Tsai and Wang *EPJ Quantum Technology* (2024) 11:63
https://doi.org/10.1140/epjqt/s40507-024-00275-5

EPJ Quantum Technology
a SpringerOpen Journal

RESEARCH Open Access

# Multi-party quantum key distribution protocol in quantum network

Chia-Wei Tsai[1*] and Chun-Hsiang Wang[1]

*Correspondence:
cwtsai@nutc.edu.tw
[1]Department of Computer Science and Information Engineering, National Taichung University of Science and Technology, No.129, Sec. 3, Sanmin Rd., North Dist., Taichung City 404, Taiwan

**Abstract**

This study proposes a measurement property of graph states and applies it to design a mediated multiparty quantum key distribution (M-MQKD) protocol for a repeater-based quantum network in a restricted quantum environment. The protocol enables remote classical users, who cannot directly transmit qubits, to securely distribute a secret key with the assistance of potentially dishonest quantum repeaters. Classical users only require two quantum capabilities, while quantum repeaters handle entanglement transmission through single-photon measurements. The one-way transmission approach eliminates the need for additional defenses against quantum Trojan horse attacks, reducing maintenance costs compared to round-trip or circular transmission methods. As a result, the M-MQKD protocol is lightweight and easy to implement. The study also evaluates the security of the protocol and demonstrates its practicality through quantum network simulations.

**Keywords:** Multiparty semi-quantum key distribution; Mediated multiparty quantum key distribution; Quantum network; Quantum repeater; Quantum Trojan horse attack

## 1 Introduction

Protecting transmitted messages on the internet against attacks is an important issue in the information era. Encryption/decryption is a solution for achieving this goal. However, the message sender and receiver must share a secret key to encrypt and decrypt the messages in advance. Sharing a secret key between a sender and receiver is critical in cryptography. In current classical cryptography, the key distribution protocol can be implemented using mathematical problems (e.g., prime factorization and discrete logarithms). Although the existing classical key distribution protocols are widely applied in various application scenarios, these protocols may be compromised when quantum computation matures. Therefore, quantum cryptography, which uses the properties of quantum mechanics to protect information against attacks, has been proposed as a cybersecurity solution in the era of quantum computers.

In 1984, Bennet and Brassard [1] proposed the first quantum cryptography protocol, the quantum key distribution (QKD) protocol, using the no-cloning theorem of non-orthogonal single photons. Since then, numerous studies have been conducted on quan-

tum cryptography. The unconditional security of BB84 protocol was proven in [2–4], and various QKD protocols [5–15] with different properties and quantum states have been designed. In addition to key distribution, quantum cryptography has been adopted for other applications. For example, the quantum secret sharing protocol (QSS) [16–19] enables a dealer to distribute confidential information among agents. Quantum secure direct communication [20–22] assists the sender and receiver in transmitting secret messages directly without preparing a private key, and quantum private computation [23–26] helps many participants to achieve a specific computation on their secret messages without disclosing any information about any participant.

Although the abovementioned quantum cryptography protocols can implement their goals securely, all participants in the protocol must be equipped with complete quantum capabilities. In terms of the current quantum technology, the implementation of some quantum devices or capabilities (e.g., storing qubits for a long time and transmitting qubits over a long distance without disturbance) remains expensive and difficult to maintain. Therefore, whether participants can use limited quantum capabilities to securely and efficiently achieve a quantum cryptography protocol is a critical research issue for popularizing quantum cryptography in Internet applications. To address this issue, Boyer et al. [27] proposed a practical quantum environment, specifically, the semi-quantum environment, having two types of users: quantum and classical users. According to the definition of the semi-quantum environment, quantum users have complete quantum capabilities, whereas classical users have limited quantum capabilities. Boyer et al. [27, 28] proposed the semi-quantum key distribution (SQKD) protocol for the semi-quantum environment. Subsequently, numerous research teams have adopted various quantum states, properties, or strategies to design SQKD protocols [29–33] and other semi-quantum cryptography protocols for various applications (e.g., semi-quantum secret sharing [34–36], semi-quantum private computation [37–39], semi-quantum directly secure communication [40–42]). Regarding the quantum capabilities classical users possess, the semi-quantum environments can be classified into two types, including: (1) measure-resend environment and (2) randomization environment. In the measure-resend environment, classical users can only generate Z-basis $\{|0\rangle, |1\rangle\}$ qubits, perform Z-basis $\{|0\rangle, |1\rangle\}$ measurement, and reflect received particles without interference. In the randomization environment, classical users are allowed to perform Z-basis $\{|0\rangle, |1\rangle\}$ measurement on particles, reflect the received particles without interference, and also permute qubits using delay fibers. Although the abovementioned SQKD protocols enable a quantum user to share secret keys with another classical user, how to distribute secret keys among classical users is another interesting issue. To address this issue, Krawec [43] proposed a mediated framework that allows classical users to execute the protocols with the assistance of a quantum third party (TP). Some mediated semi-quantum key distribution (M-SQKD) protocols [44–46] have been designed based on the mediated framework.

In some applications (e.g., broadcasting), a user must share a broadcasting key with the partners. To achieve this task, Zhang et al. [47] proposed the first multiparty semi-quantum key distribution (MSQKD) protocol that allows a quantum user to distribute a secret key with $n$ classical users in a series network environment (shown in *Fig. 1*). Zhou et al. [48] used the property of the four-particle cluster state to propose an MSQKD protocol to improve the efficiency of the protocol proposed by Zhang et al. Tian et al. [49] considered the qubit efficiency and adopted the hyperentangled Bell state (including spa-

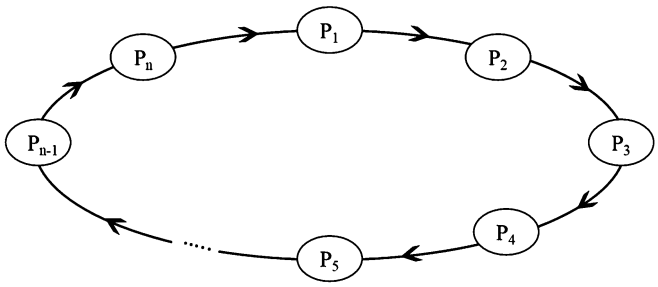


**Figure 1** Series quantum network diagram

tial and polarization degrees of freedom) to design an MSQKD protocol. Additionally, Ye et al. [50] proposed a mediated multiparty semi-quantum key distribution (M-MSQKD) protocol that utilizes Bell states and circular transmission, enabling classical users to distribute secret keys among themselves. They demonstrated that the noise tolerance of the proposed protocol approaches that of the BB84 protocol even in the worst-case scenario, where TP is untrusted.

However, the above-mentioned MSQKD protocols present two challenges as follows:

(1) *Cost overhead*: classical users must be equipped with additional quantum devices/capabilities to defend against quantum Trojan horse attacks owing to the circular qubit transmission.

(2) *Restricted applicability:* the protocols can only operate in a specific network environment, that is, the series network. Thus, these protocols cannot be used in the general network environment where the distance between the neighboring classical users may exceed the effective transmission range.

To address the first issue, Tsai et al. [51–53] proposed a new semi-quantum environment known as a restricted quantum environment, which also includes two categories of participants: classical and quantum. Classical participants have only two quantum capabilities, (1) measuring qubits in the Z-basis $\{|0\rangle, |1\rangle\}$, and (2) performing single-qubit operations. In contrast, quantum users are equipped with full quantum capabilities. Tsai and Yang [51] proposed a mediate quantum key distribution protocol in a restricted quantum environment. Because of the use of one-way qubit transmission, the protocol is free from quantum Trojan horse attacks. Therefore, classical users are not equipped with any defense devices against quantum Trojan horse attacks. However, this protocol allows only two classical users to distribute the secret keys and does not consider the multiparty key distribution situation and the general network application environment.

For the unresolved problem mentioned above, once classical users securely share entangled states, they can execute quantum communication protocols using these entangled states. Therefore, distributing multi-particle entanglement states among classical users within a quantum network is a crucial focus of this study. To address this issue, this paper introduces a measurement characteristic of quantum graph states [54] to distribute GHZ-like states among classical users within a general repeater-based quantum network. These entangled states are then used to design the first mediated multiparty quantum key distribution (M-MQKD) protocol in a restricted quantum environment. In the M-MQKD protocol, a classical user, Alice, can distribute secret keys among $n$ remote classical users (Alice and these users cannot transmit the qubits to each other directly) in a general net-

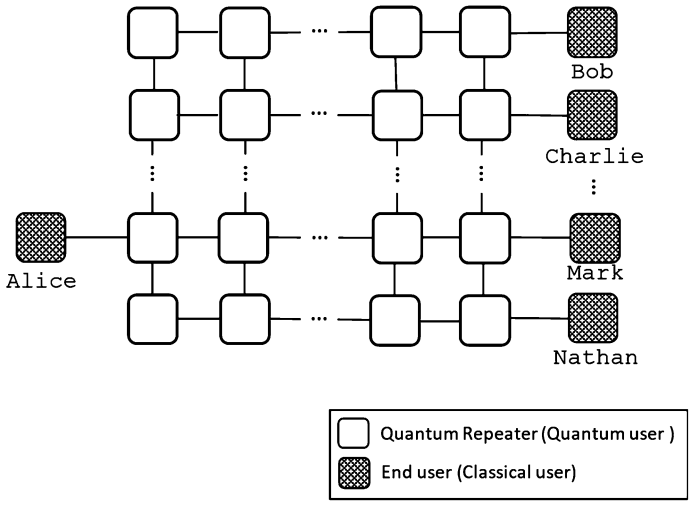


**Figure 2** A general network environment with quantum repeaters

work environment (shown in *Fig. 2*) with the help of dishonest quantum repeaters in the quantum network. Unlike common repeater-based quantum networks that utilize entanglement swapping [55–57] —which requires performing a Bell measurement or a combination of CNOT operation, Hadamard operation, and two single-photon measurements to transmit entanglement—the repeaters in our approach transfer the entanglement use only a single-photon measurement. In addition, the proposed M-MQKD protocol is free from quantum Trojan horse attacks and reduces the transmission cost of qubits owing to one-way qubit transmission. Therefore, the proposed M-MQKD method is lightweight and easy to implement. Finally, a security evaluation is conducted to demonstrate that the proposed M-MQKD protocol is free from collective and quantum Trojan horse attacks, and then the experiments conducted with the quantum network simulator were carried out to illustrate the viability of the proposed M-MQKD protocol.

The remainder of this paper is organized as follows: *Sect. 2* reviews the current research on quantum graph state. *Sect. 3* addresses the character of the graph state with a 1D+star type, which is used to propose our protocol. The processes of the proposed M-MQKD protocol are described in *Sect. 4*. Security analyses and simulation results of the proposed protocol are described in *Sect. 5*. Finally, *Sect. 6* outlines the concluding remarks and recommendations for further investigation.

## 2 Properties of graph state

This section first describes the general formula of the graph state. Then, the properties of the graph state, including the local complementation and measurement properties in the Z-, Y-, and X-bases, are described.

### 2.1 Graph state

A common quantum graph state can be expressed as $G = (V, E)$ (*Eq. (1)*), in which $V$ (vertices) and $E$ (edges) denote a set of qubits and entanglement relationships, respectively.

$$|G\rangle = \prod_{(a,b)\in E} CZ^{\{a,b\}} |+\rangle^{\otimes n}, \tag{1}$$

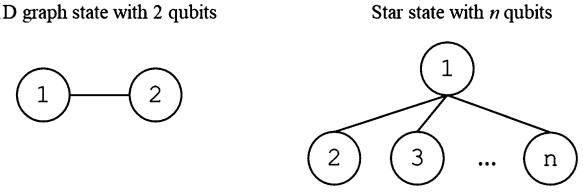


**Figure 3** Examples of 1D+star graph states

where $|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle)$ and $CZ^{\{a,b\}}$ means executing a CZ operation (*Eq. (2)*) on the qubit pairs $(a, b)$.

$$CZ^{\{a,b\}} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & -1 \end{bmatrix} = |00\rangle\langle 00| + |01\rangle\langle 01| + |10\rangle\langle 10| - |11\rangle\langle 11| \tag{2}$$

It merits attention that the 2-qubit 1D graph state, $|D\rangle_{12} = \frac{1}{\sqrt{2}}(|0+\rangle + |1-\rangle)_{12}$, and the star graph state with $n$ qubits $|S\rangle_{12\ldots n} = \frac{1}{\sqrt{2}}(|0+\cdots+\rangle + |1-\cdots-\rangle)_{12\ldots n}$ (*Fig. 3*) can be transformed into Bell and GHZ states by using Local Operation and Classical Communication (LOCC). In other words, if the Hadamard operation $H$ (*Eq. (3)*) is performed on the 2nd qubit (2nd to n$^{\text{th}}$ qubits) of the 1D (star) graph state, the quantum system undergoes a transformation into the Bell (GHZ) state.

