entropy

MDPI

Article

Multi-User Measurement-Device-Independent Quantum Key Distribution Based on GHZ Entangled State

Ximing Hua [1], **Min Hu** [1,2,*] and **Banghong Guo** [1,3,*]

[1] Guangdong Provincial Key Laboratory of Nanophotonic Functional Materials and Devices, Guangdong Provincial Key Laboratory of Quantum Engineering and Quantum Materials, South China Normal University, Guangzhou 510006, China; 2019022062@m.scnu.edu.cn
[2] National Quantum Communication (Guangdong) Co., Ltd., Guangzhou 510535, China
[3] Key Laboratory of Quantum Information, University of Science and Technology of China, Chinese Academy of Sciences, Hefei 230026, China
* Correspondence: hmin@scnu.edu.cn (M.H.); guobh@scnu.edu.cn (B.G.)

Abstract: As a multi-particle entangled state, the Greenberger–Horne–Zeilinger (GHZ) state plays an important role in quantum theory and applications. In this study, we propose a flexible multi-user measurement-device-independent quantum key distribution (MDI-QKD) scheme based on a GHZ entangled state. Our scheme can distribute quantum keys among multiple users while being resistant to detection attacks. Our simulation results show that the secure distance between each user and the measurement device can reach more than 280 km while reducing the complexity of the quantum network. Additionally, we propose a method to expand our scheme to a multi-node with multi-user network, which can further enhance the communication distance between the users at different nodes.

Keywords: quantum key distribution; GHZ entangled state; measurement-device-independent; multi-user

check for updates

Citation: Hua, X.; Hu, M.; Guo, B. Multi-User Measurement-Device-Independent Quantum Key Distribution Based on GHZ Entangled State. *Entropy* **2021**, *24*, 841. https://doi.org/10.3390/e24060841

Academic Editors: Shao-Ming Fei, Ming Li and Shunlong Luo

Received: 10 May 2022
Accepted: 16 June 2022
Published: 18 June 2022

1. Introduction

Quantum key distribution (QKD) allows two users, Alice and Bob, to share a secure key privately [1,2]. The first QKD protocol, called the BB84 protocol, was proposed in 1984 by Bennett and Brassard [3]. However, because of the gaps between reality and theory, there exist various loopholes in practical systems through which eavesdroppers can attack the QKD process [4]. Therefore, several investigators have focused on finding ways to resist such attacks [5,6]. In 2012, Lo et al. proposed a measurement-device-independent quantum key distribution (MDI-QKD) protocol [7] to prevent attacks on measurement devices and enhance the communication distance between two users.

QKD research usually begins with a point-to-point scheme. With the development of quantum networks [8–10], multi-user scenarios have become research hotspots. Multi-user QKD, known as quantum cryptography conference (QCC) such as Greenberger–Horne–Zeilinger (GHZ) states [11] based scheme [12] and measurement-device independent scheme [13] or quantum conference key agreement (CKA) such as the intensity-encoded scheme [14] and the scheme based on a W-class state [15], is effective in scenarios where multiple users share common secure keys. Multi-particle entangled states can easily apply in multi-user QKD realization [16], although the communication distance is limited by the stability of entangled states and other issues lead to such schemes being inferior compared to the existing single-photon interference schemes [17].

Ref. [18] proposed an MDI-QKD scheme with an entangled source in the middle and realized ultra-long communication. Inspired by the scheme, we propose a multi-user MDI-QKD scheme based on the GHZ entangled state. We analyze the security of our scheme and derive the secure key rate when users employ an ideal single photon source and a weak coherent source. The simulation results show that a multi-user MDI-QKD system can be realized under this scheme with a reduced number of detectors and quantum channels compared with traditional MDI-QKD, while the distance between each user and the measurement device can reach more than 280 km (more than 560 km between each two users). Additionally, we propose a method to expand our scheme to a multi-node with multi-user network, which can further enhance the communication distance between the users at different nodes. This paper is organized as follows: in Section 2, we introduce the multi-user MDI-QKD based on GHZ entangled state protocol. In Section 3, we estimate the performance of our scheme for an ideal single-photon source and a weak coherent source. In Section 4, we introduce a method to expand our scheme to a multi-node with multi-user network. Finally, a summary is presented in Section 5.

2. Protocol

Before providing details of our protocol, we simply introduce the background knowledge of our scheme. A GHZ entangled state is multi-particle entangled state in which each particle is entangled with other particles. It has maximum output mutual information, and resistance to white noise. The n-particle GHZ entangled state can be expressed as follows [19]:

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|000\ldots00\rangle + |111\ldots11\rangle)_N \tag{1}$$

Based on the distribution of an n-particle GHZ entangled state [16], n users can obtain the common secure key simultaneously. This leads to the generation of a secure key according to the measurement result of the GHZ entangled state.

In MDI-QKD [7], the measurement device utilizes the Hong–Ou–Mandel (HOM) [20] effect to construct the relationship between two input particles. According to the click of the detectors, we obtain the BSM result $|\psi^+\rangle = (|H\rangle|V\rangle + |V\rangle|H\rangle)/\sqrt{2}$ and $|\psi^-\rangle = (|H\rangle|V\rangle - |V\rangle|H\rangle)/\sqrt{2}$. In the Z basis, the successful BSM event ($|\psi^+\rangle$ and $|\psi^-\rangle$) represents the polarization of two particles being different, while the X basis $|\psi^+\rangle$ ($|\psi^-\rangle$) represents the two particles having the same (different) polarization.

Combining the distribution of the GHZ entangled state with the MDI-QKD, we can realize the multi-user QKD by entanglement swapping [21].

