leq 1$ and $S(\sigma_2) \leq 1$. Thus, the upper bound of $S(TF)$ can be calculated as follow:

$$
S(TF) \leq H(p_{0,0} + p_{1,1}, p_{0,1} + p_{1,0}) + (p_{0,0} + p_{1,1})S(\sigma_1) + (p_{0,1} + p_{1,0})S(\sigma_2).
$$

(21)

Let $|E^0_{0,0}\rangle = \alpha|0\rangle$ and $|E^1_{1,3}\rangle = \beta|1\rangle + \theta|\zeta\rangle$, where $|\zeta\rangle = \langle \zeta | = 1$ and $\langle h|\zeta\rangle = 0$. Then, we have

$$
|E^0_{0,0}\rangle = |\alpha|^2, \quad |E^1_{1,3}| = ||\beta||^2 + ||\theta||^2, \quad \text{and} \quad |E^1_{1,3}, \sigma_3 = \alpha^\ast \beta. \quad \text{Thus},
$$

$\sigma_1$ can be described as

$$
\sigma_1 = \frac{1}{N^2 - \xi_1} \left( ||\alpha||^2 + ||\beta||^2 + \beta^\ast \theta^* \right). \quad \text{such that}
$$

(22)

After that the eigenvalues of $\sigma_1$ can be calculated as

$$
\lambda_\pm = \frac{1}{2} \pm \frac{1}{2N^2 - \xi_1} \sqrt{N^4 (p_{0,0} - p_{1,1})^2 + 4|E^0_{0,0}|^2 |E^1_{1,3}|^2}.
$$

(23)

Thus, $\lambda_+ - \lambda_- = H(\lambda_+, \lambda_-)$. Using (14), (16), and (21), the key rate is simplified as

$$
r \geq S(A|TF) - H(A|B) \geq H(p_{0,0} + p_{1,0}, p_{0,1} + p_{1,1}) - p_{0,1} - p_{1,0} - (p_{0,0} + p_{1,1})S(\sigma_1) - H(p_{0,0} + p_{1,1}, p_{0,1} + p_{1,0}).
$$

(24)

What remains is to bound $S(\sigma_1)$. It’s not hard to see that $\lambda_+ \geq \frac{1}{2}$, and that $|E^0_{0,0}|^2 |E^1_{1,3}|^2$ decreases $S(\sigma_1)$ will increase. Therefore, to obtain a lower bound of $r$, we should identify a lower bound on $|E^0_{0,0}|^2 |E^1_{1,3}|^2$.

Observing the case that Alice and Bob both reflect the received qubit, we may bound $|E^0_{0,0}|^2 |E^1_{1,3}|^2$. Specifically, after TP’s attacks $U_1$ and $U_2$, the system will be

$$
U_2 U_1 |\phi^+\rangle |0\rangle_T = \frac{1}{2} \left[ |\phi^+\rangle (|F_5\rangle + |F_3\rangle) + |\phi^-\rangle (|F_6\rangle - |F_3\rangle) + |\psi^-\rangle (|F_1\rangle - |F_2\rangle) + |\psi^+\rangle (|F_1\rangle + |F_2\rangle) \right],
$$

(25)

where

$$
|F_5\rangle = |E^0_{0,0}\rangle + |E^1_{1,1}\rangle, \quad |F_1\rangle = |E^0_{0,0}\rangle + |E^1_{1,1}\rangle, \\
|F_6\rangle = |E^0_{1,2}\rangle + |E^0_{0,3}\rangle, \quad |F_3\rangle = |E^0_{1,2}\rangle + |E^0_{0,3}\rangle.
$$

(26)

Then, TP measures the qubits with Bell basis and announces her measurements. If the measurement is not $|\phi^+\rangle$, Alice and Bob know there is an error raised. Here, we use $p_{\phi^-}, p_{\phi^+},$ and $p_{\phi^-}$ to represent the probabilities that TP’s outcomes are $|\psi^-\rangle, |\psi^+\rangle,$ and $|\phi^-\rangle$, respectively. According to (25), it’s easy to get

$$
p_{\phi^-} = \frac{1}{4} \langle F_1 | F_1 \rangle - \frac{1}{2} \text{Re}(F_1 | F_2 \rangle) + \frac{1}{4} \langle F_2 | F_2 \rangle,
$$

(27)

$$
p_{\phi^+} = \frac{1}{4} \langle F_1 | F_1 \rangle + \frac{1}{2} \text{Re}(F_1 | F_2 \rangle) + \frac{1}{4} \langle F_2 | F_2 \rangle,
$$

$$
p_{\phi^-} = \frac{1}{4} \langle F_0 | F_0 \rangle - \frac{1}{2} \text{Re}(F_0 | F_3 \rangle) + \frac{1}{4} \langle F_3 | F_3 \rangle.
$$
Note that $U_1$ and $U_2$ are unitary, which means 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

$$p_{\phi^+} + p_{\phi^-} + p_{\phi^-} = 1 - \frac{1}{2} Re\langle F_0|F_3 \rangle - \frac{1}{4} (F_0|F_0 \rangle - \frac{1}{4} (F_3|F_3 \rangle. \quad (28)$$

Using (26) into (28), thus

$$Re\langle E_{0,0}^0|E_{1,3}^1 \rangle = 2 - 2(p_{\phi^+} + p_{\phi^-} + p_{\phi^-})
- Re((E_{0,0}^0|E_{0,2}^0) + \langle E_{1,1}^0|E_{1,3}^1 \rangle + \langle E_{1,1}^0|E_{1,3}^1 \rangle)
- \frac{1}{2} Re((E_{0,0}^0|E_{0,0}^0) + \langle E_{0,0}^0|E_{0,0}^0 \rangle + \langle E_{0,0}^0|E_{0,0}^0 \rangle + \langle E_{0,0}^0|E_{0,0}^0 \rangle)
- \frac{1}{2} Re((E_{0,2}^1|E_{0,2}^1) + \langle E_{1,3}^1|E_{1,3}^1 \rangle + \langle E_{1,3}^1|E_{1,3}^1 \rangle + \langle E_{1,3}^1|E_{1,3}^1 \rangle). \quad (29)$$