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

The other common properties of the graph states are introduced below.

## 2.2 Local complementation

A series of specific unitary operations can be implemented to achieve local complementation of a graph state. To perform local complementation (denoted as $LC_i(G)$) on a graph state G with the $i$-th qubit as the center vertex, we apply rotation operations $R_x\left(\frac{\pi}{2}\right)$ to the $i$-th qubit and $R_z\left(\frac{-\pi}{2}\right)$ to the qubits neighboring with the $i$-th qubit. These rotation operations, defined by *Eqs. (4)* and *(5)* respectively, ensure the desired transformation.

$$R_x\left(\frac{\pi}{2}\right) = e^{-i\frac{\pi}{4}X} = \begin{bmatrix} \cos\frac{\pi}{4} & -i\sin\frac{\pi}{4} \\ -i\sin\frac{\pi}{4} & \cos\frac{\pi}{4} \end{bmatrix} \tag{4}$$

$$R_z\left(\frac{-\pi}{2}\right) = e^{i\frac{\pi}{4}Z} = \begin{bmatrix} e^{i\frac{\pi}{4}} & 0 \\ 0 & e^{-i\frac{\pi}{4}} \end{bmatrix} \tag{5}$$

## 2.3 Measurement in Z-basis

The measurement outcome of the $i$-th qubit of a graph state in the Z-basis $\{|0\rangle, |1\rangle\}$ yields the following expression for the quantum system:

$$M_z^i|G\rangle = \frac{1}{\sqrt{2}}\left(|0\rangle_i \otimes U_0^i|G-i\rangle + |1\rangle_i \otimes U_1^i|G-i\rangle\right), \tag{6}$$

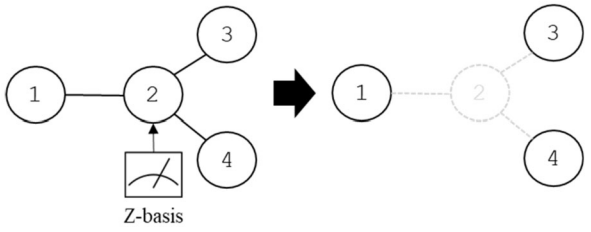


**Figure 4** An example of measurement property in Z-basis

where $U_0^i = I^{N_i}$, $U_1^i = \sigma_z^{N_i}$, and $|G-i\rangle$ denote the quantum system without the $i$-th qubit and its associated entanglement relationships. $I^{N_i}$ and $\sigma_z^{N_i}$ mean performing the identity operation I and $\sigma_z$ (*Eq. (7)*) on the neighboring qubits of the $i$-th qubit.

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} = |0\rangle\langle 0| - |1\rangle\langle 1| \tag{7}$$

From examining *Eq. (6)*, it becomes clear that to measure the $i$-th qubit of a graph state in the Z-basis, one must eliminate the $i$-th qubit along with its entangled connections, and then carry out the necessary operation on its adjacent qubits, dependent on the outcome of the measurement. The measurement property of the Z-basis is also illustrated by a simple graph, as shown in Fig. 4. Specifically, if the 2nd qubit is measured in the Z-basis, its entanglements will be eliminated.

### 2.4 Measurement in Y-basis

If performing Y-basis $\left\{ |+y\rangle = \frac{1}{\sqrt{2}}(|0\rangle + i\,|\,1\rangle), |-y\rangle = \frac{1}{\sqrt{2}}(|0\rangle - i\,|\,1\rangle) \right\}$ measurement on the $i$-th qubit of a graph state, the quantum system can be represented as *Eq. (8)*.

$$M_y^i |G\rangle = \frac{1}{\sqrt{2}} \left( |+y\rangle_i \otimes U_{+y}^i |LC_i(G) - i\rangle + |-y\rangle_i \otimes U_{-y}^i |LC_i(G) - i\rangle \right), \tag{8}$$

where $U_{+y}^i = R_z\left(\frac{\pi}{2}\right)^{N_i}$, $U_{-y}^i = R_z\left(\frac{-\pi}{2}\right)^{N_i}$, and $LC_i(G)$ denote the execution of the local complementation on the $i$-th qubit, and $|LC_i(G) - i\rangle$ denotes $LC_i(G)$ without the $i$-th qubit and its associated entanglement relationships. $R_z\left(\frac{\pm\pi}{2}\right)^{N_i}$ means performing the rotation operation $R_z\left(\frac{\pm\pi}{2}\right)$ (*Eq. (9)*) on the qubits neighboring with the $i$-th qubit.

$$R_z\left(\frac{\pm\pi}{2}\right) = e^{\mp i\frac{\pi}{4}Z} = \begin{bmatrix} e^{\mp i\frac{\pi}{4}} & 0 \\ 0 & e^{\pm i\frac{\pi}{4}} \end{bmatrix} \tag{9}$$

Based on *Eq. (8)*, it is evident that measuring the $i$-th qubit in the Y-basis entails performing $LC_i(G)$. This involves canceling the $i$-th qubit along with its associated entanglement. Subsequently, a rotation operation $R_z$ is performed on the neighboring qubits of the $i$-th qubit, with the degree of rotation determined by the measurement outcome The measurement property of the Y-basis is further explained by a simple graph, as depicted in Fig. 5. Specifically, measuring the 2nd qubit in the Y-basis is equivalent to applying $LC_2(G)$, followed by measuring the 2nd qubit in the Z-basis.

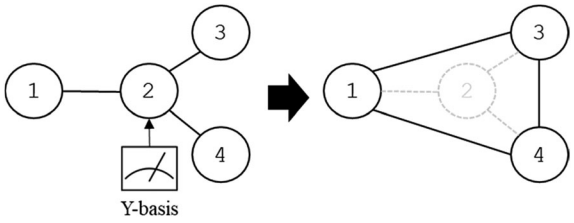


**Figure 5** An example of measurement property in Y-basis

### 2.5 Measurement in X-basis

When performing X-basis $\left\{|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle), |-\rangle = \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)\right\}$ measurement on the $i$-th qubit of a graph state, the operations required are more intricate compared to measurements in Z- or Y-bases. To represent the resulting quantum system, we must designate an arbitrary neighboring qubit of the $i$-th qubit (referred to as the $j$-th qubit) as the auxiliary qubit, as follows:

$$\begin{aligned} & M_x^i |G\rangle \\ & = \frac{1}{\sqrt{2}} \left( |+\rangle_i \otimes U_+^i \left| LC_j \left( LC_i \left( LC_j (G) \right) - i \right) \right\rangle + |-\rangle_i \otimes U_-^i \left| LC_j \left( LC_i \left( LC_j (G) \right) - i \right) \right\rangle \right), \end{aligned} \tag{10}$$

where $U_+^i = R_y\left(\frac{-\pi}{2}\right)^j \sigma_z^{N_i - (N_j \cup j)}$, $U_-^i = R_y\left(\frac{\pi}{2}\right)^j \sigma_z^{N_j - (N_i \cup i)}$, and $N_i - \left(N_j \cup j\right)$ $(N_j - (N_i \cup i))$ denotes the difference set of $N_i$ $(N_j)$ and $N_j \cup j$ $(N_i \cup i)$. Here, $R_y\left(\frac{\pm\pi}{2}\right)^j$ means performing the rotation operation $R_y\left(\frac{\pm\pi}{2}\right)$ (*Eq. (11)*) on the assistant qubit, that is, the $j$-th qubit; $\sigma_z^{N_i - (N_j \cup j)}$ and $\sigma_z^{N_j - (N_i \cup i)}$ indicate that $\sigma_z$ is performed on the qubit in the sets $N_i - \left(N_j \cup j\right)$ and $N_j - (N_i \cup i)$, respectively.

$$R_y\left(\frac{\pm\pi}{2}\right) = e^{\mp i \frac{\pi}{4} Y} = \begin{bmatrix} \pm\cos\frac{\pi}{4} & \mp\sin\frac{\pi}{4} \\ \pm sin\frac{\pi}{4} & \pm\cos\frac{\pi}{4} \end{bmatrix} \tag{11}$$

By examining *Eq. (10)*, we can conclude that performing X-basis measurement on the $i$-th qubit and designating the $j$-th qubit as the auxiliary qubit is tantamount to conducting local complementation on the $j$-th qubit, subsequently performing Y-basis measurement on the $i$-th qubit, and ultimately performing local complementation on the $j$-th qubit once more. The measurement property of the X-basis is further represented by a simple graph, as depicted in Fig. 6. Specifically, measuring the 2nd qubit in X-basis and selecting the 1st qubit as the assistant qubit is equivalent to applying $LC_1(G)$, then measuring 2nd qubit in Y-basis, and applying $LC_1(G)$ again.

## 3 Proposed measurement property of 1D+star graph state

This section expresses a 1D + Star graph state and proposes the measurement characteristic of this graph state. The 1D+Star graph state is composed of a 1D graph and a star graph state. *Fig. 7* shows a 1D+star graph state with $n$ qubits, in which the 1st to $(k-1)$-th qubits belong to the 1D graph state, and the $k$-th to $n$-th qubits belong to the star graph state. In this study, the graph state's properties were used to extend an innovative character to a 1D+star graph state in the X-basis measurement. If we perform X-basis $\{|+\rangle, |-\rangle\}$ measurement on the 2nd to the $k$-th qubits and always take the 1st qubit as the assistant qubit,

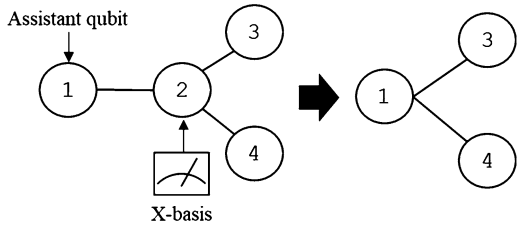


**Figure 6** An example of measurement property in X-basis

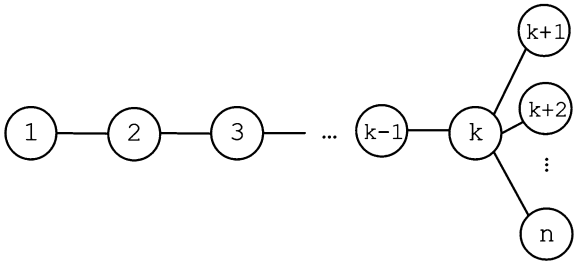


**Figure 7** Schematic diagram of a 1D+star graph state

the remaining quantum system will be a graph state with a star type after performing the corresponding operation $U^R$. The remaining quantum state system is expressed as

$$U^R \cdot |S\rangle_{1,k+1,..,n} = \frac{1}{\sqrt{2}} (|0++\cdots+\rangle + |1--\cdots-\rangle)_{1,k+1,..,n}, \tag{12}$$

where $U^R = R_y^1(\theta) \otimes U_v^{N_1}$, $R_y^1(\theta)$ means performing $R_y(\theta)$ on the 1st qubit, and $U_v^{N_1}$ means performing $U_v$ on the neighbors of the 1st qubit (i.e., the $(k+1)$-th to $n$-th qubits). Here, $\theta = \sum_{i=2}^{k} \left((-1)^{MR_i \oplus_{j=2}^{i-1} \overline{MR_j}} \frac{\pi}{2}\right)$, $v = \oplus_{j=2}^{i-1} \overline{MR_j}$, $U_0 = I$, and $U_1 = \sigma_Z$, where $MR_j$ means the result of the $j$-th qubit obtaining from measurement, and $\overline{MR_j}$ denotes the complement number of $MR_j$. In this study, the measurement results $|+\rangle$ and $|-\rangle$ were encoded as the classical bits 0 and 1, respectively.