As depicted in Figure 1, there is a case of an n-user MDI-QKD system based on GHZ entangled states. The system can divide into four parts: user, measurement device, GHZ entangled state source (GHZ-ESS) and channel. The n-user system includes n users, n measurement devices, a GHZ-ESS, and channel. The user mainly contains a source, a polarization modulator, and a upper computer. In practice, we usually use a weak coherent source with a decoy-state instead of a single photon source. The user uses a polarization modulator to modulate BB84 polarization states. The upper computer control the source, the polarization modulator and the information processing. The information processing includes sifting the efficient data, post-processing, etc. Each user has a corresponding measurement device. The GHZ-ESS connects to all measurement devices. The number of particles in the GHZ entangled state is similar to the number of users. Each particle of the GHZ entangled state will interfere with the polarization state prepared by users in the corresponding measurement device. They will perform Bell state measurement (BSM) in the measurement device. The channel including quantum channel and classical channel. Quantum channels are used to transmit quantum signals. Classical information such as the basis of prepared polarization state is transmitted in classical channel.

As shown in Figure 2, our protocol consists of five main steps:

Step 1: Preparation. Each user randomly prepares one of the BB84 states such as $|+\rangle$,$|-\rangle$ in the X basis or $|H\rangle$,$|V\rangle$ in the Z basis, while the GHZ-ESS randomly prepares an n-particle GHZ entangled state. The number of particles in the GHZ entangled state is equal to the number of users (in principle, each user only sends one photon).

Step 2: Transmission. Users (the GHZ-ESS) transmit the BB84 state (the GHZ entangled state) in different quantum channels between each user (the GHZ-ESS) and measurement device.

Step 3: Measurement. The measurement device performs BSM on the BB84 state and the GHZ entangled-state particles. Each particle of the GHZ entangled quantum state can interfere with a particle sent by its corresponding user. If there are only two detectors responding we call it a successful BSM event (a click in D1H and D2V, or in D1V and D2H are $|\psi^{-}\rangle$; a click in D1H and D1V, or in D2H and D2V are $|\psi^{+}\rangle$), similar to traditional MDI-QKD.

Step 4: Sifting. All users retain the bits when all the corresponding measurement device generates a successful BSM event. All users announce the basis of the prepared BB84 state, and the GHZ entangled source broadcasts the GHZ state it has prepared through the classical channels. In our scheme, only the states in the Z basis are used to generate a secure key; the states in the X basis are used to estimate the error rate. Hence, users retain the data prepared in the same basis by all users and discard the remaining data. Then, each user should either flip or not flip its local bits according to the BSM result, the GHZ states, and the prepared basis; see following and Appendix A for details. At this point, each user obtains the raw key.

Step 5: Post-processing. Similar to traditional point-to-point QKD protocols, users perform post-processing under the control of upper computer, which includes error correction and privacy amplification. They finally obtain the same secure keys.

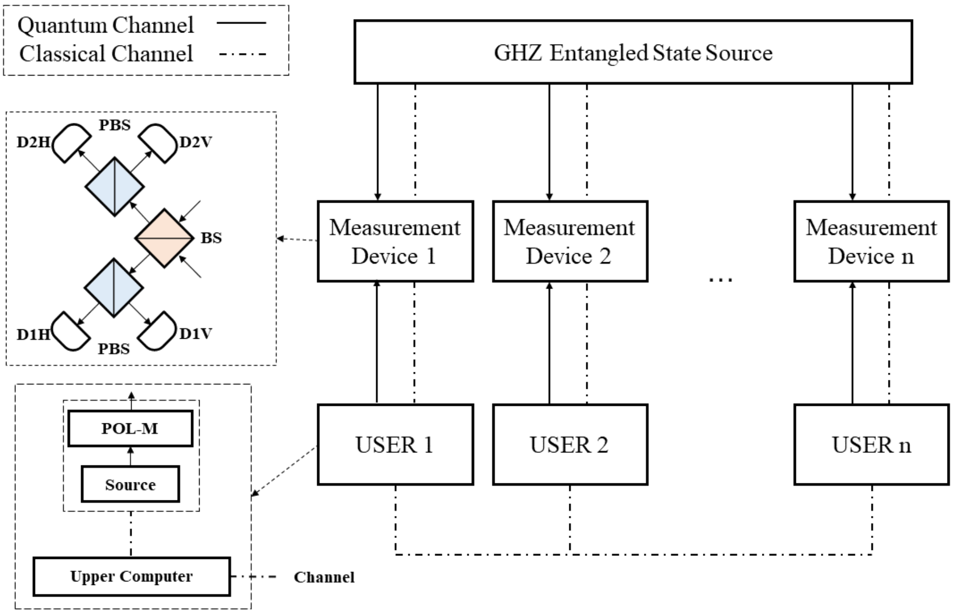

Figure 1. Schematic diagram of n-user MDI-QKD system. **POL-M**: polarization modulator; **BS**: beam splitter; **PBS**: polarization beam splitter; **D1H**, **D1V**, **D2H**, **D2V**: single-photon detector; **Source**: single-photon source or weak coherent source. We use solid line to depict the quantum channel and dotted line to depict the classical channel. The measurement device includes a BS, two PBSs, and four single-photon detectors, and implements the Bell state measurement (BSM) the same as the polarization-based MDI-QKD protocol. The GHZ-ESS can prepare GHZ entangled states with different numbers of particles corresponding to the number of users.

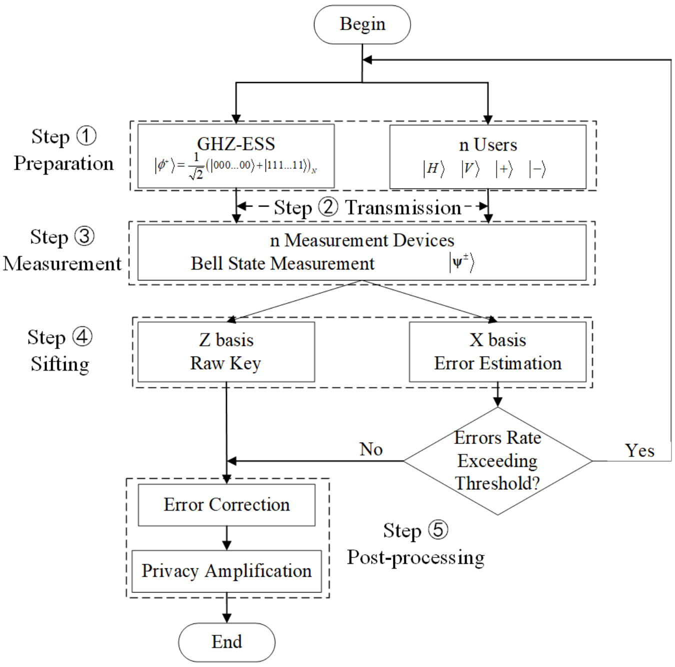

Figure 2. Flow chart of our protocol.