Then, according to the Cauchy-Schwarz inequality (i.e., $|Re\langle a|b \rangle| \leq |\langle a|b \rangle| \leq \sqrt{\langle a|a \rangle \langle b|b \rangle}$) and (10), the lower bound of $Re\langle E_{0,0}^0|E_{1,3}^1 \rangle$ can be obtained

$$Re\langle E_{0,0}^0|E_{1,3}^1 \rangle \geq 2 - 2(p_{\phi^+} + p_{\phi^-} + p_{\phi^-})
- \left(\sqrt{p_{0,0}^c p_{1,1}^c} + \sqrt{p_{0,0}^c p_{1,1}^c} + \sqrt{p_{0,0}^c p_{1,1}^c} \right)
- \frac{1}{2} \left(\sqrt{p_{0,0}^c p_{0,0}^c} + \sqrt{p_{0,1}^c p_{0,1}^c} + \sqrt{p_{0,1}^c p_{0,1}^c} \right)
- \frac{1}{2} \left(\sqrt{p_{1,0}^c p_{1,0}^c} + \sqrt{p_{1,1}^c p_{1,1}^c} + \sqrt{p_{1,1}^c p_{1,1}^c} \right). \quad (30)$$

From (23) and (30), we can bound $S(\sigma_1)$. So far, we have derived the bounds of $H(A|B)$, $S(ATF)$, and $S(TF)$ which depend on the probabilities observed in (10), (12) and (27). Hence, the key rate can be derived.

### 3.1.3 Key rate evaluation

The system’s errors (or noise) are all caused by the attacks from TP. Thus, we need to model the errors introduced by TP attacks. In particular, suppose that the errors introduced by TP’s attacks can be characterized as (This is a typical assumption applied to the security analysis):

1. Let $Q$ express the probability that Alice and Bob’s measurement results are different.
2. Let $Q_M$ represent the probability that TP announces the wrong message when Alice and Bob choose measurement. For example, they observe the same quantum state, but TP publishes $|\psi^+ \rangle$ or $|\psi^- \rangle$.
3. Let $Q_R$ represent the probability that TP announces the wrong result when Alice and Bob reflect the qubits. That is, $p_{\phi^+} + p_{\phi^-} + p_{\phi^-} = Q_R$

Note that the error rates for $Q$, $Q_M$, and $Q_R$ can be easily observed in this protocol. Thereby, (10) can be represented by $Q$ and $Q_M$ as follows

$$p_{\phi^+} = \frac{(1 - Q)(1 - Q),}{2(1 - Q)(1 - Q)} = Q_{M}, \quad p_{\phi^-} = \frac{(1 - Q)(1 - Q)}{2(1 - Q)(1 - Q) + 2QQ_{M}}, \quad p_{\phi^-} = \frac{(1 - Q)(1 - Q)}{2(1 - Q)(1 - Q) + 2QQ_{M}}. \quad (31)$$

Then (12) can be rewritten as

$$p_{0,0} = \frac{Q_{M}}{2(1 - Q)(1 - Q) + 2QQ_{M}}, \quad p_{0,1} = \frac{Q_{M}}{2(1 - Q)(1 - Q) + 2QQ_{M}}, \quad p_{1,0} = \frac{Q_{M}}{2(1 - Q)(1 - Q) + 2QQ_{M}}, \quad p_{1,1} = \frac{Q_{M}}{2(1 - Q)(1 - Q) + 2QQ_{M}}. \quad (32)$$

Moreover, (30) can be expressed as

$$Re\langle E_{0,0}^0|E_{1,3}^1 \rangle \geq 2 - 2Q_R - 4\sqrt{1 - Q)(1 - Q)QQ_{M}}
- 2QQ_{M} - (1 - Q)(1 - Q), \quad (33)$$
so that $S(\sigma_1)$ also can be denoted by $Q$, $Q_M$, and $Q_R$.

Fig. 2. Key rate of the proposed protocol when TP is semi-honest. This graph assumes the error rates of $Q_R$, $Q_M$, and $Q$ are equal, i.e., $Q_R = Q_M = Q$. Observe that the protocol can work with the noise of less than 16.02%.

3.2 The scenario of untrusted TP

In the above subsection, we discussed a particular scenario where TP is semi-honest. However, in practice, it is often not so ideal. Here, we consider the worst scenario where TP is untrusted. In this scenario, TP can do anything she likes, including preparing fake particles and publishing fake results.

3.2.1 The attack strategy of untrusted TP

TP is adversarial, so she unnecessarily follows the protocol description to prepare Bell state, but instead any arbitrary state $|\phi\rangle = \sum_{i=0}^{1} |i\rangle \otimes |g_i\rangle$, where the $|g_i\rangle$ are TP’s private ancilla and the normalized parameters of $|\phi\rangle$ are incorporated into $|g_i\rangle$. Similar to Sect. 3.1, we also first consider the case where Alice and Bob both measure and resend the received qubit. To obtain the raw key, TP’s attack strategy is modeled as follows (also see Fig. 3).