Furthermore, the operation $R_y(\theta)$ was analyzed in this study. The global phase is the only difference between $R_y(\theta)$ and $R_y(\theta + 2x\pi)$, where $x \in Z$. Because the measurement results are not influenced by the global phase, $R_y(\theta)$ is equivalent to $R_y(\theta + 2x\pi)$. Based on the above reasoning, *Eqs. (13)* and *(14)* were used to express $\theta$ and $R_y(\theta)$, respectively.

$$\theta = \sum_{i=2}^{k} \left((-1)^{MR_i \oplus_{j=2}^{i-1} \overline{MR_j}} \frac{\pi}{2}\right) = 2x\pi + r, \tag{13}$$

where $x \in Z$ and $r \in \left\{0, \frac{1}{2}\pi, \pi, \frac{3}{2}\pi\right\}$.

$$R_y(\theta) = (-1)^x R_y(r) = (-1)^x R_t, \tag{14}$$

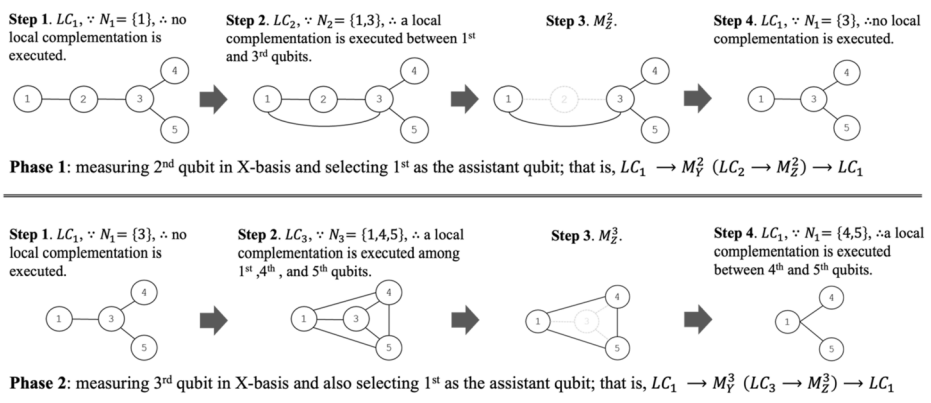


**Figure 8** Schematic of the proposed measurement character of a 1D+star state with 5 qubits

where $t = \frac{2r}{\pi}$, $R_0 = I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$, $R_1 = H\sigma_z = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$, $R_2 = i\sigma_y = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$, and $R_3 = \sigma_z H = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 & 1 \\ -1 & 1 \end{bmatrix}$. From *Eqs. (12)* and *(14)*, it is obvious that the accomplishment of $U^R$ needs only the two Pauli operations (i.e., $\sigma_z$ and $i\sigma_y$) and $H$ operation. Notice that $i\sigma_y$ can be expressed using $H$ and $\sigma_z$, i.e., $i\sigma_y = \sigma_z H \sigma_z H$. Thus, only two operations ($H$ and $\sigma_z$.) are needed to transform a 1D+star graph state into a star graph state after performing the X-basis measurement.

We illustrate the proposed property using a 5-qubit 1D+star graph state as an example, as depicted in *Fig. 8* and *Eq. (15)*. Initially, we perform the X-basis $\{|+\rangle, |-\rangle\}$ measurement on the 2nd qubit, with the 1st qubit selected as the auxiliary qubit. This measurement operation is equivalent to executing local complementation on the 1st qubit ($LC_1$), followed by performing the Y-basis $\{|+i\rangle, |-i\rangle\}$ measurement on the 2nd qubit ($M_z^2$), and ultimately conducting local complementation on the 1st qubit again. Because Y-basis measurement is also equivalent to executing the local complementation on the qubit and then measuring the qubit in Z-basis $\{|0\rangle, |1\rangle\}$, the foregoing processes can be expressed as $LC_1 \longrightarrow LC_2 \longrightarrow M_z^2 \longrightarrow LC_1$ (also shown in Phase 1 of *Fig. 8*). After performing the X-basis $\{|+\rangle, |-\rangle\}$ measurement on the 2nd qubit, the original qubit state undergoes a reduction to a 1D+star graph state with 4 qubits. Subsequently, we measure the 3rd qubit in the X-basis $\{|+\rangle, |-\rangle\}$. In other words, the operation sequence $LC_1 \longrightarrow LC_3 \longrightarrow M_z^3 \longrightarrow LC_1$ is applied to the 4-qubit quantum state, as illustrated in Phase 2 of *Fig. 8*. Following this operation, the state of the remaining quantum system is transformed into a 3-qubit graph state with a star type after the remaining qubits are executed by the inverse operation $U^{Rec} = R_y^1(\theta) \otimes U_v^{N_1}$. The operations corresponding to the proposed properties and *Eq. (16)* are listed in *Table 1*. Assume the measurement results of the 2nd and 3rd qubits are $|+-\rangle$; the corresponding operations for the 1st, 4th, and 5th qubits are $i\sigma_y$, $\sigma_Z$, and $\sigma_Z$, respectively. After executing these operations, the resulting quantum system will be a star graph state $|S\rangle_{145} = \frac{1}{\sqrt{2}}(|0++\rangle + |1--\rangle)_{145}$. Because the star graph state can be transformed to the GHZ state by LOCC, it can be transferred to a GHZ-like state (i.e., $|\Psi\rangle = \frac{1}{\sqrt{2}}(|+++\rangle + |---\rangle) = \frac{1}{2}(|000\rangle + |011\rangle + |101\rangle + |110\rangle)$) after performing the

**Table 1** Operations corresponding to the measurement results

| Measurement results | $\theta$ | $R_t$ for 1st qubit | $v$ | $U_v$ for 4th and 5th qubits |
|---|---|---|---|---|
| $\|++\rangle$ | 0 | $R_0 = I$ | 0 | $I$ |
| $\|+-\rangle$ | 180 | $R_2 = i\sigma_y$ | 1 | $\sigma_Z$ |
| $\|-+\rangle$ | 0 | $R_0 = I$ | 1 | $\sigma_Z$ |
| $\|--\rangle$ | 180 | $R_2 = i\sigma_y$ | 0 | $I$ |

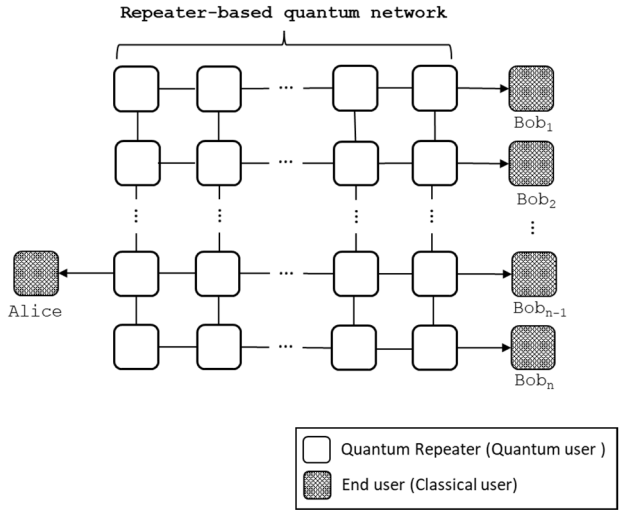


**Figure 9** Environment of the proposed protocol in the grid repeater-based quantum network

$H$ operation on the 1st qubit.

$$|G\rangle_{12345} = \frac{\sqrt{2}}{4}\begin{pmatrix} |0++++\rangle + |0+-++\rangle + |0-++-\rangle + |0----\rangle \\ +|1+++-\rangle - |1+---\rangle + |1-+++\rangle + |1--++\rangle \end{pmatrix}_{12345} \tag{15}$$

$$= \frac{1}{2}\begin{pmatrix} |++\rangle_{23} \otimes (|0++\rangle + |1--\rangle)_{145} \\ +|+-\rangle_{23} \otimes (|0++\rangle - |1--\rangle)_{145} \\ +|-+\rangle_{23} \otimes (|0--\rangle + |1++\rangle)_{145} \\ +|--\rangle_{23} \otimes (-|0--\rangle + |1++\rangle)_{145} \end{pmatrix} \tag{16}$$

## 4 Proposed M-MQKD protocol

This section first describes the execution environment and then introduces the M-MQKD protocol within this quantum environment.

### 4.1 Description of execution environment

Assume that a classical user Alice wants to distribute a secret key to $n$ remote classical users $\mathrm{Bob_1}$–$\mathrm{Bob_n}$. Classical users cannot transmit qubits directly owing to the limitation on the transmission distance; therefore, they require the help of a repeater-based quantum network to achieve key distribution. Here, a grid repeater-based quantum network is used for the application environment, as shown in *Fig. 9*. In the application environment, the classical users (i.e., Alice, $\mathrm{Bob_1}$, $\mathrm{Bob_2}$, …, $\mathrm{Bob_n}$) have limited quantum capabilities, namely, (1) Z-basis measurement and (2) single-qubit operations. A quantum repeater in

a quantum network is a quantum user with all quantum capabilities. Moreover, quantum repeaters perform only single-photon measurements rather than the entanglement swapping to transfer the entanglement in the proposed protocol. In order to align a realistic scenario, quantum repeaters are assumed to be dishonest, meaning they are malicious entities capable of carrying out various attacks. This includes collusion with other dishonest repeaters to pilfer information regarding the participants' secret keys.

However, none of the participants conspires with any malicious repeater. In addition, this study assumed that each classical user is connected with at least one quantum repeater through a one-way quantum channel (from the repeater to the classical user), and authenticated classical channels exist between the classical users, and the messages transmitted through the authenticated channels can be eavesdropped but cannot be modified.

This study focused on the design of a quantum cryptography protocol and did not consider network routing issues. Therefore, this study assumed that quantum repeaters can determine an optimal routing path and establish the 1D+star graph state among Alice and other protocol participants, where the repeaters can use the routing algorithm of the quantum network [58, 59] to determine the optimal path and then use the intuitive relay method, graph state distribution [60, 61], or other methods to establish the 1D+star graph state. A small grid network with nine quantum repeaters and three protocol participants (*Fig. 10*) was used as an example to prove the feasibility of establishing 1D+star graph states. In this example, a classical user Alice wants to distribute a secret key to two classical users $Bob_1$ and $Bob_2$. Assume that $\{R_3, R_6, R_9, R_8, R_7\}$ is chosen as the routing path, and the quantum repeaters in this routing path assist the three participants in establishing the 1D+star graph states used to achieve the goal of key distribution.

$R_3$ generates a graph state with 3 qubits $|G\rangle_{A12}$. It keeps the first two qubits (labeled as A and 1) and sends the final qubit (labeled as 2) to $R_6$. $R_6$ generates a qubit in $|+\rangle$ (labeled as 3) and then performs a control-Z operation on Nos. 2 and 3 qubits, where No. 2 is the control bit and the other is the target bit. Then, $R_6$ sends qubit No. 3 to $R_9$. Finally, $R_7$, $R_8$, and $R_9$ use similar methods to establish the graph state (shown in *Fig. 11 (a)*). Subsequently, $R_7$ and $R_8$ measure qubits 5 and 4 in Y-basis. The entanglement relations of the remaining qubits are shown in *Fig. 11 (b)* and *(c)*, respectively. $R_3$, $R_7$, and $R_9$ send qubit Nos. A, $B_1$, and $B_2$ to Alice, $Bob_1$, and $Bob_2$, respectively (*Fig. 11 (d)*). Thus, a 1D+star graph state is established among the repeaters and protocol participants.