Following the original MDI-QKD protocol [7], users need to operate on their local bits based on the GHZ entangled state and the BSM results to generate secure keys. Taking three users (named Alice, Bob, and Charles) as an example, Table 1 shows the relationship between the prepared GHZ state, the BSM results, and the operations of the three participants. The users can retain the signal to generate a secure key only when all the BSM results are $|\psi^{+}\rangle$ or $|\psi^{-}\rangle$.

Table 1. Participants and their operations in the Z basis.

GHZ State	BSM 1	BSM 2	BSM 3	Alice	Bob	Charles
$\frac{1}{\sqrt{2}}(\|H\rangle\|H\rangle\|H\rangle \pm \|V\rangle\|V\rangle\|V\rangle)$	$\|\psi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	No Flip	No Flip	No Flip
$\frac{1}{\sqrt{2}}(\|H\rangle\|V\rangle\|H\rangle \pm \|V\rangle\|H\rangle\|V\rangle)$	$\|\psi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	No Flip	Flip	No Flip
$\frac{1}{\sqrt{2}}(\|H\rangle\|H\rangle\|V\rangle \pm \|V\rangle\|V\rangle\|H\rangle)$	$\|\psi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	No Flip	No Flip	Flip
$\frac{1}{\sqrt{2}}(\|H\rangle\|V\rangle\|V\rangle \pm \|V\rangle\|H\rangle\|H\rangle)$	$\|\psi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	$\|\psi^{\pm}\rangle$	No Flip	Flip	Flip

For example, when the state prepared by the GHZ-ESS is $\frac{1}{\sqrt{2}}(|H\rangle|H\rangle|H\rangle \pm |V\rangle|V\rangle|V\rangle)$, the message can be retained as a sifted key only if Alice, Bob, and Charles have prepared the same polarization state and all the BSM results are $|\psi^{+}\rangle$ or $|\psi^{-}\rangle$.

3. Secure Key Rate

Next, we derive the secure key and error rates to investigate the performance of our scheme with a single-photon source and a weak coherent source.

By combining the MDI-QKD technique [7] and the GLLP method [22], the security key rate is given by

$$R = Q_1^Z[1 - H\left(e_1^X\right)] - Q^Z f H\left(E^{Z*}\right) \tag{2}$$

where Q^Z and E^{Z*} denote the gain and quantum bit error rate (QBER) in the Z basis, respectively; f is the inefficiency function for the error correction process; Q_1^Z denotes the gain when all users send a single-photon state; e_1^X denotes the phase error rate; and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. $E^{Z*} = \max\{E^Z_{U_1U_2}, E^Z_{U_1U_3} \dots E^Z_{U_1U_n}\}$, where $E^Z_{U_1U_2}\left(E^Z_{U_1U_3} \dots E^Z_{U_1U_n}\right)$ is the marginal quantum bit error rate between user 1 and user 2 (3…n) in the Z basis. In practice, Q^Z and E^{Z*} can be obtained from experimental data.

3.1. Key Rate of Single-Photon Source

For simplicity, we consider the case of three users in our scheme and estimate the secure key rate for a single photon source.

When the users use an ideal single-photon source to prepare the BB84 state, the gain in the Z basis is

$$Q^Z = Q_1^Z = Y_1 \tag{3}$$

where Y_1 denotes the probability of obtaining a successful BSM when all the users send a single-photon state. The yield Y_1 is given by

$$\begin{aligned} Y_1 = \frac{1}{64}\{&(1-P_d)^2[1-(1-P_d)(1-\eta)][1-(1-P_d)(1-\eta_d)] \\ &+2P_d(1-P_d)^2[1-(1-P_d)(1-\eta)(1-\eta_d)]\}^3 \end{aligned} \tag{4}$$

where P_d is the dark count, η_d is the detection efficiency, $\eta = \eta_l \times \eta_b = 10^{-\alpha L/10} \times \eta_b$ is the transmittance between the users and measurement device, and η_l represents the channel loss. $\frac{1}{64}$ represents the possibility that users send similar or different polarization states to the particles of the GHZ entangled state in the Z basis.

We assume that our entangled source is perfect; therefore, the error rate contains two main contributions: (1) the error rate e_0 caused by background counts and (2) the error rate e_d corresponding to the misalignment and instability of the optical system. The total error rate is as follows:

$$E^{Z*} = E^Z_{U_1U_2} = E^Z_{U_1U_3} = e_0 - \frac{(e_0-e_d)(\frac{1}{16}\eta^2\eta_d^2(1-P_d)^4)}{Y_{U_1U_2}} \tag{5}$$

where $Y_{U_1U_2}$ denotes the probability of both measurement devices obtaining a successful BSM when user 1 and user 2 send a single-photon state. Similarly, we obtain the error rate in the X basis as follows:

$$e_1^X = e_0 - \frac{(e_0-e_d)(\frac{1}{64}\eta^3\eta_d^3(1-P_d)^6)}{Y_1} \tag{6}$$

Utilizing the experimental parameters in Table 2 [23], we obtained the simulation results shown in Figure 3. These results show that the communication distance between each user and the GHZ-ESS can exceed 280 km using optical fibers. Using an ideal single-photon source and a perfect GHZ-ESS, the GHZ-ESS can be located at the center to establish a star-configuration quantum network with a radius of 280 km.