1) TP sends the qubit $|i\rangle$ to Alice. Then, Alice measures and resends the received qubit. Thus the density operator describing the system can be expressed as

$$\rho'_1 = |0\rangle\langle 0| \otimes |g_0\rangle\langle g_0| + |1\rangle\langle 1| \otimes |g_1\rangle\langle g_1|,$$

(34)

2) Then, TP executes the $V_1$ operation on the qubit from Alice and her auxiliary state, where $V_1|i,g_i\rangle = \sum_{j=0}^{1} |j,g_{i,j}\rangle$. Thus the system of Alice, transmitted qubit, and TP’s auxiliary qubit is

$$\rho'_2 = |00\rangle\langle 00|_{AA'} \otimes |g_{0,0}\rangle\langle g_{0,0}|_T + |01\rangle\langle 01|_{AA'} \otimes |g_{0,1}\rangle\langle g_{0,1}|_T$$

$$+ |10\rangle\langle 10|_{AA'} \otimes |g_{1,0}\rangle\langle g_{1,0}|_T + |11\rangle\langle 11|_{AA'} \otimes |g_{1,1}\rangle\langle g_{1,1}|_T,$$

(35)

where $A$ denotes Alice’s measurement result, $A'$ represents the state received by Bob, and $T$ means TP’s auxiliary state. After that, Bob measures and resends the received qubit. Then, the system
1) TP prepares a fake qubit instead of Bell state and sends the fake qubit to Alice.
2) TP launches her attack. She may obtain Alice and Bob's secret key by observing her auxiliary state.
3) TP performs an isometry mapping on the received qubits and her auxiliary state to obtain the fake message in the form of Bell states. Then she publishes this message to Alice and Bob.

Fig. 3. A diagram of untrusted TP’s attack strategy. TP can do anything she likes, including preparing fake particles and publishing fake results. TP may obtain the raw key by observing her auxiliary particles.

of Alice, Bob and TP is

$$\rho'_2 = |000\rangle\langle 000|_{ABB'} \otimes |g_{0,0}\rangle\langle g_{0,0}|_T$$
$$+ |011\rangle\langle 011|_{ABB'} \otimes |g_{0,1}\rangle\langle g_{0,1}|_T$$
$$+ |100\rangle\langle 100|_{ABB'} \otimes |g_{1,0}\rangle\langle g_{1,0}|_T$$
$$+ |111\rangle\langle 111|_{ABB'} \otimes |g_{1,1}\rangle\langle g_{1,1}|_T, \quad (36)$$

where $B$ denotes Bob’s measurement result, and $B'$ represents the state sent by Bob.

3) Then following the protocol steps, TP is required to post the message in the form of Bell states. This process can be modeled as an isometry mapping \[25,30\] on the qubit sent by Bob and her auxiliary state, where the isometry mapping $V_2$ is defined as

$$V_2 |j,g\rangle_{i,j} = \sum_{m=0}^{3} |m,g\rangle_{i,j}.$$ 

Thus the system can be expressed as

$$\rho'_4 = |00\rangle\langle 00|_{AB} \otimes \sum_{m=0}^{3} |m,g^m_{0,0}\rangle\langle m,g^m_{0,0}|_T$$
$$+ |01\rangle\langle 01|_{AB} \otimes \sum_{m=0}^{3} |m,g^m_{0,1}\rangle\langle m,g^m_{0,1}|_T$$
$$+ |10\rangle\langle 10|_{AB} \otimes \sum_{m=0}^{3} |m,g^m_{1,0}\rangle\langle m,g^m_{1,0}|_T$$
$$+ |11\rangle\langle 11|_{AB} \otimes \sum_{m=0}^{3} |m,g^m_{1,1}\rangle\langle m,g^m_{1,1}|_T. \quad (37)$$

TP can observe the value of $m$ to obtain the message published to Alice and Bob, where $m = 0, 1, 2, 3$ represents that the message published by TP is $|\phi^+\rangle$, $|\phi^-\rangle$, $|\psi^+\rangle$ and $|\psi^-\rangle$, respectively.

However, Alice and Bob only accept the event where TP’s measurement result is $|\phi^+\rangle$ or $|\phi^-\rangle$. That is, $m = 0, 1$. Conditioning on this event, thus the final contributing raw key system is

$$\rho'_{ABT} = \frac{1}{N^'} \sum_{i,j \in \{0,1\}} |i,j\rangle\langle i,j|_{AB} \otimes \sum_{m=0}^{1} |g^m_{i,j}\rangle\langle g^m_{i,j}|_T, \quad (38)$$

where $N'$ is the normalization term: $N' = \sum_{i,j \in \{0,1\}} |g^0_{i,j}\rangle\langle g^0_{i,j}| + |g^1_{i,j}\rangle\langle g^1_{i,j}|$. Then, TP may obtain the raw keys by observing the states of her auxiliary state.

Let $p_{i,j}^m_0$ be the probability that TP sends message ‘$m$’ and Alice and Bob’s measurement results
are \( i \) and \( j \). From (38), we have

\[
\begin{align*}
\rho_{0,0}^0 &= \langle g_{0,0}^0 | g_{0,0}^0 \rangle, \\
\rho_{0,1}^0 &= \langle g_{0,1}^0 | g_{0,1}^0 \rangle, \\
\rho_{1,0}^0 &= \langle g_{1,0}^0 | g_{1,0}^0 \rangle, \\
\rho_{1,1}^0 &= \langle g_{1,1}^0 | g_{1,1}^0 \rangle, \\
p_{0,0}^1 &= \langle g_{0,0}^1 | g_{0,0}^1 \rangle, \\
p_{0,1}^1 &= \langle g_{0,1}^1 | g_{0,1}^1 \rangle, \\
p_{1,0}^1 &= \langle g_{1,0}^1 | g_{1,0}^1 \rangle, \\
p_{1,1}^1 &= \langle g_{1,1}^1 | g_{1,1}^1 \rangle.
\end{align*}
\]

(39)

Note that the probabilities of \( p_{i,i}^0 \) and \( p_{i,i}^1 \) is higher than \( p_{i,1-i} \) (\( i = 0, 1 \)); otherwise, there is too much error, and Alice and Bob will abort. Next, let \( q_{i,j} \) represent the probability that Alice’s and Bob’s raw keys are \( i \) and \( j \). It’s not hard to see that

\[
q_{i,j} = \frac{1}{N} (p_{i,j}^0 + p_{i,j}^1).
\]