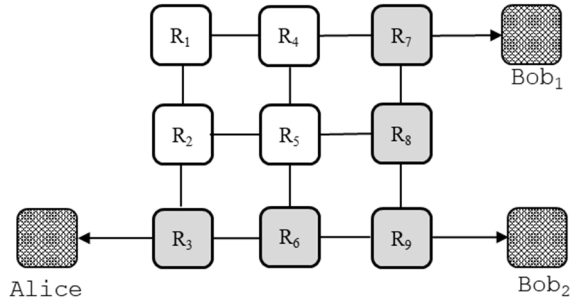


**Figure 10** Example of establishment of 1D+star graph states

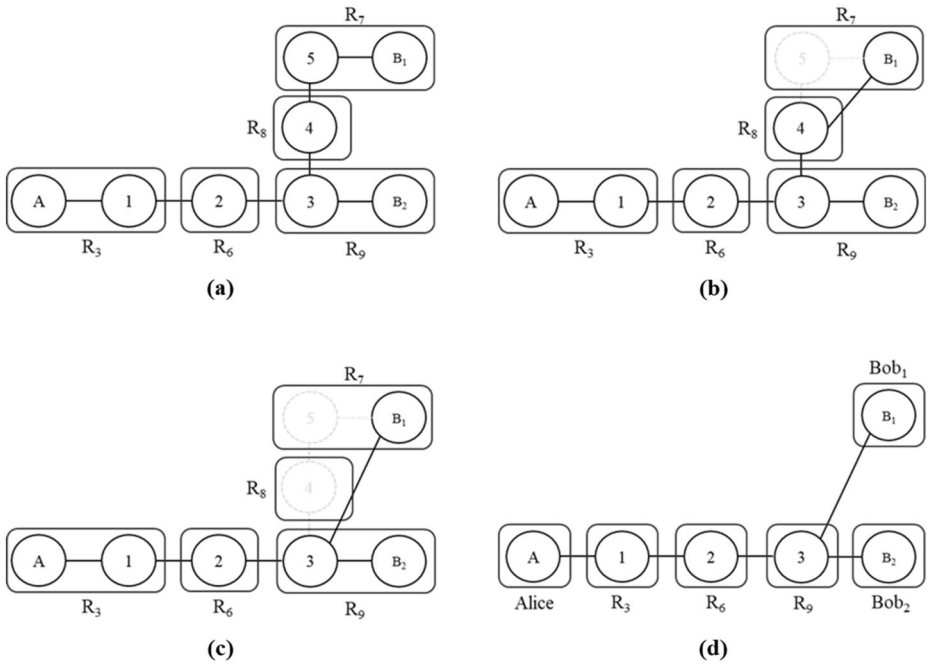


**Figure 11** Establishment of graph state among routing repeaters and protocol participants

## 4.2 Proposed protocol

Let's imagine a scenario where a classical user named Alice needs to share a secret key among several classical users, named $\mathrm{Bob}_1$, $\mathrm{Bob}_2$ through to $\mathrm{Bob}_n$, utilizing quantum repeaters within a quantum network. The suggested method unfolds as follows:

*Step 1.* An optimal routing path is determined for the key distribution task. We assume that $k$ quantum repeaters exist along the routing path. These quantum repeaters use a graph state distribution or other methods to establish the 1D+star graph state among the protocol participants and quantum repeaters. After distributing the graph state, a repeater $R_j$ measures the qubit in hand in X-basis $\{|+\rangle, |-\rangle\}$ and announces the measurement result $MR_j$ to the protocol participants, where $j \in \{1, 2, \ldots, k\}$.

*Step 2.* When receiving the qubits, Alice and the other participants perform the corresponding operations to transfer the quantum state to the GHZ-like state based on the measurement results announced by the quantum repeaters; thus, Alice and the other participants perform $H \cdot R_y(\theta)$ and $U_v$ on their qubits, respectively (the details have been explained in *Sect. 2-2*). After performing these operations, the quantum system shared between Alice and the other participants becomes a GHZ-like state *(Eq. (17))*. Alice and each participant then choose the *Share* or *Check mode* randomly. The operations of these two modes are listed in *Table 2*. Alice and the other participants $\mathrm{Bob}_1$, $\mathrm{Bob}_2$, …, $\mathrm{Bob}_n$ store the measurement results $mr_A^i$, $mr_{B_1}^i$, $mr_{B_2}^i$, …, $mr_{B_n}^i$, respectively. Here, the measurement results $|0\rangle$ ($|1\rangle$) is encoded as the classical bits 0 (1).

$$|\Psi\rangle_{\mathrm{A},B_1,\ldots,B_n} = \frac{1}{\sqrt{2}}\left(|+\cdots+\rangle + |-\cdots-\rangle\right)_{\mathrm{A},B_1,\ldots,B_n} \tag{17}$$

**Table 2** Operations in the two modes

| Mode | Operations |
|---|---|
| Share | • Performing $H$ operation on the qubit.<br>• Performing Z-basis measurement on the qubits. |
| Check | • Performing Z-basis measurement on the qubits. |

*Steps 1* and *2* are iteratively performed multiple times until Alice and the participants accumulate enough measurement outcomes to successfully detect any potential eavesdropping and to distribute the key effectively.

*Step 3.* Alice and the other participants disclose their chosen modes from *Step 2* over an authenticated classical channel. During each iteration, if Alice and the participants pick the *Share mode* (or *Check mode*), they utilize their measurement outcomes as raw key bits (check bits), denoted as $rk_A^i, rk_{B_1}^i, \ldots, rk_{B_n}^i (cb_A^i, cb_{B_1}^i, \ldots, cb_{B_n}^i)$; otherwise, they discard the measurement results.

*Step 4.* To determine if an attack has been initiated by malicious outsiders or repeaters, Alice selects $l$ bits at random from the raw key bits, employing all the check bits as discussion bits for disclosure. She then announces the locations of these discussion bits and requests all participants to reveal their bits at these specified positions through an authenticated classical channel. If a discussion bit belongs to the raw key bits, Alice verifies whether the bit announced by all participants are the same as her bit (i.e., $rk_A^i = rk_{B_1}^i = \cdots = rk_{B_n}^i$); otherwise, she verifies whether $\oplus_{j=1}^n cb_{B_j}^i \oplus cb_A^i = 0$, where $\oplus_{j=1}^n cb_{B_j}^i$ means $cb_{B_1}^i \oplus cb_{B_2}^i \oplus \cdots \oplus cb_{B_n}^i$. From the public discussion, Alice calculates the error rate. Should the error rate exceed the pre-established noise threshold $\varepsilon$ (set by default to the quantum channel's inherent noise rate), the participants involved in the protocol will terminate the current session and initiate the protocol anew. If the error rate remains below this threshold, they proceed with the subsequent stages of the suggested protocol.

*Step 5.* The remaining raw keys, i.e., $RK_A = \left\{rk_A^1, rk_A^2, \ldots, rk_A^m\right\}$, $RK_{B_1} = \left\{rk_{B_1}^1, rk_{B_1}^2, \ldots, rk_{B_1}^m\right\}, \ldots$, and $RK_{B_n} = \left\{rk_{B_n}^1, rk_{B_n}^2, \ldots, rk_{B_n}^m\right\}$, are used to share the secret key by Alice and the other participants. Alice uses the error rate obtained from the previous step to perform post-processing procedures [62] (including error correction and privacy amplification) along with the other participants to obtain the final secret key.

## 5 Security analysis, simulation, and comparison

In this section, security analyses are presented to prove that the proposed M-MQKD protocol is robust under a collective attack situation and immune to quantum Trojan horse attacks. The findings from simulations are analyzed to demonstrate that the proposed protocol is practical and effective for a quantum network incorporating $n$ quantum repeaters. Finally, a comparison is provided to demonstrate that the proposed protocol is more practical than existing MSQKD protocols designed only for a series quantum network.

### 5.1 Security analysis

This subsection details the security assessments conducted to establish the robustness of the proposed M-MQKD protocol against various attack strategies in quantum communications. These strategies include individual, collective, and coherent attacks. Among these, an individual attack has the greatest limitations on the attacker, rendering it the least

powerful. In contrast, a coherent attack offers an attacker more freedom, making it potentially more dangerous. However, no research has highlighted the increased benefits that an attacker gains from using a coherent attack as opposed to a collective attack. This study delves into the collective and quantum Trojan horse attacks and validates the robustness of the proposed protocol against these threats through security analyses.

#### *5.1.1 Collective attack*

Within the framework of quantum networks utilizing repeaters, these repeaters hold a crucial advantage over potential internal or external adversaries because they control essential operations such as quantum state creation and transmission. This study showcases the robustness of the proposed protocol against this attack from repeaters, where "robustness" is defined according to the framework established by Boyer et al. [27, 28]. This definition implies that legitimate participants can detect all forms of attacks via a security verification process with a probability greater than zero of identifying such attacks. In addition, because the neighboring repeaters of Alice and the other participants have the greatest advantage in attacking the proposed protocol (e.g., $R_3$ and $R_9$ in *Fig. 8*), this study assumes that these repeaters will conspire with each other to steal the secret keys.

**Theorem 1** *Suppose a scenario where malicious repeaters launch a collective attack on the qubits sent to Alice and the other participants. To execute this attack, these nefarious repeaters deviate from the prescribed steps of the proposed protocol, specifically, bypassing the established procedures for generating the* 1*D+star graph states. In their attack strategy, these malicious repeaters distribute the GHZ-like states* (*as described in* Eq. (17)) *through the application of a unitary operation denoted as* $U_e$ *to embed a probe* $|E\rangle$ *within the GHZ-like state. Then, repeaters can potentially extract secret key information by measuring the ancillary qubits. It is important to recognize that* $U_e$ *must comply with the fundamental principles of quantum mechanics. However, in the scenario of a collective attack, no unitary operation that allows malicious repeaters to covertly acquire knowledge about the secret keys exists. This means that participants always have a chance to be aware of any attempts by malicious repeaters to compromise security.*

*Proof* An attack operation, $U_e$, is applied by the malicious repeater to insert the probe $|E\rangle$ into the GHZ-like state. The malicious repeater keeps the probe in its memory, and it sends the 1st qubit of the GHZ-like state to Alice and the other qubits to the other participants to allow the protocol participant to execute the proposed M-MQKD protocol. Based on the principles of quantum mechanics, once the unitary operation $U_e$ is applied, the state of the quantum system transforms according to the equation that follows:

$$\begin{aligned} U_e\left(|\Psi\rangle_{12\ldots n}\otimes|E\rangle\right) &= a_0\,|00..0\rangle\,|e_0\rangle + a_1\,|00\ldots1\rangle\,|e_1\rangle + \cdots + a_{2^n-1}\,|11\ldots1\rangle\,|e_{2^n-1}\rangle \\ &= \sum_{j=0}^{2^n-1} a_j\left|j_{(2)}\right\rangle_{12\ldots n}\left|e_j\right\rangle, \end{aligned} \tag{18}$$

where $j_{(2)}$ denotes the binary format of $j$, $\sum_{j=0}^{2^n-1}\left|a_j\right|^2 = 1$. For all $j$ belonging to the set $\{0,1,\ldots,2^n-1\}$, $|e_j\rangle$ can be differentiated by the malicious repeater, as the states $|e_x\rangle$ and $|e_y\rangle$ are orthogonal to each other when $x \neq y$. To successfully pass through the discussion

phase in *Step 4* of the proposed M-MQKD protocol, the malicious repeater is required to modify $U_e$. This adjustment ensures that the quantum state, as depicted in *Eq. (18)*, aligns with the dual measurement characteristics inherent to the GHZ-like state:(1) the outcome of executing XOR operations on all measurement results should be 0 when the designated discussion bit is chosen from the verification bits, and (2) all participants have identical measurement results when the discussion bit is selected from the raw key bits.

Therefore, for the 1st measurement property, the malicious repeater adjusts $U_e$ to ensure that the following equation holds:

$$a_j \left| e_j \right\rangle = \overrightarrow{0}, \text{ if } wt\left(j\right) \text{ is odd}, \tag{19}$$

where $wt\left(j\right)$ denotes the Hamming weight of $j$.