Table 2. Experimental parameters used in the simulation. e_d is the system intrinsic bit error rate, P_d is the dark count, f is the error correction inefficiency, and α is the optical fiber transmission loss.

e_d	P_d	f	α
2%	8×10^{-8}	1.16	0.2

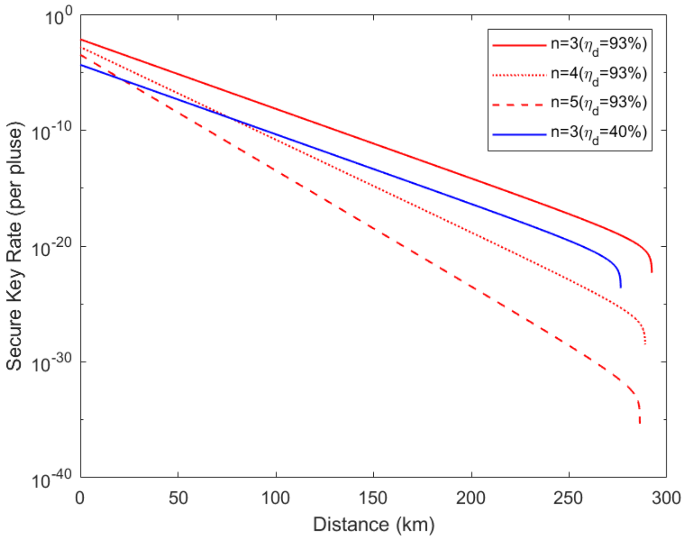

Figure 3. Secure key rate with single-photon state. The red line corresponds to the detection efficiency η_d of 93% [24], and the blue line corresponds to the detection efficiency η_d of 40% [23]. **n** is the number of communication users. The distance refers to the length of the quantum channel between any user and the measurement device.

3.2. Key Rate of Weak Coherent Source with Decoy State

In this section, we analyze the realization of the decoy state using our protocol. Users use the decoy state to resist a photon number splitting (PNS) attack on a weak coherent source. In our protocol, we use the Z basis to generate the secure key and the X basis to detect the error bit. Therefore, we take the quantum state in the Z basis as the signal state (only preparing the signal state) and that in the X basis as the decoy state (preparing both signal state and decoy state).

In our analysis, two decoy-state techniques (signal state v, vacuum state μ_2, decoy-state μ_1) are used, where $v > \mu_1 > \mu_2 = 0$ represents the mean photons of the sources.

We consider the situation consisting of three users as an example to derive the secure key rate. According to the decoy state method [25], in the Z basis, for each measurement device, we can estimate the gain Q_m^Z and error rate E_m^Z as follows:

$$Q_m^Z = \sum_{i=0}^{\infty} e^{-v} Y_{1i} \frac{v^i}{i!} \tag{7}$$

$$E_m^Z Q_m^Z = \sum_{i=0}^{\infty} e^{-v} e_{1i} Y_{1i} \frac{v^i}{i!} \tag{8}$$

where Y_{1i} (e_{1i}) represents the yield (error rate) from the GHZ-ESS and the corresponding user. The subscript 1 that different from the traditional MDI-QKD [7] represents the particle of GHZ entangled state in each measurement device. Therefore, we can estimate the total gain and error rate in the Z basis as follows:

$$Q^Z = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} e^{-3v} Y_{111ijk} \frac{v^{i+j+k}}{i!j!k!} \tag{9}$$

$$E^Z Q^Z = \sum_{i=0}^{\infty} \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} e^{-3v} e_{111ijk} Y_{111ijk} \frac{v^{i+j+k}}{i!j!k!} \tag{10}$$

where Y_{111ijk} (e_{111ijk}) represents the overall yield (error rate) in the Z basis. We optimized the formula in the Ref. [26] and added the subscript 111 to describe the influence of GHZ entangled state. We Similarly, we can obtain the total gain and error rate in the X basis.

Because we use the decoy state technique in the X basis, we can obtain the total gain in the Z basis when all users send a single photon pulse as

$$Q_1^Z = v^3 e^{-3v} Y_1^Z \tag{11}$$

where Y_1^Z represents the yield when all users send a single photon pulse.

Next, we need to estimate the lower bound of the yield and the upper bound of the error rate that each user sends for a single-photon pulse in the X basis. According to the decoy-state method [25–27], we can estimate that

$$\begin{aligned} Y_1^X \geq & \frac{1}{v^3 {\mu_1}^3 (v-\mu_1)} [v^4 (e^{3\mu_1} Q^X_{111\mu_1\mu_1\mu_1} - e^{2\mu_1} Q^X_{111\mu_1\mu_1 0} - e^{2\mu_1} Q^X_{111\mu_1 0\mu_1} - e^{2\mu_1} Q^X_{1110\mu_1\mu_1} \\ & + e^{\mu_1} Q^X_{111\mu_1 00} + e^{\mu_1} Q^X_{1110\mu_1 0} + e^{\mu_1} Q^X_{11100\mu_1} - Q^X_{111000}) \\ & - {\mu_1}^4 (e^{3v} Q^X_{111vvv} - e^{2v} Q^X_{111vv0} - e^{2v} Q^X_{111v0v} - e^{2v} Q^X_{1110vv} \\ & + e^{v} Q^X_{111v00} + e^{v} Q^X_{1110v0} + e^{v} Q^X_{11100v} - Q^X_{111000}) \end{aligned} \tag{12}$$

$$\begin{aligned} e_1^X \leq & \frac{1}{{\mu_1}^3 Y_1^X} (e^{3\mu_1} E^X_{111\mu_1\mu_1\mu_1} Q^X_{111\mu_1\mu_1\mu_1} - e^{2\mu_1} E^X_{111\mu_1\mu_1 0} Q^X_{111\mu_1\mu_1 0} - e^{2\mu_1} E^X_{111\mu_1 0\mu_1} Q^X_{111\mu_1 0\mu_1} \\ & - e^{2\mu_1} E^X_{1110\mu_1\mu_1} Q^X_{1110\mu_1\mu_1} + e^{\mu_1} E^X_{111\mu_1 00} Q^X_{111\mu_1 00} + e^{\mu_1} E^X_{1110\mu_1 0} Q^X_{1110\mu_1 0} \\ & + e^{\mu_1} E^X_{11100\mu_1} Q^X_{11100\mu_1} - E^X_{111000} Q^X_{111000}) \end{aligned} \tag{13}$$

where Q^X_{111ijk} (i,j,k = 0, μ_1, v represent the mean photon number intensities of users' sources) is the overall gain in the X basis when users choose the corresponding intensities. E^X_{111ijk} is the overall error rate in the X basis when users choose corresponding intensities.