(40)

### 3.2.2 Key rate derivation

We have derived the final contributing raw key system \( \rho_{AT}’ \). According to the definition of key rate, as long as \( r = S(A|T) - H(A|B) > 0 \), a secure key can be obtained. To compute the key rate \( r \), we need a bound of the entropy \( S(A|T) \) and \( H(A|B) \). Obviously, the latter is easy to obtain. Based to the value of \( q_{i,j} \), \( H(A|B) \) can be calculated as follows.

\[
H(A|B) = H(q_{0,0}, q_{0,1}, q_{1,0}, q_{1,1}) - H(q_{0,0} + q_{1,0}, q_{0,1} + q_{1,1}).
\]

(41)

Then, we need to bound the entropy \( S(A|T) \). It is more challenging to calculate \( S(A|T) \) in the case that TP is untrusted than in the semi-honest scenario. Unlike the approach adopted in the previous subsection, we will use the following theorem from [25]:

**Theorem 1** Given a quantum state \( \rho_{AT}^* \) of the form:

\[
\rho_{AT}^* = \frac{1}{N} \left( |0\rangle\langle 0|_A \otimes \sum_{i=0}^{m} |E_i\rangle\langle E_i| + |1\rangle\langle 1|_A \otimes \sum_{i=0}^{m} |F_i\rangle\langle F_i| \right),
\]

where \( N > 0 \) is a normalization term. Then, it holds that:

\[
S(A|T)_{\rho} \geq \sum_{i=0}^{m} \left( \frac{|\langle E_i|E_i\rangle + |F_i|F_i\rangle}{N} \right) \cdot \left( h \left( \frac{\langle E_i|E_i\rangle}{|\langle E_i|E_i\rangle + |F_i|F_i\rangle} \right) - h(\lambda_i) \right)
\]

(43)

where:

\[
\lambda_i = \frac{1}{2} + \frac{\sqrt{(\langle E_i|E_i\rangle - |F_i|F_i\rangle)^2 + 4Re^2(E_i|F_i\rangle)}}{2(|\langle E_i|E_i\rangle + |F_i|F_i\rangle)}.
\]

(44)

Here, \( h(x) \) means the binary Shannon entropy, i.e., \( h(x) = -x\log_2 x - (1-x)\log_2(1-x) \).

For the detailed proof process, the reader is referred to [25]. From (38), we can obtain \( \rho_{AT}' \) by tracing out \( B \) from \( \rho_{AT}^* \).

\[
\rho_{AT}' = \frac{1}{N'} \left( |0\rangle\langle 0|_A \otimes \sum_{m,j=0}^{1} |g_{0,j}^m\rangle\langle g_{0,j}^m|_T + |1\rangle\langle 1|_A \otimes \sum_{m,j=0}^{1} |g_{1,j}^m\rangle\langle g_{1,j}^m|_T \right)
\]

(45)

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

\[
S(A|T)_{\rho} \geq \sum_{i,j,m} \left( \frac{|\langle g_{0,j}^m|g_{0,j}^m\rangle + |g_{1,1-j}^m|g_{1,1-j}^m\rangle}{N'} \right) \cdot \left( h \left( \frac{|\langle g_{0,j}^m|g_{0,j}^m\rangle}{|\langle g_{0,j}^m|g_{0,j}^m\rangle + |g_{1,1-j}^m|g_{1,1-j}^m\rangle} \right) - h(\lambda_{j,m}) \right),
\]

(46)

where

\[
\lambda_{j,m} = \frac{1}{2} + \frac{\sqrt{(\langle g_{0,j}^m|g_{0,j}^m\rangle - |g_{1,1-j}^m|g_{1,1-j}^m\rangle)^2 + 4Re^2(g_{0,j}^m|g_{1,1-j}^m\rangle)}}{2(|\langle g_{0,j}^m|g_{0,j}^m\rangle + |g_{1,1-j}^m|g_{1,1-j}^m\rangle)}.
\]

(47)
According to the Cauchy-Schwarz inequality, we have
\[ A \leq B \implies 2\langle A | B \rangle \leq \langle A | A \rangle \langle B | B \rangle. \]
This provides a way to bound \( \Re \langle g_{0,j}^m | g_{1,j}^m \rangle \). Specifically, Alice and Bob both reflect the qubit directly, so the whole transmission process can be modeled as
\[
\begin{align*}
V_2 V_1 (|0\rangle \otimes |g_0\rangle + |1\rangle \otimes |g_1\rangle) & = V_2 (|0\rangle \otimes |g_{0,0}\rangle + |1\rangle \otimes |g_{1,0}\rangle + |0\rangle \otimes |g_{1,1}\rangle + |1\rangle \otimes |g_{1,1}\rangle) \\
& = \sum_{m=0}^{3} |m\rangle \otimes (|g_{0,0}^m\rangle + |g_{0,1}^m\rangle + |g_{1,0}^m\rangle + |g_{1,1}^m\rangle). 
\end{align*}
\] (48)

According the value of \( m \), TP then announces the message in the form of Bell states. If the message is not \( |\varphi^+\rangle \), Alice and Bob know there is an error introduced. We first discuss the case that TP announces \( |\varphi^-\rangle \), i.e., \( m = 1 \) (the case of \( m = 0 \) is similar).