Next, considering the 2nd measurement property, because the protocol participants perform $H$ operations on their qubits, the state shown in *Eq. (18)* can be modified as follows:

$$\begin{aligned} &H^{\otimes n} \cdot U_e \left( \left| \Psi \right\rangle_{12\ldots n} \otimes \left| E \right\rangle \right) \\ &= \frac{1}{\sqrt{2^n}} \sum_{k=0}^{2^n-1} \left| k_{(2)} \right\rangle_{12\ldots n} \otimes \sum_{j=0}^{2^n-1} (-1)^{wt\left(j_{(2)} \& k_{(2)}\right)} a_j \left| e_j \right\rangle, \end{aligned} \tag{20}$$

where $k_{(2)}$ denotes the binary format of $k$ and & denotes the bitwise AND operation. To pass the public discussion on the 2nd measurement property, the malicious repeater must set $\sum_{j=0}^{2^{n-1}} (-1)^{wt\left(j \& k_{(2)}\right)} a_j \left| e_j \right\rangle = \overrightarrow{0}$ if $0 < k < 2^{n-1}$. Therefore, the states expressed in *Eq. (20)* are transformed into the following equation.

$$\begin{aligned} &H^{\otimes n} \cdot U_e \left( \left| \Psi \right\rangle_{12\ldots n} \otimes \left| E \right\rangle \right) \\ &= \left| 0_{(2)} \right\rangle_{12\ldots n} \otimes \sum_{j=0}^{2^n-1} (-1)^{wt\left(j_{(2)} \& 0_{(2)}\right)} a_j \left| e_j \right\rangle + \left| \left(2^n - 1\right)_{(2)} \right\rangle_{12\ldots n} \\ &\quad \otimes \sum_{j=0}^{2^n-1} (-1)^{wt\left(j_{(2)} \& \left(2^n-1\right)_{(2)}\right)} a_j \left| e_j \right\rangle \end{aligned} \tag{21}$$

To pass the public discussion on the 1st and 2nd measurement properties, the malicious repeater must let $U_e$ conform to *Eqs. (19)* and *(21)*, respectively. From the base property of the bitwise AND operation, we can infer that $wt\left(j_{(2)} \& 0_{(2)}\right) = 0$ and $wt\left(j_{(2)} \& 2^{n-1}_{(2)}\right) = wt\left(j_{(2)}\right)$. Then, $wt\left(j_{(2)}\right)$ must be even depending on the setting of *Eq. (19)*. Therefore, the states in *Eq. (21)* can be expressed as follows:

$$\begin{aligned} H^{\otimes n} \cdot U_e \left( \left| \Psi \right\rangle_{12\ldots n} \otimes \left| E \right\rangle \right) &= \left| 0_{(2)} \right\rangle_{12\ldots n} \otimes \sum_{j=0}^{2^n-1} a_j \left| e_j \right\rangle + \left| \left(2^n - 1\right)_{(2)} \right\rangle_{12\ldots n} \otimes \sum_{j=0}^{2^n-1} a_j \left| e_j \right\rangle \\ &= \frac{1}{\sqrt{2}} \left( \left| 0_{(2)} \right\rangle + \left| \left(2^n - 1\right)_{(2)} \right\rangle \right)_{12\ldots n} \otimes \sum_{j=0}^{2^n-1} a_j \left| e_j \right\rangle \end{aligned} \tag{22}$$

If we remove the effect of $H^{\otimes n}$ in *Eq. (22)*, the following equation is obtained.

$$\begin{aligned} U_e\left(|\Psi\rangle_{12\ldots n}\otimes|\ E\rangle\right) &= H^{\otimes n}\otimes I\left(\frac{1}{\sqrt{2}}\left(\left|0_{(2)}\right\rangle+\left|2^{n-1}_{(2)}\right\rangle\right)_{12\ldots n}\otimes\sum_{j=0}^{2^{n-1}}a_j\left|e_j\right\rangle\right) \\ &= \frac{1}{\sqrt{2^{n-1}}}\sum_{j=0}^{2^n-1}\left|j_{(2)}\right\rangle_{12\ldots n}\otimes\sum_{j=0}^{2^n-1}a_j\left|e_j\right\rangle,\ \text{where} wt\left(j\right)\ \text{is even} \\ &= \frac{1}{\sqrt{2}}\left(|++\cdots+\rangle+|--\cdots-\rangle\right)_{12\ldots\mathrm{n}}\otimes\sum_{j=0}^{2^n-1}a_j\left|e_j\right\rangle \end{aligned} \tag{23}$$

Therefore, to pass the participants' public discussions, a malicious repeater must adjust $U_e$ to conform to *Eq. (23)*. It is evident that *Eq. (23)* represents the product state of the GHZ-like and ancillary qubits. Consequently, a malicious repeater cannot infer the secret key bit of any participant. If the malicious repeater attempts to extract the information about the secret keys, Alice and the other participants have a probability, above zero, of identifying the attacker's actions. Therefore, the proposed M-MQKD protocol has robustness under collective attacks. □

### *5.1.2 Collusion attack*

To demonstrate that the proposed M-MQKD protocol is robust against various attacks, this study examines a worst-case scenario: a collusion attack, discussed in this section. In this attack scenario, we assume that all quantum repeaters are malicious and collaborate to steal information about the participants' secret keys. Since all the repeaters are acting maliciously, we can treat them as a single attacker, referred to as Eve, who assists the protocol participants in distributing a GHZ-like state. Eve does not follow the processes of the proposed protocol to distribute GHZ-like states. Instead, she attempts to obtain the participants' measurement results by distributing alternative quantum states. To achieve this, she can distribute two types of states: (1) GHZ-like states with probes and (2) product states.

If Eve distributes GHZ-like states embedded with probes to all participants and attempts to measure these probes to extract the participants' measurement results, her attack will inevitably be detected. This is because her strategy is the same as the collective attack, which participants can detect. When Eve tries to steal the participants' measurement results by using the product state, she needs to generate specific product states which can pass the check of Step 4 in the proposed M-MQKD protocol. For the check of *Share mode*, she can generate $|+\rangle^{\otimes n+1}$ or $|-\rangle^{\otimes n+1}$. Alternatively, for the *Check mode*, she can generate $\otimes_{i=1}^{n+1}|\ v_i\rangle$ in Z-basis, where $\oplus_{i=1}^{n+1}v_i=0$ and $v_i\in\{0,1\}$.

Since the participants randomly chose between *Share* and *Check modes*, Eve cannot determine which mode was selected in any session. If she distributes $\otimes_{i=1}^{n+1}|v_i\rangle$ to the participants, and all of them choose the *Sharing mode* during a session, her attack behavior can go undetected with a probability of $\left(\frac{3}{4}\right)^n$. That is because each participant's measurement result must match Alice's, and the probability of $\mathrm{Bob_i}$'s measurement result matching Alice's is $\frac{3}{4}$, where $i=\{1,2,\ldots,n\}$. Therefore, the probability that Eve's attack remains undetected in a single check session is $\left(\frac{3}{4}\right)^n$. Since the participants use $l$ raw key bits for checking, the overall probability that Eve's attack goes undetected over the entire check session of

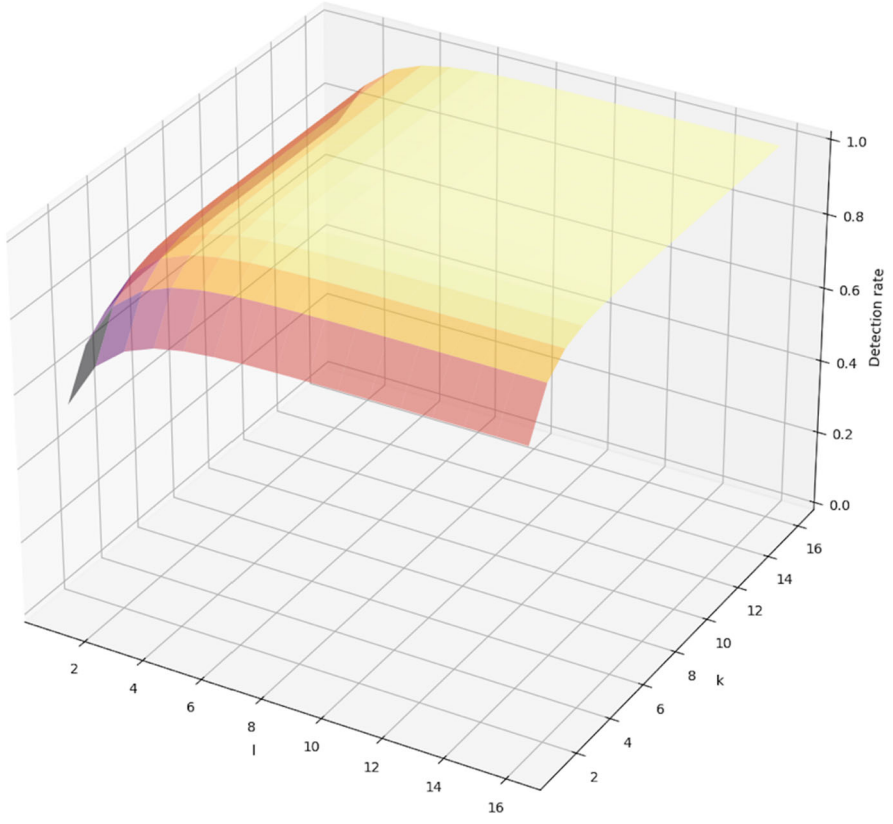


**Figure 12** Detection rate analysis of collusion attack

is $\left(\frac{3}{4}\right)^{ln}$. On the other hand, she distributes either $|+\rangle^{\otimes n+1}$ or $|-\rangle^{\otimes n+1}$ to the participants, and all of them choose the *Check mode* during a session. If the XOR result of all $\text{Bob}_\text{i}$'s measurement results (i.e., $\oplus_{j=1}^{n} cb_{B_j}^{i}$) is equal to Alice's measurement result (i.e., $cb_A^i$), the participants will not detect Eve's attack behavior. Because the probability that the measurement result of each $\text{Bob}_\text{i}$ and Alice being 0 or 1 is $\frac{1}{2}$, the probability of $\oplus_{j=1}^{n} cb_{B_j}^{i} = cb_A^i$ is $\frac{1}{2}$. Assume there are $k$ check bits consumed by each participant, the overall probability that Eve's attack goes undetected over the entire check session of is $\left(\frac{1}{2}\right)^k$.

Because the participants choose *Sharing* or *Check mode* with the payability of $\frac{1}{2}$, the final probability of detecting Eve's attack is $1 - \frac{1}{2}\left(\left(\frac{3}{4}\right)^{ln} + \left(\frac{1}{2}\right)^k\right)$. To clearly illustrate the analysis results of the collusion attack, Fig. 12 presents the detection rates under various values of $l$ and $k$ with three participants fixed (i.e., $n = 3$). According to the detection rate analysis, there is an approximate 100% probability that the participants can detect Eve's attack when $l$ and $k$ are greater than a certain value (e.g. $l \geq 5$ and $k \geq 10$ or $l \geq 6$ and $k \geq 8$). This demonstrates that the proposed M-MQKD protocol remains robust against collusion attacks.

### *5.1.3 Trojan horse attack*

Quantum Trojan horse assaults, as referenced in [63, 64], represent a category of attacks contingent upon specific implementations, whereby an attacker employs strategies like using undetectable or deferred photons to stealthily acquire confidential information from participants unnoticed. Because the attacker can only extract the information regarding

participant operations when retrieving Trojan horse photons, these attacks are most effective during two-way or circular quantum transmissions. In contrast, one-way quantum communication, in which the qubits are not returned, prevents attackers from retrieving the secret information because they cannot reclaim the attack qubits.

While protocols that utilize two-way or circular quantum communication methods can address these attacks by incorporating extra quantum devices or strategies, like the use of the specific technique addressed by Boyer et al. [65], the proposed M-MQKD protocol inherently counters quantum Trojan horse attacks through its adoption of one-way communication. This one-way method not only circumvents the complexities associated with such attacks but also facilitates a reduced transmission distance for qubits compared to those required in two-way or circular communication schemes. Consequently, this leads to lower qubit transmission costs relative to the expenses associated with protocols that depend on circular quantum communication.

### 5.2 Comparison and simulation

To illustrate the practical superiority of the proposed M-MQKD protocol over the existing MSQKD [47–50] protocol in a general quantum network environment, this study compared the types of quantum resources, quantum capability of the protocol participants, quantum communication methods, limitation on transmission distance, additional devices/mechanisms for Trojan horse attacks, and application network of these protocols. A comparison of the results is shown in *Table 3*.