Finally, utilizing the experimental parameters in Table 2, we can obtain the performance of our protocol when three users use weak coherent sources as shown in Figure 4. The simulation results show that the communication distance between each user and the GHZ-ESS can reach further than 210 km using optical fibers. Compared with a single photon source, the weak coherent source has a lower secure key rate and shorter communication distance while still realizing a signal transmission of more than 420 km between each two users.

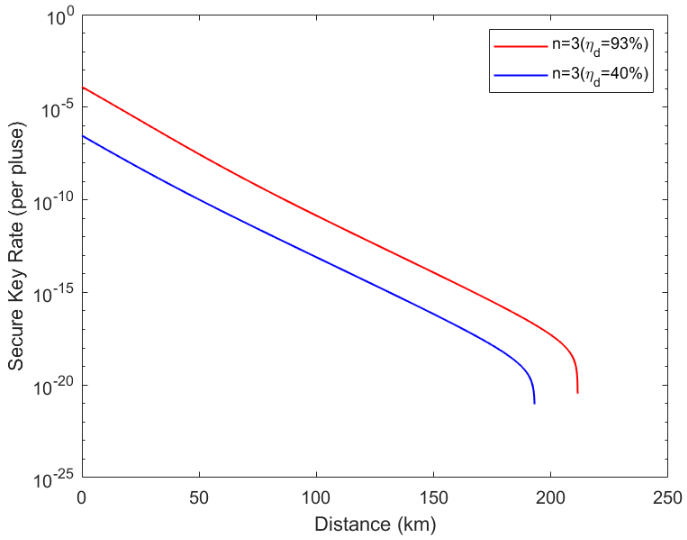

Figure 4. Secure key rate with weak coherent source. The simulation performed for the situation of three users had detection efficiency results of $\eta_d = 93\%$ and $\eta_d = 40\%$. The mean photons of signal state $v = 0.48$, and the mean photons of decoy-state $\mu_1 = 0.05$. The distance refers to the length of the quantum channel between any user and measurement device.

3.3. Security and Discussion

In this section, we will analyze the security of our protocol and compare our protocol with other schemes.

Without loss of generality, we can depict the three-particle GHZ entangled state in eight orthogonal GHZ states as [26]:

$$
\begin{aligned}
|\alpha_1\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle|H\rangle + |V\rangle|V\rangle|V\rangle) = \frac{1}{2}(|+++\rangle + |+--\rangle + |-+-\rangle + |--+\rangle) \\
|\alpha_2\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle|H\rangle - |V\rangle|V\rangle|V\rangle) = \frac{1}{2}(|++-\rangle + |+-+\rangle + |-++\rangle + |---\rangle) \\
|\alpha_3\rangle &= \frac{1}{\sqrt{2}}(|V\rangle|H\rangle|H\rangle + |H\rangle|V\rangle|V\rangle) = \frac{1}{2}(|+++\rangle + |+--\rangle - |-+-\rangle - |--+\rangle) \\
|\alpha_4\rangle &= \frac{1}{\sqrt{2}}(|V\rangle|H\rangle|H\rangle - |H\rangle|V\rangle|V\rangle) = \frac{1}{2}(|++-\rangle + |+-+\rangle - |-++\rangle - |---\rangle) \\
|\alpha_5\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|V\rangle|H\rangle + |V\rangle|H\rangle|V\rangle) = \frac{1}{2}(|+++\rangle - |+--\rangle + |-+-\rangle - |--+\rangle) \\
|\alpha_6\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|V\rangle|H\rangle - |V\rangle|H\rangle|V\rangle) = \frac{1}{2}(|++-\rangle - |+-+\rangle + |-++\rangle - |---\rangle) \\
|\alpha_7\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle|V\rangle + |V\rangle|V\rangle|H\rangle) = \frac{1}{2}(|+++\rangle - |+--\rangle - |-+-\rangle + |--+\rangle) \\
|\alpha_8\rangle &= \frac{1}{\sqrt{2}}(|H\rangle|H\rangle|V\rangle - |V\rangle|V\rangle|H\rangle) = \frac{1}{2}(|++-\rangle - |+-+\rangle - |-++\rangle + |---\rangle)
\end{aligned}
\tag{14}
$$

Taking $|\alpha_1\rangle$ as an example, it will randomly collapse into $|\gamma_1\rangle = |H\rangle|H\rangle|H\rangle$ or $|\gamma_2\rangle = |V\rangle|V\rangle|V\rangle$ in the Z basis. In the X basis, any user obtains $|+\rangle$ ($|-\rangle$) when the other obtains the same (different) polarization. We use the character that provides the security of the GHZ entangled sources to generate a secure key in the Z basis and error detection in the X basis.

Based on the principle of MDI-QKD [7], our scheme can resist attacks on the measurement devices. In addition to resisting attacks on the measurement device, our scheme can resist a PNS attack using the decoy state technique [22,25,28,29]. Users can employ weak coherent sources with a decoy-state. The GHZ entangled state is equivalent to an ideal single-photon state in each quantum channel. A PNS attack is ineffective for an ideal single-photon source. Therefore, our scheme can resist PNS attacks.