From (48), the probability that TP announces \( |\varphi^-\rangle \) can be estimated:
\[
p_{\varphi^-} = \left| \sum_{i,j} \langle g_{i,j}^1 | g_{i,j}^1 \rangle - \sum_{i,j} \langle g_{i,j}^0 | g_{i,j}^0 \rangle \right|.
\] (49)

This provides a way to bound \( \Re \langle g_{0,0}^1 | g_{1,1}^1 \rangle \) and \( \Re \langle g_{1,0}^1 | g_{1,0}^1 \rangle \). After some algebra, we have
\[
\left| p_{\varphi^-} - \sum_{i,j} \langle g_{i,j}^1 | g_{i,j}^1 \rangle \right| = \left| \frac{2\Re \langle g_{0,0}^1 | g_{1,1}^1 \rangle + 2\Re \langle g_{0,0}^1 | g_{1,0}^1 \rangle + 2\Re \langle g_{0,1}^1 | g_{1,0}^1 \rangle}{+ 2\Re \langle g_{1,0}^1 | g_{1,0}^1 \rangle + 2\Re \langle g_{1,1}^1 | g_{1,1}^1 \rangle} \right| .
\] (50)

According to the Cauchy-Schwarz inequality, we have \( \Re \langle g_{0,0}^1 | g_{1,1}^1 \rangle \leq \sqrt{\langle g_{0,0}^1 | g_{0,0}^1 \rangle \langle g_{1,1}^1 | g_{1,1}^1 \rangle} \) and \( \Re \langle g_{0,1}^1 | g_{1,0}^1 \rangle \leq \sqrt{\langle g_{0,1}^1 | g_{0,1}^1 \rangle \langle g_{1,0}^1 | g_{1,0}^1 \rangle} \). In general the values of \( \langle g_{0,0}^1 | g_{0,0}^1 \rangle \) and \( \langle g_{1,1}^1 | g_{1,1}^1 \rangle \) are higher than \( \langle g_{0,1}^1 | g_{0,1}^1 \rangle \) and \( \langle g_{1,0}^1 | g_{1,0}^1 \rangle \); otherwise, there is too much error, and Alice and Bob will abort. Therefore, the value of \( \Re \langle g_{0,0}^1 | g_{1,1}^1 \rangle \) is generally greater than \( \Re \langle g_{0,1}^1 | g_{1,0}^1 \rangle \). Let \( \Re \langle g_{0,1}^1 | g_{1,0}^1 \rangle = \sqrt{\langle g_{0,1}^1 | g_{0,1}^1 \rangle \langle g_{1,0}^1 | g_{1,0}^1 \rangle} \), then we focus on bounding \( \Re \langle g_{0,0}^1 | g_{1,1}^1 \rangle \). Following the Cauchy-Schwarz inequality and Absolute value inequality, we can obtain the range of \( \Re \langle g_{0,0}^1 | g_{1,1}^1 \rangle \)
\[
\Re \langle g_{0,0}^1 | g_{1,1}^1 \rangle \geq \left| \frac{1}{2} p_{\varphi^-} - \frac{1}{2} \sum_{i,j} \langle g_{i,j}^1 | g_{i,j}^1 \rangle - \sqrt{\langle g_{0,0}^1 | g_{0,0}^1 \rangle \langle g_{1,1}^1 | g_{1,1}^1 \rangle} \right|
- \sqrt{\langle g_{0,1}^1 | g_{0,1}^1 \rangle \langle g_{1,0}^1 | g_{1,0}^1 \rangle} - \sqrt{\langle g_{1,1}^1 | g_{1,1}^1 \rangle \langle g_{0,0}^1 | g_{0,0}^1 \rangle}.
\] (51)

where \( \langle g_{i,j}^1 | g_{i,j}^1 \rangle \) for \( i, j \in \{0, 1\} \) can be estimated in (39), and \( p_{\varphi^-} \) can be estimated by Alice and Bob. Following this fact, we have obtained the bounds of \( \Re \langle g_{0,0}^1 | g_{1,1}^1 \rangle \) and \( \Re \langle g_{0,1}^1 | g_{1,0}^1 \rangle \).

For the case that TP announces \( |\varphi^+\rangle \), i.e., \( m = 0 \), we can adopt the same method to derive the bounds of \( \Re \langle g_{0,0}^0 | g_{1,1}^0 \rangle \) and \( \Re \langle g_{0,1}^0 | g_{1,0}^0 \rangle \). So far, we have derived the bounds of \( \Re \langle g_{0,0}^1 | g_{1,1}^1 \rangle \), \( \Re \langle g_{0,1}^1 | g_{1,0}^1 \rangle \), \( \Re \langle g_{0,0}^0 | g_{1,1}^0 \rangle \), and \( \Re \langle g_{0,1}^0 | g_{1,0}^0 \rangle \), which depend on the parameters available to Alice and Bob. Naturally, we can obtain the value of \( S(A|T) \) and \( H(A|B) \). Hence, the key rate under the case that TP is untrusted can be derived.

### 3.2.3 Key rate evaluation

Same as in Sect. 3.1.3, the errors introduced by TP’s attacks can be characterized by the parameters \( Q_M \) and \( Q_R \); and these parameters may be easily observed by users. Then, we will use these parameters to represent \( \langle g_{0,j}^m | g_{1,j}^m \rangle \) and \( \Re \langle g_{0,j}^m | g_{1,j}^m \rangle \).

Here, we use \( \langle g_{0,0}^1 | g_{0,0}^1 \rangle \) as an example. In more detail, the probability that Alice and Bob measure the same result is \( 1 - Q \), while the probability that TP announces \( |\varphi^-\rangle \) (i.e., \( m = 1 \))
\[ \frac{1}{2}(1 - Q_M) \] when Alice and Bob both measure. Thus, we have \( \langle g^1_{0,0} | g^0_{0,0} \rangle = \frac{1}{2}(1 - Q)(1 - Q_M) \). It is not difficult to see (39) can be expressed as

\[ p^0_{0,0} = \langle g^0_{0,0} | g^0_{0,0} \rangle = p^0_{0,0} = \langle g^1_{0,0} | g^1_{0,0} \rangle = \frac{1}{2}(1 - Q)(1 - Q_M), \]

\[ p^0_{i,1} = \langle g^0_{i,1} | g^0_{i,1} \rangle = p^0_{i,1} = \langle g^1_{i,1} | g^1_{i,1} \rangle = \frac{1}{2} Q M, \]

\[ p^1_{1,0} = \langle g^1_{1,0} | g^0_{1,0} \rangle = p^1_{0,0} = \langle g^1_{1,0} | g^0_{1,0} \rangle = \frac{1}{2} Q M, \]

\[ p^1_{1,1} = \langle g^1_{1,1} | g^1_{i,1} \rangle = p^1_{1,1} = \langle g^1_{1,1} | g^1_{1,1} \rangle = \frac{1}{2}(1 - Q)(1 - Q_M). \]