Although the proposed protocol adopts a graph state for the design, the main cost of generating and distributing the graph state is borne by the quantum repeaters with sufficient quantum capabilities and resources. In addition, with the assistance of quantum repeaters, the proposed protocol can overcome the limitations of quantum communication distance and allow the participants to achieve the goal of key distribution in a general quantum network. Notably, Zhang et al.'s protocol [47] is more practical in terms of implementation

**Table 3** Comparison between proposed protocol and existing MSQKD protocols

| | This study | Zhang et al. [47] | Zhou et al. [48] | Tian et al. [49] | Ye et al. [50] |
|---|---|---|---|---|---|
| Quantum resource | Graph state | Single photon | Cluster state | Hyperentangled Bell state | Bell state |
| Quantum capability of classical participants | 1. Performing Pauli and $H$ operations<br>2. Measuring qubits in Z-basis | 1. Generating qubits in Z-basis<br>2. Reflecting qubits without disturbance<br>3. Measuring qubits in Z-basis | | | |
| Quantum communication method | One-way communication | Circular communication | | | |
| Limitation of transmission distance | No | Yes | | | |
| Additional devices/mechanisms for Trojan horse attacks | No | Yes | | | |
| Application network situation | General network environment | Series network environment | | | |
| Routing algorithm | Need | No need | | | |
| Qubit efficiency | $\frac{1}{2^n n+r}$ | $\frac{1}{2^n(n+1)}$ | $\frac{1}{2^{\lfloor \frac{n}{2} \rfloor+1}(n+3)}$ | $\frac{1}{2^{n+1}(n+3)}$ | $\frac{1}{2^n(n+4)}$ |

compared to protocols using entanglement states (i.e., ours and other MSQKD protocols), as it only requires single photons in two complementary bases. Therefore, designing an MSQKD protocol that uses single photons within a general network environment remains an unresolved challenge. In terms of quantum capabilities, the proposed protocol is more lightweight than existing protocols since classical users only need two quantum capabilities instead of the three required in other protocols. While other MSQKD protocols with circular communication can incorporate additional devices or mechanisms to resist quantum Trojan horse attacks, the proposed protocol is inherently immune to such attacks. Additionally, although our protocol does not impose any limitations on transmission distance, it does require an additional quantum network routing algorithm. Compared to other MSQKD protocols designed for series network environments, this algorithm adds an extra cost. However, this cost is necessary for applications in a general quantum network environment.

To analyze the performance of our protocol and existing MSQKD protocols, this study calculates the qubit efficiency $\eta$ using the following equation. The calculation results are summarized in *Table 3*.

$$\eta = \frac{m}{\text{The number of qubits consumed to share } m \text{ secrets}}, \tag{24}$$

where $n$ is the number of participants and $m$ is the length of the secret key. Since the number of repeaters is not fixed in practical scenarios, we use a variable $r$ to denote the number of quantum repeaters in the comparison. Based on the results of this metric, the qubit efficiency of our protocol is less efficient than that of existing MSQKD protocols in network environments with a large number of repeaters. However, our protocol can be applied in general quantum networks, whereas the existing MSQKD protocols cannot. Although directly comparing qubit efficiency may be unfair due to the differing quantum topologies between our protocol and the existing MSQKD protocols, these results nonetheless offer valuable insights into the performance differences between the two quantum network topologies.

In addition to comparing with existing MSQKD protocols, this study further examines the differences between using the 1D+star graph state measurement properties and using entanglement swapping to achieve entanglement distribution. Simple examples (as shown in *Fig. 13*) are provided to analyze the cost of entanglement distribution between the two methods, where a repeater $R_j$ aims to distribute an entanglement state to another repeater $R_i$. This study assumes that the repeaters can generate qubits in the initial state $|0\rangle$ and use controlled gates (i.e., CNOT and CZ) to generate the entangled states. When the repeaters adopt the 1D+star graph state measurement properties, $R_j$ generates a qubit (labeled as i), performs an $H$ operation on this qubit, applies a CZ operation between qubits $j$ and $i$, and then sends qubit $i$ to $R_i$ (as shown in *Figs. 13a* and *13b*) Finally, $R_j$ measures the qubit $j$ in X-basis which requires one H operation followed by one Z-basis measurement to achieve the entanglement distribution (as shown in *Fig. 13c*). Alternatively, if the repeaters use the entanglement swapping to distribute entanglement states, $R_j$ will generate a Bell state (labeled as i and i+1), send the qubit $i$ to $R_i$, and then perform a Bell measurement between qubits $i + 1$ and $j$ (as shown in *Figs. 13d* and *13e*) to complete the entanglement distribution (as shown in *Fig. 13f).* Generating a Bell state requires generation of 2 qubits, one $H$ operation, and one CNOT operation, and performing Bell measurement requires one

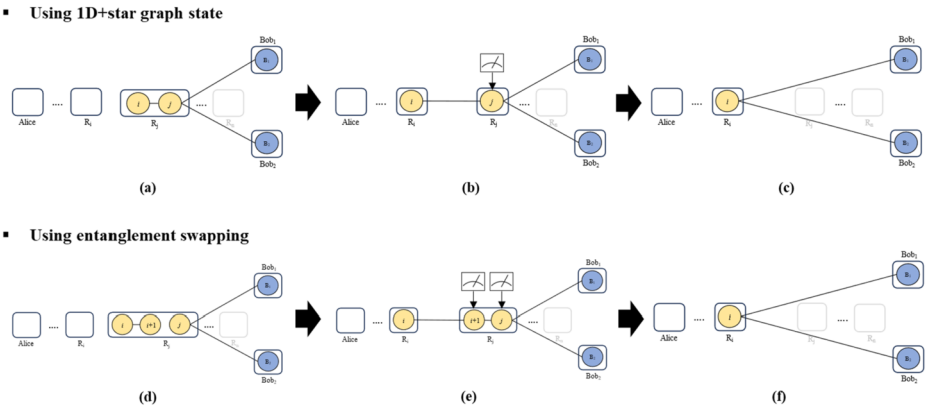


**Figure 13** Examples of entanglement distribution using our method and entanglement swapping

**Table 4** Cost comparison between our method and entanglement swapping

| Method | Number of generating qubits | Controlled gate | Hadamard operation | Z-basis measurement |
|---|---|---|---|---|
| Our method | 1 | 1 | 2 | 1 |
| Entanglement Swapping | 2 | 2 | 2 | 2 |

CNOT operation, one $H$ operation and two Z-basis measurement. The costs of entanglement distribution are summarized in *Table 4*. From the cost comparisons, we can see that our proposed method reduces the number of qubits generated, eliminates the need for one controlled gate, and requires one less Z-basis measurement. Importantly, compared to single-photon gates, implementing controlled gates is more resource-intensive. Therefore, using the measurement properties of the 1D+star graph state to distribute entangled states is more efficient than entanglement swapping in the context of our protocol.

The proposed protocol was implemented via simulation software to verify the proposed characteristics of the graph states with the 1D+star type and analyze the realizability of the proposed M-MQKD protocol. To design a protocol tailored to quantum communication, this study used NetSquid [66], a dedicated simulation tool for quantum networks. This choice was made due to NetSquid's specific applicability to quantum networking scenarios.

During the simulation trials, the proposed M-MQKD protocol was executed under two distinct scenarios: (1) a quantum network with a fixed number of participants and varying numbers of repeaters, and (2) a quantum network with a varying number of participants but a fixed number of repeaters. Additionally, two types of noise—depolarizing and dephasing—were analyzed in both experimental scenarios to assess their effects on the success rate of establishing graph states.

In the first scenario, the study assumes the presence of three participants (Alice, $\text{Bob}_1$, and $\text{Bob}_2$) who aim to distribute secret keys. Due to limited computer resources available for the experiment, a quantum network environment with a maximum of 20 repeaters was simulated. Thus, environments with 1 to 20 repeaters were explored. In each scenario, repeaters helped participants establish 1024 graph states, and the average of these results was used to calculate success rates. The results for depolarizing and dephasing noise environments are presented in *Fig. 14* and summarized in *Tables 5* and 6, respectively. The

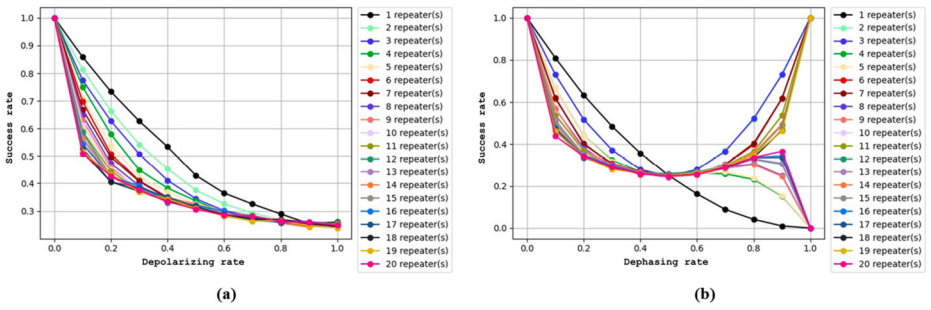


**Figure 14** Simulation results for the quantum network with various numbers of repeaters

**Table 5** Experiment results in the quantum network with various numbers of repeaters for depolarizing noise

| % of noise | # of repeaters | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 0 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| 0.1 | 0.86 | 0.81 | 0.77 | 0.75 | 0.71 | 0.70 | 0.67 | 0.65 | 0.60 | 0.61 | 0.59 | 0.58 | 0.57 | 0.56 | 0.54 | 0.54 | 0.53 | 0.51 | 0.52 | 0.51 |
| 0.2 | 0.73 | 0.66 | 0.63 | 0.58 | 0.54 | 0.51 | 0.50 | 0.47 | 0.46 | 0.45 | 0.44 | 0.43 | 0.43 | 0.42 | 0.42 | 0.42 | 0.40 | 0.41 | 0.43 | 0.43 |
| 0.3 | 0.63 | 0.54 | 0.51 | 0.45 | 0.42 | 0.41 | 0.41 | 0.39 | 0.37 | 0.38 | 0.37 | 0.38 | 0.38 | 0.37 | 0.38 | 0.39 | 0.38 | 0.37 | 0.37 | 0.38 |
| 0.4 | 0.53 | 0.45 | 0.41 | 0.38 | 0.37 | 0.35 | 0.35 | 0.34 | 0.35 | 0.34 | 0.35 | 0.35 | 0.33 | 0.34 | 0.33 | 0.33 | 0.35 | 0.34 | 0.34 | 0.33 |
| 0.5 | 0.43 | 0.38 | 0.34 | 0.34 | 0.33 | 0.32 | 0.31 | 0.31 | 0.32 | 0.31 | 0.31 | 0.31 | 0.32 | 0.32 | 0.32 | 0.32 | 0.31 | 0.31 | 0.31 | 0.31 |
| 0.6 | 0.36 | 0.33 | 0.30 | 0.29 | 0.30 | 0.30 | 0.30 | 0.29 | 0.30 | 0.29 | 0.29 | 0.29 | 0.30 | 0.30 | 0.29 | 0.30 | 0.28 | 0.29 | 0.28 | 0.29 |
| 0.7 | 0.32 | 0.29 | 0.28 | 0.28 | 0.27 | 0.28 | 0.28 | 0.27 | 0.27 | 0.28 | 0.27 | 0.27 | 0.28 | 0.28 | 0.28 | 0.20 | 0.28 | 0.20 | 0.26 | 0.28 |
| 0.8 | 0.29 | 0.27 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.27 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.27 | 0.27 | 0.26 |
| 0.9 | 0.25 | 0.25 | 0.26 | 0.24 | 0.25 | 0.26 | 0.25 | 0.26 | 0.25 | 0.25 | 0.26 | 0.26 | 0.25 | 0.24 | 0.25 | 0.26 | 0.26 | 0.25 | 0.25 | 0.26 |
| 1.0 | 0.26 | 0.25 | 0.20 | 0.26 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.24 | 0.25 | 0.25 | 0.24 | 0.24 | 0.24 | 0.24 | 0.25 |