Compared with traditional MDI-QKD, ref. [30] reported the longest communication record that reached 404 km in experiments, while the simulation result shows that our protocol can be utilized with greater than 560 km between each two users. Four detectors are required to build a traditional MDI-QKD system between two users. Therefore, 2n (n − 1) detectors are required to establish a quantum communication system using the MDI-QKD protocol between n users. However, in our protocol, the number of detectors required to establish communications between n users is reduced to only 4n. Moreover, only 2n channels rather than n (n − 1)/2 channels are required if a traditional point-to-point protocol [7] is used between the users and the measurement device. Thus, the cost and complexity of the network are reduced.

We compare our scheme with other multi-user schemes in Table 3. When we employ a single photon source with $\eta_d = 93\%$, the available distance can reach more than 560 km between each two users. When we employ a weak coherent source with $\eta_d = 93\%$, the available distance can reach more than 420 km between each two users.

Unlike the MDI-QCC based on a post-selection GHZ entangled state [26] and PM-QCC based on a post-selection GHZ entangled state [19], our protocol uses a GHZ entangled state and the polarization state prepared by users to execute BSM and realize multi-user sharing of a common secret key.

Table 3. Comparison of multi-user schemes.

Items	**GHZ State MDI-QCC** [26]	**W State Multi-User MDI-QKD** [31]	**GHZ State Multi-User MDI-QKD** [23]	**Our Scheme**
Entangled State	GHZ state	W state	GHZ state	GHZ state
Users	≥3	≥4	≥3	≥3
Secure Key Rate	10^{-16} ($\eta_d = 93\%$, 400 km between two users, weak coherent)	10^{-16} ($\eta_d = 93\%$, 260 km between two users, single photon)	10^{-21} ($\eta_d = 40\%$, 400 km between two users, single photon)	10^{-15} ($\eta_d = 93\%$, 400 km between two users, single photon)
Available Distance	420 km between two users (weak coherent)	260 km between two users (single photon)	520 km between two users (single photon)	560 km between two users (single photon) 420 km between two users (weak coherent)

CKA schemes [32] based on the principle of twin-field QKD [33] can realize a high secure key rate and long communication distance through the single photon interference. In our scheme, with a more flexible number of users, we can increase the distance between the GHZ-ESS and the measurement device to enhance the communication distance between each two users. In addition, we can expand our scheme further into a multi-node quantum network, as detailed in Section 4.

Because of the coincidence measurement at the measurement device, increasing the number of users will lead to an obvious decrease in the secure key rate. We propose a system that uses an adaptive technique in Appendix B, while we need to investigate the specific performance in our scheme. At the same time, we will consider using asynchronous time multiplexing technology [34,35], which idea is based on adaptive techniques, to further improve our scheme through enhancing the secure key rate under multi-user scenarios.

4. Expansion of Our Protocol

Based on the location-changeable GHZ-ESS, we can expand our scheme further into a multi-node quantum network without quantum memory. An example of two nodes with two users per node is shown in Figure 5, and we can extend the system to n nodes with n users per node.

In the system, we use measurement devices that perform BSM to construct the entangled relationship between two adjacent GHZ entangled sources and extend the communication distance between users in different nodes by increasing the distance between the GHZ-ESS and the measurement device. We use the example shown in Figure 5 to detail the process. In theory, the longest secure communication between user 3 and user 1 can be estimated as follows:

$$L_{U_1U_3} = L_{U_1M_1} + L_{GHZ_1M_1} + L_{GHZ_1M_{GHZ}} + L_{GHZ_2M_{GHZ}} + L_{GHZ_2M_3} + L_{U_3M_3} \tag{15}$$

where $L_{U_1M_1}$ ($L_{U_3M_3}$) is the distance between the user and the corresponding measurement device, $L_{GHZ_1M_1}$ ($L_{GHZ_2M_3}$) is the distance between the GHZ-ESS and the corresponding measurement device, and $L_{GHZ_1M_{GHZ}}$ ($L_{GHZ_1M_{GHZ}}$) is the distance between the GHZ-ESS and the measurement device that is between the adjacent GHZ-ESSs.

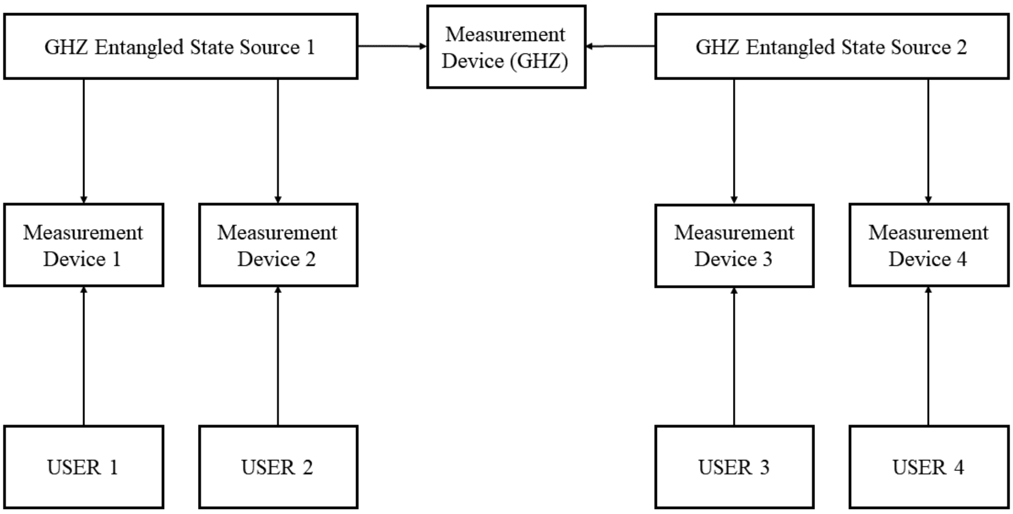

Figure 5. An example of two users per node. The system can help user 1, user 2, user 3, and user 4 to share a common secure key. Unlike our system shown in Figure 1, we build the relationship between two GHZ-ESSs with measurement devices that use BSM like ordinary MDI-QKD devices.