Then (40) can be rewritten as

\[ q_{0,0} = \frac{(1 - Q)(1 - Q_M)}{2(1 - Q)(1 - Q_M) + 2QQ_M}, \quad q_{0,1} = \frac{QQ_M}{2(1 - Q)(1 - Q_M) + 2QQ_M}, \]

\[ q_{1,0} = \frac{QQ_M}{2(1 - Q)(1 - Q_M) + 2QQ_M}, \quad q_{1,1} = \frac{(1 - Q)(1 - Q_M)}{2(1 - Q)(1 - Q_M) + 2QQ_M}. \]

\[ Re\langle g^m_{0,j} | g^m_{1,1-j} \rangle \] for \( j, m = 0, 1 \) can also be denoted by \( Q, Q_M, \) and \( Q_R \). We use \( \langle g^1_{0,0} | g^1_{1,1} \rangle \) as an example for illustration, and other cases can be obtained by analogy. Applying (52) into (51), we have

\[ \langle g^1_{0,0} | g^1_{1,1} \rangle \geq \left| \frac{1}{2} \left[ (1 - Q)(1 - Q_M) + QQ_M \right] - \frac{1}{2} p_{\psi^-} \right| - 2\sqrt{(1 - Q)(1 - Q_M)QQ_M} - \frac{1}{2} QQ_M, \]

where \( p_{\psi^-} \) can be obtained by \( Q_R \). Recall the definition of \( Q_R = p_{\psi^+} + p_{\psi^-} + p_{\phi^-} \). To simplify the calculation, we assume that the probability of different errors is the same, that is, \( p_{\psi^+} = p_{\psi^-} = p_{\phi^-} = \frac{1}{2} Q_R \). Hence, \( r = S(A|T) - H(A|B) \) can be denoted by \( Q, Q_M, \) and \( Q_R \).

To better compare with other similar protocols later, we assume that \( Q = Q_M = Q_R \). Integrating everything into the (41) and (46), the key rate \( r \) can be estimated by the variable \( Q \). As shown in Fig. 4, in the worst case, the noise tolerated by our protocol can reach 13.19%, which is better than the BB84 protocol’s 11% [2].

![Fig. 4](image-url) A diagram of our protocol’s key rate when TP is untrusted. Observe that the protocol can work with the noise of less than 13.19%.

12
4 Performance analysis and Comparison

Here, we evaluate the performance of our protocol in terms of noise tolerance, qubit efficiency, communication cost, and scalability.

As an essential indicator of the semi-quantum protocol, noise tolerance is the focus of our attention. In the above analysis, we have given the noise tolerance of the protocol under different conditions, respectively. In particular, if TP is semi-honest (i.e., TP follows the protocol description thoroughly, but otherwise, she can do anything she likes), our protocol’s noise tolerance is 16.02%. If TP is untrusted (TP can do anything she wants, including preparing fake particles and publishing fake results), our protocol’s noise tolerance can reach 13.19%, which is better than the BB84 protocol’s 11%. The results show that our M-SQKD protocol has similar security as the full quantum protocol.

Qubit efficiency is defined as the ratio of the number of raw keys to the total number of qubits consumed [28]. The previous protocols mainly considered the noiseless case when calculating qubit efficiency [24–32]. To better highlight the advantages and disadvantages of qubit efficiency between different protocols, this paper will calculate the qubit efficiency under noiseless conditions. In this paper, generating 1-bit raw key, TP should prepare 4 Bell states in the form of $|\phi^+\rangle$, and two “classical” users, Alice and Bob, need to prepare 2 qubits to substitute their measured qubits, respectively. Following this, our protocol’s qubit efficiency is $\frac{1}{12}$.

Communication cost is also a metric to evaluate protocol performance. It refers to the number of qubits that need to be transmitted to generate one bit of the raw key [13]. The transmission of qubits in our protocol is from TP to Alice, to Bob, and then back to TP. Thus, for producing a 1-bit raw key, four qubits (TP should prepare 4 Bell states and send the second qubit of these Bell states to Alice) need to be transmitted three times between TP, Alice, and Bob. That is, 12 qubits are transmitted for the whole process.

Lastly, we consider scalability as one of the protocol performance metrics. If a protocol has good scalability, there is no doubt that it will be applicable to more scopes and scenarios. Due to the characteristics of the circular transport structure, our protocol is well scalable and can be easily extended to more than two “classical” users’ key distribution scenarios (which will be described in the next subsection).

For clarity, we compare similar M-SQKD protocols [24–28,30] from the above aspects. A detailed comparison is shown in Table 1. It’s clear from the table that our protocol’s noise tolerance is close to previous protocols, and our protocol can be applied to more than two “classical” user scenarios, while previous protocols are only applicable to two “classical” user scenarios. In addition, our protocol still has some advantages in terms of qubit efficiency and communication cost.

| Noise tolerance under untrusted TP | Qubit efficiency | Communication cost | Scalability |
|-----------------------------------|-----------------|-------------------|-------------|
| Ref. [24] 10.65%                  | $\frac{1}{24}$  | 32-qubits         | ×           |
| Ref. [25] 13.04%                  | $\frac{1}{24}$  | 32-qubits         | ×           |
| Ref. [26] /                       | $\frac{1}{12}$  | 24-qubits         | ×           |
| Ref. [27] /                       | $\frac{1}{24}$  | 32-qubits         | ×           |
| Ref. [28] /                       | $\frac{1}{5}$   | 12-qubits         | ✓           |
| Ref. [30] 9.1%                    | $\frac{1}{12}$  | 16-qubits         | ×           |
| Our protocol 13.19%               | $\frac{1}{12}$  | 12-qubits         | ✓           |

Note that Refs. [26–28] only give security analysis under several specific attacks and no noise tolerance is calculated for such protocols.