**Table 6** Experiment results in the quantum network with various numbers of repeaters for dephasing noise

| % of noise | # of repeaters | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 0 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| 0.1 | 0.81 | 0.73 | 0.73 | 0.66 | 0.66 | 0.62 | 0.62 | 0.57 | 0.57 | 0.54 | 0.54 | 0.51 | 0.51 | 0.49 | 0.50 | 0.48 | 0.47 | 0.46 | 0.46 | 0.44 |
| 0.2 | 0.63 | 0.52 | 0.52 | 0.44 | 0.44 | 0.40 | 0.40 | 0.38 | 0.37 | 0.37 | 0.30 | 0.35 | 0.35 | 0.35 | 0.35 | 0.34 | 0.34 | 0.34 | 0.34 | 0.34 |
| 0.3 | 0.49 | 0.37 | 0.37 | 0.32 | 0.32 | 0.31 | 0.30 | 0.29 | 0.30 | 0.29 | 0.28 | 0.29 | 0.30 | 0.29 | 0.29 | 0.30 | 0.29 | 0.29 | 0.28 | 0.29 |
| 0.4 | 0.36 | 0.28 | 0.28 | 0.27 | 0.26 | 0.26 | 0.27 | 0.26 | 0.27 | 0.26 | 0.26 | 0.26 | 0.25 | 0.25 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 |
| 0.5 | 0.25 | 0.25 | 0.25 | 0.25 | 0.26 | 0.25 | 0.25 | 0.24 | 0.24 | 0.25 | 0.25 | 0.26 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 | 0.25 |
| 0.6 | 0.16 | 0.28 | 0.28 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.25 | 0.27 | 0.26 | 0.27 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.26 | 0.25 |
| 0.7 | 0.09 | 0.37 | 0.37 | 0.26 | 0.27 | 0.30 | 0.30 | 0.29 | 0.28 | 0.30 | 0.30 | 0.29 | 0.29 | 0.29 | 0.29 | 0.28 | 0.29 | 0.29 | 0.29 | 0.20 |
| 0.8 | 0.04 | 0.52 | 0.52 | 0.23 | 0.24 | 0.40 | 0.40 | 0.31 | 0.30 | 0.37 | 0.36 | 0.33 | 0.33 | 0.36 | 0.35 | 0.34 | 0.34 | 0.34 | 0.35 | 0.34 |
| 0.9 | 0.01 | 0.73 | 0.73 | 0.15 | 0.15 | 0.62 | 0.62 | 0.25 | 0.25 | 0.54 | 0.54 | 0.30 | 0.31 | 0.50 | 0.49 | 0.34 | 0.34 | 0.47 | 0.46 | 0.37 |
| 1.0 | 0.00 | 1.00 | 1.00 | 0.00 | 0.00 | 1.00 | 1.00 | 0.00 | 0.00 | 1.00 | 1.00 | 0.00 | 0.00 | 1.00 | 1.00 | 0.00 | 0.00 | 1.00 | 1.00 | 0.00 |

simulations reveal that a 100% success rate in establishing graph states is possible with the help of various numbers of repeaters in an ideal quantum channel (with a 0% noise rate), demonstrating the feasibility of designing the proposed M-MQKD protocol for a quantum network with any number of repeaters. In depolarizing noise environments (*Fig. 14a*), an increase in noise rate leads to a decrease in success rate, especially when more repeaters are used, showing a more pronounced decline. It is worth noting that in dephasing noise environments (*Fig. 14b*), an unexpected phenomenon occurs at certain numbers of repeaters (e.g., 3, 7, 11,…), where the success rate actually improves as the noise rate in-

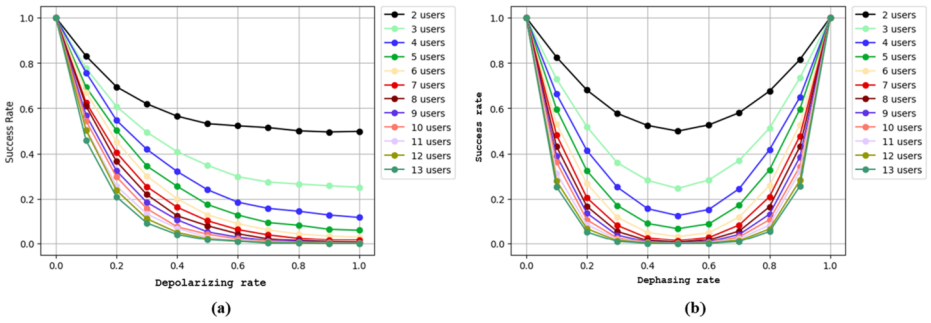


**Figure 15** Simulation results for the quantum network with various numbers of participants

**Table 7** Experiment results in the protocol with various numbers of participants for depolarizing noise

| % of noise | # of participants | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 0 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| 0.1 | 0.83 | 0.78 | 0.76 | 0.69 | 0.67 | 0.62 | 0.61 | 0.57 | 0.54 | 0.51 | 0.50 | 0.46 |
| 0.2 | 0.69 | 0.61 | 0.55 | 0.50 | 0.45 | 0.40 | 0.36 | 0.32 | 0.30 | 0.26 | 0.24 | 0.21 |
| 0.3 | 0.62 | 0.49 | 0.42 | 0.34 | 0.30 | 0.25 | 0.22 | 0.18 | 0.16 | 0.13 | 0.11 | 0.09 |
| 0.4 | 0.56 | 0.41 | 0.32 | 0.25 | 0.20 | 0.16 | 0.12 | 0.11 | 0.08 | 0.07 | 0.05 | 0.04 |
| 0.5 | 0.53 | 0.35 | 0.24 | 0.17 | 0.13 | 0.10 | 0.08 | 0.05 | 0.04 | 0.03 | 0.02 | 0.02 |
| 0.6 | 0.52 | 0.30 | 0.18 | 0.13 | 0.09 | 0.06 | 0.05 | 0.03 | 0.02 | 0.01 | 0.01 | 0.01 |
| 0.7 | 0.51 | 0.27 | 0.16 | 0.09 | 0.06 | 0.04 | 0.02 | 0.02 | 0.01 | 0.01 | 0.00 | 0.00 |
| 0.8 | 0.50 | 0.27 | 0.14 | 0.08 | 0.04 | 0.02 | 0.01 | 0.01 | 0.00 | 0.00 | 0.00 | 0.00 |
| 0.9 | 0.50 | 0.26 | 0.13 | 0.07 | 0.04 | 0.02 | 0.01 | 0.01 | 0.00 | 0.00 | 0.00 | 0.00 |
| 1.0 | 0.50 | 0.25 | 0.12 | 0.06 | 0.03 | 0.02 | 0.01 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |

creases. This counterintuitive result arises because a 1D+star graph state with a specific number of qubits is immune to collective dephasing noise. Collective noise refers to quantum noise that affects multiple qubits simultaneously in a correlated manner, with collective dephasing noise being one such example. In the presence of collective noise, certain special quantum states, known as "free states," can resist this type of disturbance. Due to the dephasing-free property of certain 1D+star graph states, the success rate improves once the noise rate exceeds 0.5. Remarkably, the success rate reaches 1.0 when the noise rate is 100%, indicating a fully collective noise environment. Based on these simulation results, we conclude that these 1D+star graph states are dephasing-free states, making them suitable for designing other dephasing-tolerant quantum communication protocols.

In the second scenario, the study includes three repeaters aiding various participants (e.g., Alice, $\mathrm{Bob}_1$, $\mathrm{Bob}_2$, …, $\mathrm{Bob}_n$) in establishing graph states. Again, due to the limitation of computer resources, a quantum network environment with up to 13 participants was simulated. The results for depolarizing and dephasing noise environments are presented in *Fig. 15* and summarized in *Tables 7* and 8, respectively. Similar to the first scenario, it's evident that graph states can be perfectly established with various numbers of participants in an ideal quantum channel. Furthermore, the number of participants significantly impacts the success rate in different depolarizing noise conditions (*Fig. 15a*). Similar to the analysis of the previous scenario, the 1D+star graph state can also withstand collective dephasing noise when the 1D part contains 4 qubits, as demonstrated by the results under dephasing noise conditions (*Fig. 15b*). This finding further reinforces the potential of the

**Table 8** Experiment results in the protocol with various numbers of participants for dephasing noise

| % of noise | # of participants | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 0 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |
| 0.1 | 0.83 | 0.73 | 0.66 | 0.60 | 0.53 | 0.48 | 0.43 | 0.39 | 0.36 | 0.31 | 0.28 | 0.25 |
| 0.2 | 0.68 | 0.52 | 0.41 | 0.32 | 0.27 | 0.20 | 0.17 | 0.14 | 0.11 | 0.09 | 0.07 | 0.05 |
| 0.3 | 0.58 | 0.36 | 0.25 | 0.17 | 0.12 | 0.08 | 0.06 | 0.04 | 0.03 | 0.02 | 0.01 | 0.01 |
| 0.4 | 0.52 | 0.28 | 0.16 | 0.09 | 0.05 | 0.03 | 0.02 | 0.01 | 0.01 | 0.00 | 0.00 | 0.00 |
| 0.5 | 0.50 | 0.25 | 0.13 | 0.07 | 0.03 | 0.01 | 0.01 | 0.00 | 0.00 | 0.00 | 0.00 | 0.00 |
| 0.6 | 0.53 | 0.28 | 0.15 | 0.09 | 0.05 | 0.03 | 0.02 | 0.01 | 0.01 | 0.00 | 0.00 | 0.00 |
| 0.7 | 0.58 | 0.37 | 0.24 | 0.17 | 0.12 | 0.08 | 0.06 | 0.04 | 0.03 | 0.02 | 0.02 | 0.01 |
| 0.8 | 0.68 | 0.51 | 0.42 | 0.33 | 0.26 | 0.21 | 0.16 | 0.13 | 0.11 | 0.08 | 0.07 | 0.06 |
| 0.9 | 0.81 | 0.73 | 0.65 | 0.60 | 0.53 | 0.48 | 0.43 | 0.38 | 0.34 | 0.32 | 0.28 | 0.26 |
| 1.0 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 | 1.00 |

1D+star graph state for future developments in dephasing-tolerant quantum communication protocols.

Finally, this research meticulously compiles and discusses the outcomes derived from conducting two distinct simulation experiments aimed at exploring quantum networking. In a noisy quantum network environment, the number of qubits significantly influences the success rate of establishing entanglement. Since the number of participants in real applications is fixed, reducing the number of repeaters in the routing path emerges as a solution to mitigate the impact of noise. Thus, employing fewer repeaters (i.e., creating shorter routing paths) for key distribution is crucial for enhancing qubit efficiency.

Additionally, there are certain types of noise that were not considered or discussed in the simulations of this study. These noises—such as photon loss, relaxation, gate errors, dark counts in measurement devices, and others—could pose potential limitations to the proposed entanglement distribution method and M-MQKD protocol. For example, they could affect the communication distances and success rates of the proposed protocol. Analyzing the complexities of quantum network environments requires a separate, comprehensive research effort, which is beyond the scope of this work. Therefore, we consider these analyses as future work.

## 6 Conclusion

The existing MSQKD and M-MSQKD protocols have two challenges: (1) the need for additional devices to defend against quantum Trojan horse attacks and (2) conformance to a specific network environment, namely, the series network. Therefore, this study proposes a property of 1D+star graph state and then uses this property to distribute GHZ-like states among classical participants within a general repeater-based quantum network. These GHZ-like states are then used to propose an M-MQKD protocol, specifically designed for a restricted quantum environment. In the proposed M-MQKD protocol, the classical participants have only two quantum capabilities—single-qubit operation (i.e., $\sigma_Z$ and $H$) and Z-basis measurement—and they do not need an additional quantum device/mechanism to protect against quantum Trojan horse attacks. Moreover, unlike the existing repeater-based quantum network, repeaters use single-qubit measurement (i.e., X-basis measurement) rather than the entanglement swapping to transmit the entanglement. Therefore, the proposed M-MQKD protocol is more practical and lightweight than the existing MSQKD and M-MSQKD protocols. Security analyses and simulation exper-

iments were conducted to prove that the proposed M-MQKD protocol is secure and feasible.