When we assume that two GHZ-ESSs prepare the same GHZ entangled state and all measurement devices obtain successful BSM events ($|\psi^+\rangle$ or $|\psi^-\rangle$), the operations of users in the Z basis are as shown in Table 4.

Table 4. The operations of users in different GHZ states in the Z basis. The operation of bit flip according to user 1 and all measurement devices obtain successful BSM events ($|\psi^+\rangle$ or $|\psi^-\rangle$). We assume that the first particle of the first GHZ is entangled, corresponding to measurement device 1, and the first particle of the second GHZ entangled state corresponds to measurement device 3.

GHZ state	USER 1	USER 2	USER 3	USER 4
$\frac{1}{\sqrt{2}}(\|H\rangle\|H\rangle\|H\rangle \pm \|V\rangle\|V\rangle\|V\rangle)$	No Flip	No Flip	Flip	Flip
$\frac{1}{\sqrt{2}}(\|H\rangle\|V\rangle\|H\rangle \pm \|V\rangle\|H\rangle\|V\rangle)$	No Flip	Flip	Flip	No Flip
$\frac{1}{\sqrt{2}}(\|H\rangle\|H\rangle\|V\rangle \pm \|V\rangle\|V\rangle\|H\rangle)$	No Flip	No Flip	Flip	Flip
$\frac{1}{\sqrt{2}}(\|H\rangle\|V\rangle\|V\rangle \pm \|V\rangle\|H\rangle\|H\rangle)$	No Flip	Flip	Flip	No Flip

5. Conclusions

In this study, we presented a multi-user MDI-QKD scheme based on the GHZ entangled state. We analyzed the security of our scheme and derived the secure key rate when users use an ideal single photon source and a weak coherent source. The MDI-QKD-based scheme is also immune to attacks on the measurement devices, and the communication distance is increased. Furthermore, in contrast to the multi-user quantum network implemented by the original MDI-QKD protocol, the number of detectors required in our scheme is reduced from 2n (n −1) to 4n, and the number of quantum channels is reduced from n (n − 1)/2 to 2n. Our scheme realizes an ultra-long QKD available communication distance that can reach more than 280 km between each user and measurement device (i.e., the longest communication distance between any two users can reach more than 560 km) and further extend by changing the location of the GHZ-ESS. In addition, we can expand our scheme further to a multi-node quantum network without quantum memory, which enhances the communication distance between two users.

Although our scheme can be flexibly applied to QKD networks, there are still two issues remaining to be studied in the future. On one hand, the location of the GHZ entangled source can be changed in our scheme, and we can extend the communication distance between two users by increasing the distance between the GHZ entangled source and the measurement device. Therefore, we will study the influence of GHZ entangled state long-distance division. On the other hand, in our estimation of the secure key rate, we assume that the distance between each user and the corresponding measurement device is similar. Therefore, it will be interesting to consider an asymmetric situation.

Author Contributions: Conceptualization, X.H. and M.H.; methodology, X.H. and M.H.; software, X.H.; validation, X.H. and M.H.; formal analysis, X.H.; investigation, X.H. and M.H.; writing—original draft preparation, X.H.; writing—review and editing, X.H. and M.H.; visualization, X.H.; supervision, M.H. and B.G.; funding acquisition, B.G. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Key-Area Research and Development Program of Guangdong Province (Grant No. 2018B030325002).

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: We thank Ming-Hao Zhu, Cong Chen, and Fan Yang for their helpful discussions.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A. Protocol Analysis

In this section, we analyze the generation of the secure key. The key generation in the Z basis in our protocol can be equivalent to the construction shown in Figure A1. The GHZ entangled source distributes a particle of the n-particle GHZ entangled states to each user. Users measure the polarization of the particle and obtain the secure key.

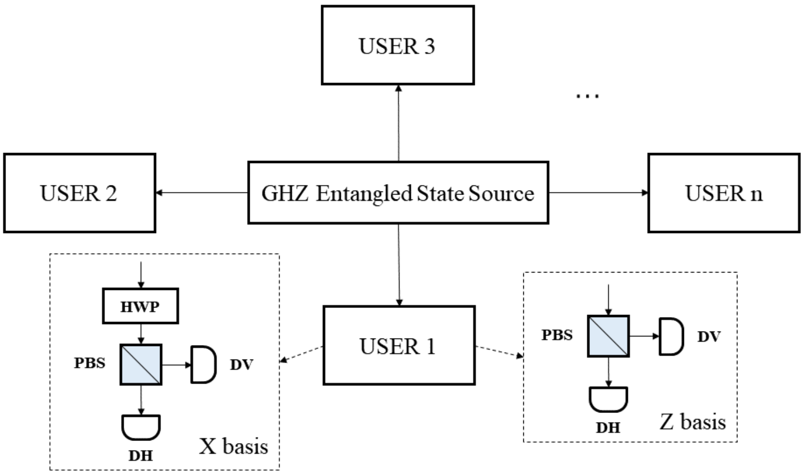

Figure A1. The equivalent topological schematic diagram of the GHZ entangled source distributing a particle of the n-particle GHZ entangled states to each user. **HWP**: half wave plate; **PBS**: polarization beam splitter; **DH**, **DV**: single photon detector.

We also considered the case of three users. As shown in Table A1, the GHZ-ESS prepares different GHZ states and sends them to users. Users measure the polarization in the Z basis. They obtain value "0" when the measurement result is $|H\rangle$, and value "1" corresponds to $|V\rangle$.

Table A1. Measurement result and value of the secure key. **GHZ entangled state** is the GHZ state sent by the entangled source. **MR1**, **MR2**, and **MR3** are the measurement results of user 1, user 2, and user 3. and **Value1**, **Value2**, and **Value3** are the values of the users' secure keys.