5 Extention of the protocol to multi-party scenarios

Our protocol adopts the circular transport structure. The advantage of this structure is that it makes the protocol very flexible. Following this fact, our protocol can be easily expanded to multi-party scenarios, allowing the key distribution between more than two “classical” users. Therefore, it can be successfully used for multi-party M-SQKD and multi-party SQKD.
5.1 The multi-party M-SQKD protocol

Our protocol can be developed into a multi-party M-SQKD protocol involving \( L \) users. We use \( C_1, C_2, \ldots, C_L \) to denote these “classical” users. Only TP is a fully quantum user in this protocol, while other users are both “classical” whose quantum power is limited. The specific steps are as follows.

**Step 1:** TP prepares \( 2^{L+1}(N + \delta) \) Bell states in the form of \(|\phi^+\rangle\), where \( \delta \) is a fixed parameter. Then she sends the second qubit of each Bell state to \( C_1 \).

**Step 2:** For \( l = 1, 2, \ldots, L - 1 \) : \( C_l \) randomly decides to reflect the qubit to \( C_{l+1} \) or measure and resend the qubit to \( C_{l+1} \).

**Step 3:** Upon receiving qubit from \( C_{L-1} \), \( C_L \) randomly chooses to reflect it to TP or measure and resend it to TP.

**Step 4:** TP adopts the Bell basis to measure the received qubits and those left in her hands. Then, TP announces her measurement results to \( C_1, C_2, \ldots, C_L \).

**Step 5:** After TP releases her measurements, \( C_1, C_2, \ldots, C_L \) publish their choices through the authenticated classical channel.

a) If all \( C_1, C_2, \ldots, C_L \) reflect the received qubit, TP should always get \(|\phi^+\rangle\). This case is used for checking TP’s honesty and eavesdropping. When the error rate of this case surpasses the threshold, the protocol ends.

b) If all \( C_1, C_2, \ldots, C_L \) measure and resend the received qubit, \( C_1, C_2, \ldots, C_L \) will use these measurement results as their raw keys when TP’s announcement is \(|\phi^+\rangle\) or \(|\phi^-\rangle\).

c) If their operations are inconsistent, \( C_1, C_2, \ldots, C_L \) will discard these qubits.

**Step 6:** \( C_1, C_2, \ldots, C_L \) randomly pick out a small subset to publish their measurement results for eavesdropping detection. Once the error rate is over the threshold, the protocol ends. If not, the protocol continues.

**Step 7:** After the classical post-processing, the “classical” users \( C_1, C_2, \ldots, C_L \) can obtain the final secure key.

5.2 The multi-party SQKD protocol

The previous subsection gave detailed steps for the multi-party M-SQKD protocol. In this part, we can extend the protocol to a multi-party SQKD protocol by slightly changing the steps. Note that in the SQKD protocol, the quantum user is fully trusted, so here we redefine TP, which is trusted in this protocol. The revised steps are detailed below, while others are the same as described in Sect. 5.1.

**Step 4*:** After confirming that TP has obtained the qubits, \( C_1, C_2, \ldots, C_L \) publish their choices through the authenticated classical channel.

**Step 5*:** TP performs different operations according to the following cases:

- (i) If all \( C_1, C_2, \ldots, C_L \) reflect the received qubit, TP will measure the received qubit and the qubit in her hand with the Bell basis. This case is used for checking the eavesdropping. Once the error rate of this case surpasses the threshold, the protocol ends.

- (ii) If all \( C_1, C_2, \ldots, C_L \) measure and resend the received qubit, TP will measure the received qubit with Z basis. This case will be used for generating the raw keys.

- (iii) If \( C_1, C_2, \ldots, C_L \) choose different operations, this case will be discarded.

**Step 7*:** After the classical post-processing, TP and \( C_1, C_2, \ldots, C_L \) can obtain the final secret key.

In this section, we extend the protocol to multi-party M-SQKD and multi-party SQKD protocols. The results show that the protocol has good scalability to enable key distribution among multiple classical users.
6 Conclusion

In this paper, we design a scalable mediated semi-quantum key distribution protocol, which allows more than two “classical” users to establish a secret key with the help of an adversarial TP. Then, we give a detailed security proof to show the security of this circular M-SQKD protocol. By utilizing the parameters observed in the channel, a lower bound of the protocol’s key rate and noise tolerance can be derived. The classical users can distill a secure key when the noise is less than the threshold value. Indeed, even if TP is untrusted, our protocol’s noise tolerance is better than the BB84 protocol. That is, our protocol holds similar security to a fully quantum one. Compared with previous M-SQKD protocols, our protocol has comparable noise tolerance and advantages in qubit efficiency and communication cost. In addition, our protocol can work on more than two “classical” user scenarios, while previous protocols are only applicable to two “classical” user scenarios. Due to these features, this protocol may have potential applications in future quantum communications.

Acknowledgments This work was supported by the Open Research Fund of Key Laboratory of Cryptography of Zhejiang Province No. ZCL21006, and the BUPT Excellent Ph.D. Students Foundation No. CX2021117.