Our future research could explore leveraging the proposed measurement properties of the 1D+star graph state to develop additional lightweight and practical quantum communication protocols within quantum networks (e.g., quantum secret sharing). Furthermore, designing a routing algorithm for efficiently distributing the graph state among protocol participants is another promising direction. However, there are potential limitations and challenges for our method in larger quantum networks with complex noise environments. For instance, what is the maximum distance in our proposed protocol that can securely distribute keys in a noisy network? Therefore, the unresolved issues include analyzing the key rate bound in complex noisy quantum networks, mitigating decoherence, extending the storage time of entangled states, and designing efficient quantum error correction codes and purification techniques.

**Abbreviations**
QKD, Quantum Key Distribution; M-MQKD, Mediated Multiparty Quantum Key Distribution; QSS, Quantum Secret Sharing; SQKD, Semi-Quantum Key Distribution; TP, Third Party; MSQKD, Multiparty Semi-Quantum Key Distribution; M-MSQKD, Mediated Multiparty Semi-Quantum Key Distribution.

**Author contributions**
Chia-Wei Tsai: Conceptualization, Methodology, Formal Analysis, Writing – Original Draft. Chun-Hsiang Wang: Experimentation and Review manuscript.

**Funding**
Project supported by the National Science and Technology Council, Taiwan, R.O.C. (Grant Nos. NSTC 113-2221-E-025-014 and NSTC 113-2634-F-005-001-MBK).

**Data Availability**
No datasets were generated or analysed during the current study.

## Declarations

**Ethics approval and consent to participate**
Not applicable.

**Consent for publication**
Not applicable.

**Competing interests**
The authors declare no competing interests.

Received: 4 August 2024 Accepted: 18 September 2024 Published online: 27 September 2024

**References**

1. Bennett CH, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: IEEE int. conf. Computers, systems and signal processing, Bangalore, India. 1984. p. 175–9.
2. Shor PW, Preskill J. Simple proof of security of the BB84 quantum key distribution protocol. Phys Rev Lett. 2000;85(2):441–4.
3. Gottesman D, Lo H-K. Proof of security of quantum key distribution with two-way classical communications. IEEE Trans Inf Theory. 2003;49(2):457–75.
4. Tsurumaru T, Tamaki K. Security proof for quantum-key-distribution systems with threshold detectors. Phys Rev A. 2008;78(3):032302.
5. Bennett CH, Brassard G, Mermin ND. Quantum cryptography without Bell's theorem. Phys Rev Lett. 1992;68(5):557–9.
6. Cerf NJ, Bourennane M, Karlsson A, Gisin N. Security of quantum key distribution using d-level systems. Phys Rev Lett. 2002;88(12):127902.
7. Long G-L, Liu X-S. Theoretically efficient high-capacity quantum-key-distribution scheme. Phys Rev A. 2002;65(3):032302.
8. Grosshans F, Van Assche G, Wenger J, Brouri R, Cerf NJ, Grangier P. Quantum key distribution using Gaussian-modulated coherent states. Nature. 2003;421(6920):238–41.
9. Hwang W-Y. Quantum key distribution with high loss: toward global secure communication. Phys Rev Lett. 2003;91(5):057901.
10. Lo HK, Ma XF, Chen K. Decoy state quantum key distribution. Phys Rev Lett. 2005;94(23):230504.

11. Hwang T, Lee KC, Li CM. Provably secure three-party authenticated quantum key distribution protocols. IEEE Trans Dependable Secure Comput. 2007;4(1):71–80.
12. Li X-H, Deng F-G, Zhou H-Y. Efficient quantum key distribution over a collective noise channel. Phys Rev A. 2008;78(2):022321.
13. Hwang T, Hwang CC, Tsai CW. Quantum key distribution protocol using dense coding of three-qubit W state. Eur Phys J D. 2011;61:785–90.
14. Lo H-K, Curty M, Qi B. Measurement-device-independent quantum key distribution. Phys Rev Lett. 2012;108(13):130503.
15. Yang C-W. New probabilistic quantum key distribution protocol. Int J Theor Phys. 2018;57(12):3651–7.
16. Hillery M, Bužek V, Berthiaume A. Quantum secret sharing. Phys Rev A. 1999;59(3):1829.
17. Gottesman D. Theory of quantum secret sharing. Phys Rev A. 2000;61(4):042311.
18. Zhang Z-J, Li Y, Man Z-X. Multiparty quantum secret sharing. Phys Rev A. 2005;71(4):044301.
19. Hsu JL, Chong SK, Hwang T, Tsai CW. Dynamic quantum secret sharing. Quantum Inf Process. 2013;12:331–44.
20. Deng F-G, Long GL. Secure direct communication with a quantum one-time pad. Phys Rev A. 2004;69(5):052319.
21. Long GL, Deng FG, Wang C, Li XH, Wen K, Wang WY. Quantum secure direct communication and deterministic secure quantum communication. Front Phys China. 2007;2:251–72.
22. Zhang W, Ding DS, Sheng YB, Zhou L, Shi BS, Guo GC. Quantum secure direct communication with quantum memory. Phys Rev Lett. 2017;118(22):220501.
23. Yang YG, Cao WF, Wen QY. Secure quantum private comparison. Phys Scr. 2009;80(6):065002.
24. Yang YG, Wen QY. An efficient two-party quantum private comparison protocol with decoy photons and two-photon entanglement. J Phys A, Math Theor. 2009;42(5):055305.
25. Liu W, Liu C, Wang H, Jia T. Quantum private comparison: a review. IETE Tech Rev. 2013;30(5):439–45.
26. Fitzsimons JF. Private quantum computation: an introduction to blind quantum computing and related protocols. npj Quantum Inf. 2017;3(1):23.
27. Boyer M, Kenigsberg D, Mor T. Quantum key distribution with classical Bob. In: 2007 first int. conf. Quantum, nano, and micro technologies (ICQNM'07), Guadeloupe, French Caribbean, Jan. 2–5. IEEE; 2007. p. 2–5.
28. Boyer M, Gelles R, Kenigsberg D, Mor T. Semiquantum key distribution. Phys Rev A. 2009;79(3):032341.
29. Zou X, Qiu D, Li L, Wu L, Li L. Semiquantum-key distribution using less than four quantum states. Phys Rev A. 2009;79(5):052312.
30. Wang J, Zhang S, Zhang Q, Tang CJ. Semiquantum key distribution using entangled states. Chin Phys Lett. 2011;28(10):100301.
31. Yu K-F, Yang C-W, Liao C-H, Hwang T. Authenticated semi-quantum key distribution protocol using Bell states. Quantum Inf Process. 2014;13:1457–65.
32. Zou X, Qiu D, Zhang S, Mateus P. Semiquantum key distribution without invoking the classical party's measurement capability. Quantum Inf Process. 2015;14:2981–96.
33. Li Q, Chan WH, Zhang S. Semiquantum key distribution with secure delegated quantum computation. Sci Rep. 2016;6(1):19898.
34. Li Q, Chan WH, Long DY. Semiquantum secret sharing using entangled states. Phys Rev A. 2010;82(2):022303.
35. Yang CW, Hwang T. Efficient key construction on semi-quantum secret sharing protocols. Int J Quantum Inf. 2013;11(05):1350052.
36. Tsai CW, Yang CW, Lee NY. Semi-quantum secret sharing protocol using W-state. Mod Phys Lett A. 2019;34(27):1950213.
37. Chou WH, Hwang T, Gu J. Semi-quantum private comparison protocol under an almost-dishonest third party. 2016. ArXiv preprint. arXiv:1607.07961.
38. Lang Y-F. Semi-quantum private comparison using single photons. Int J Theor Phys. 2018;57:3048–55.
39. Ye T-Y, Ye C-Q. Measure-resend semi-quantum private comparison without entanglement. Int J Theor Phys. 2018;57:3819–34.
40. Zou X, Qiu D. Three-step semiquantum secure direct communication protocol. Sci China, Phys Mech Astron. 2014;57:1696–702.
41. Zhang M-H, Li H-F, Xia Z-Q, Feng X-Y, Peng J-Y. Semiquantum secure direct communication using EPR pairs. Quantum Inf Process. 2017;16:1–14.
42. Yang CW. Efficient and secure semi-quantum secure direct communication protocol against double CNOT attack. Quantum Inf Process. 2020;19:1–15.
43. Krawec WO. Mediated semiquantum key distribution. Phys Rev A. 2015;91(3):032323.
44. Lin P-H, Tsai C-W, Hwang T. Mediated semi-quantum key distribution using single photons. Ann Phys. 2019;531(8):1800347.
45. Chen L, Li Q, Liu C, Peng Y, Yu F. Efficient mediated semi-quantum key distribution. Phys A, Stat Mech Appl. 2021;582:126265.
46. Guskind J, Krawec WO. Mediated semi-quantum key distribution with improved efficiency. Quantum Sci Technol. 2022;7(3):035019.
47. Zhang X-Z, Gong W-G, Tang Y-G, Ren Z-Z, Guo X-T. Quantum key distribution series network protocol with M-classical Bobs. Chin Phys B. 2009;18(6):2143.
48. Zhou NR, Zhu KN, Zou XF. Multi-party semi-quantum key distribution protocol with four-particle cluster states. Ann Phys. 2019;531(8):1800520.
49. Tian Y, Li J, Ye C, Li C. Multi-party semi-quantum key distribution protocol based on hyperentangled Bell states. Front Phys. 2022;966.
50. Ye CQ, Li J, Chen XB, Hou Y, Dong M, Ota K. Circular mediated semi-quantum key distribution. Quantum Inf Process. 2023;22(4):170.
51. 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.
52. Tsai CW, Yang CW, Lin J. Multiparty mediated quantum secret sharing protocol. Quantum Inf Process. 2022;21(2):63.
53. Tsai CW, Wang CH. Efficient mediated quantum secret sharing protocol in a restricted quantum environment. Ann Phys. 2023;535(11):2300116.

54. Berkolaiko G, Kuchment P. Introduction to quantum graphs. Providence: Am. Math. Soc.; 2013.
55. Bennett CH, Brassard G, Crépeau C, Jozsa R, Peres A, Wootters WK. Teleporting an unknown quantum state via dual classsical and Einstein-Podolsky-Rosen Channles. Phys Rev Lett. 1993;70(13):1895.
56. Zukowski M, Zeilinger A, Horne MA, Ekert AK. Bell experiment via entanglement swapping. Phys Rev Lett. 1993;71:4287.
57. Bose S, Vedral V, Knight PL. Multiparticle generalization of entanglement swapping. Phys Rev A. 1998;57(2):822.
58. Caleffi M. Optimal routing for quantum networks. IEEE Access. 2017;5:22299–312.
59. Le L, Nguyen TN. DQRA: deep quantum routing agent for entanglement routing in quantum networks. IEEE Trans Quantum Eng. 2022;3:1–12.
60. Meignant C, Markham D, Grosshans F. Distributing graph states over arbitrary quantum networks. Phys Rev A. 2019;100(5):052333.
61. Fischer A, Towsley D. Distributing graph states across quantum networks. In: 2021 IEEE int. conf. Quantum comput. Eng. (QCE), Broomfield, CO, USA; 2021.
62. Fung C-HF, Ma X, Chau HF. Practical issues in quantum-key-distribution postprocessing. Phys Rev A. 2010;81(1):012318.
63. Deng F-G, Li X-H, Zhou H-Y, Zhang Z-J. Improving the security of multiparty quantum secret sharing against Trojan horse attack. Phys Rev A. 2005;72(4):044302.
64. Cai Q-Y. Eavesdropping on the two-way quantum communication protocols with invisible photons. Phys Lett A. 2006;351(1–2):23–5.
65. Boyer M, Katz M, Liss R, Mor T. Experimentally feasible protocol for semiquantum key distribution. Phys Rev A. 2017;96(6):062335.
66. Coopmans T, Knegjens R, Dahlberg A, Maier D, Nijsten L, de Oliveira Filho J, Papendrecht M, Rabbie J, Rozpędek F, Skrzypczyk M, Wubben L, de Jong W, Podareanu D, Torres-Knoop A, Elkouss D, Wehner S. NetSquid, a NETwork simulator for quantum information using discrete events. Commun Phys. 2021;4(1):164.


## Publisher's Note