References

[1] C. H. Bennet, Quantum cryptography: Public key distribution and coin tossing, in: Proc. of IEEE Int. Conf. on Comp. Sys. and Signal Proc., Dec. 1984.
[2] R. Renner, N. Gisin, B. Kraus, Information-theoretic security proof for quantum-key-distribution protocols, Physical Review A 72 (1) (2005) 012332.
[3] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, M. Peev, The security of practical quantum key distribution, Reviews of modern physics 81 (3) (2009) 1301.
[4] M. Boyer, D. Kenigsberg, T. Mor, Quantum key distribution with classical bob, Phys. Rev. Lett. 99 (2007) 140501.
[5] X. Zou, D. Qiu, L. Li, L. Wu, L. Li, Semiquantum-key distribution using less than four quantum states, Physical Review A 79 (5) (2009) 052312.
[6] W. O. Krawec, Security proof of a semi-quantum key distribution protocol, in: 2015 IEEE International Symposium on Information Theory (ISIT), IEEE, 2015, pp. 686–690.
[7] W. Zhang, D. Qiu, P. Mateus, Security of a single-state semi-quantum key distribution protocol, Quantum Information Processing 17 (6) (2018) 1–21.
[8] N.-R. Zhou, K.-N. Zhu, X.-F. Zou, Multi-party semi-quantum key distribution protocol with four-particle cluster states, Annalen der Physik 531 (8) (2019) 1800520.
[9] W. O. Krawec, Quantum key distribution with mismatched measurements over arbitrary channels, arXiv preprint arXiv:1608.07728.
[10] M.-M. Wang, L.-M. Gong, L.-H. Shao, Efficient semiquantum key distribution without entanglement, Quantum Information Processing 18 (9) (2019) 1–10.
[11] O. Amer, W. O. Krawec, Semiquantum key distribution with high quantum noise tolerance, Physical Review A 100 (2) (2019) 022319.
[12] H. Iqbal, W. O. Krawec, High-dimensional semiquantum cryptography, IEEE Transactions on Quantum Engineering 1 (2020) 1–17.
[13] Y. Chongqiang, L. Jian, C. Xiubo, T. Yuan, H. Yanyan, An efficient semi-quantum key distribution protocol and its security proof, IEEE Communications Letters.
[14] X. Zou, D. Qiu, Three-step semiquantum secure direct communication protocol, Science China Physics, Mechanics & Astronomy 57 (9) (2014) 1696–1702.
[15] Y.-P. Luo, T. Hwang, Authenticated semi-quantum direct communication protocols using bell states, Quantum Information Processing 15 (2) (2016) 947–958.

[16] M.-H. Zhang, H.-F. Li, Z.-Q. Xia, X.-Y. Feng, J.-Y. Peng, Semiquantum secure direct communication using epr pairs, Quantum Information Processing 16 (5) (2017) 1–14.

[17] Q. Li, W. H. Chan, D.-Y. Long, Semiquantum secret sharing using entangled states, Physical Review A 82 (2) (2010) 022303.

[18] L. Li, D. Qiu, P. Mateus, Quantum secret sharing with classical bobs, Journal of Physics A: Mathematical and Theoretical 46 (4) (2013) 045304.

[19] K.-F. Yu, J. Gu, T. Hwang, P. Gope, Multi-party semi-quantum key distribution-convertible multi-party semi-quantum secret sharing, Quantum Information Processing 16 (8) (2017) 1–14.

[20] K. Thapliyal, R. D. Sharma, A. Pathak, Orthogonal-state-based and semi-quantum protocols for quantum private comparison in noisy environment, International Journal of Quantum Information 16 (05) (2018) 1850047.

[21] P.-H. Lin, T. Hwang, C.-W. Tsai, Efficient semi-quantum private comparison using single photons, Quantum Information Processing 18 (7) (2019) 1–14.

[22] Y. Chongqiang, L. Jian, C. Xiubo, T. Yuan, Efficient semi-quantum private comparison without using entanglement resource and pre-shared key, Quantum Information Processing 20 (8) (2021) 1–19.

[23] H. Iqbal, W. O. Krawec, Semi-quantum cryptography, Quantum Information Processing 19 (3) (2020) 1–52.

[24] W. O. Krawec, Mediated semiquantum key distribution, Phys. Rev. A 91 (2015) 032323.

[25] W. O. Krawec, An improved asymptotic key rate bound for a mediated semi-quantum key distribution protocol, arXiv preprint arXiv:1509.04797, 2015.

[26] Z.-R. Liu, T. Hwang, Mediated semi-quantum key distribution without invoking quantum measurement, Annalen der Physik 530 (4) (2018) 1700206.

[27] P.-H. Lin, C.-W. Tsai, T. Hwang, Mediated semi-quantum key distribution using single photons, Annalen der Physik 531 (8) (2019) 1800347.

[28] L. Chen, Q. Li, C. Liu, Y. Peng, F. Yu, Efficient mediated semi-quantum key distribution, Physica A: Statistical Mechanics and its Applications 582 (2021) 126265.

[29] Krawec W O. Multi-mediated semi-quantum key distribution, 2019 IEEE Globecom Workshops (GC Wkshps). IEEE, 1-6, (2019).

[30] J. Guskind, W. Krawec, Mediated semi-quantum key distribution with improved efficiency, Quantum Science and Technology. 7(3) (2022) 035019.

[31] Tsai C.W, Yang C.W, Lightweight mediated semi-quantum key distribution protocol with a dishonest third party based on Bell states, Scientific Reports, 11(1) (2021) 1-10.

[32] Zou X, Rong Z, Zhou N.R, Three Attacks on the Mediated Semi-quantum Key Distribution without Invoking Quantum Measurement, Annalen der Physik, 532(8) (2020) 2000251.

[33] M. Christianell, R. König, R. Renner, Postselection technique for quantum channels with applications to quantum cryptography, Physical review letters 102 (2) (2009) 020504.

[34] R. Renner, Symmetry of large physical systems implies independence of subsystems, Nature Physics 3 (9) (2007) 645–649.