GHZ Entangled State	MR1	Value1	MR2	Value2	MR3	Value3
$\frac{1}{\sqrt{2}}(\vert H\rangle\vert H\rangle\vert H\rangle \pm \vert V\rangle\vert V\rangle\vert V\rangle)$	$\vert H\rangle$ $\vert V\rangle$	0 1	$\vert H\rangle$ $\vert V\rangle$	0 1	$\vert H\rangle$ $\vert V\rangle$	0 1
$\frac{1}{\sqrt{2}}(\vert V\rangle\vert H\rangle\vert H\rangle \pm \vert H\rangle\vert V\rangle\vert V\rangle)$	$\vert V\rangle$ $\vert H\rangle$	1 0	$\vert H\rangle$ $\vert V\rangle$	0 1	$\vert H\rangle$ $\vert V\rangle$	0 1
$\frac{1}{\sqrt{2}}(\vert H\rangle\vert V\rangle\vert H\rangle \pm \vert V\rangle\vert H\rangle\vert V\rangle)$	$\vert H\rangle$ $\vert V\rangle$	0 1	$\vert V\rangle$ $\vert H\rangle$	1 0	$\vert H\rangle$ $\vert V\rangle$	0 1
$\frac{1}{\sqrt{2}}(\vert H\rangle\vert H\rangle\vert V\rangle \pm \vert V\rangle\vert V\rangle\vert H\rangle)$	$\vert H\rangle$ $\vert V\rangle$	0 1	$\vert H\rangle$ $\vert V\rangle$	0 1	$\vert V\rangle$ $\vert H\rangle$	1 0

Compared with the equivalent topological scheme, our protocol can resist attacks on measurement devices and enhance the communication distance between two users. Moreover, if we locate the GHZ entangled source near the measurement device, can we greatly reduce the effect of decoherence of GHZ entangled states. However, we can also increase the distance between the GHZ-ESS and measurement device to increase the communication distance between the two users. Therefore, our protocol can realize multi-user QKD over an ultra-long distance.

Appendix B. Increasing the Secure Key Rate with an Adaptive Technique

According to the idea in [36], we propose our multi-user MDI-QKD system with an adaptive technique as shown in Figure A2.

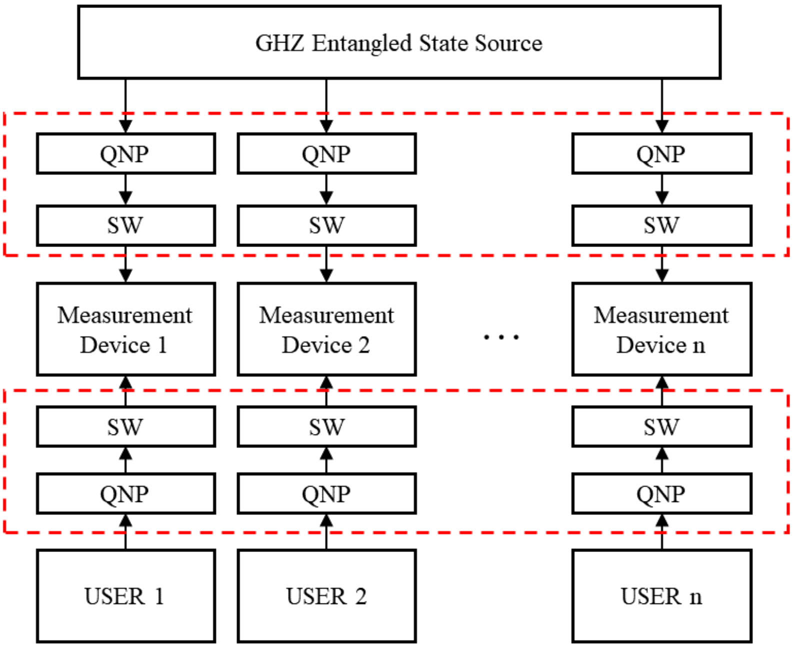

Figure A2. Multi-user MDI-QKD system with adaptive method. **QNP**: quantum non-demolition measurement; **SW**: optical switches. The adaptive technology structures are shown inside the red dashed frames.

The implementation process is as follows. Firstly, all users and GHZ-ESSs send many signal states to the corresponding measurement device; secondly, the QNP performs the quantum non-demolition measurement to detect the arrival of the signal; thirdly, the SW is used to match the arrival signal from the GHZ-ESS and users; fourthly, the measurement device performs BSM between the matched signals and broadcasts the matched result as well as measurement result; lastly, the user keeps the signal data that relate to successful BSM events and other post-processing.

Through the use of an adaptive technique, we can enhance the secure key rate in our multi-user QKD scheme. However, the lack of any particles in the GHZ entangled state will lead to the entire entangled state being unusable, and the GHZ-ESS will need to prepare more signal states than users in principle. We will study the specific performance of using an adaptive technique in future research.

References

1. Xu, F.; Ma, X.; Zhang, Q.; Lo, H.K.; Pan, J.W. Secure quantum key distribution with realistic devices. *Rev. Mod. Phys.* **2020**, *92*, 025002. [CrossRef]
2. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
3. Bennett, C.H.; Brassard, G. Quantum Cryptography: Public Key distribution and Coin Tossing. In Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, 10–12 December 1984 ; Institute of Electrical and Electronics Engineers: Bangalore, India, 1984; pp. 174–179.
4. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441–444. [CrossRef] [PubMed]
5. Hwang, W.Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef] [PubMed]
6. Acín, A.; Brunner, N.; Gisin, N.; Massar, S.; Pironio, S.; Scarani, V. Device-independent security of quantum cryptography against collective attacks. *Phys. Rev. Lett.* **2007**, *98*, 230501. [CrossRef]
7. Lo, H.K.; Curty, M.; Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
8. Wang, S.; Chen, W.; Yin, Z.Q.; Li, H.W.; He, D.Y.; Li, Y.H.; Zhou, Z.; Song, X.T.; Li, F.Y.; Wang, D.; et al. Field and long-term demonstration of a wide area quantum key distribution network. *Opt. Express* **2014**, *22*, 21739. [CrossRef]
9. Cheng, G.; Guo, B.; Zhang, C.; Guo, J.; Fan, R. Wavelength division multiplexing quantum key distribution network using a modified plug-and-play system. *Opt. Quantum Electron.* **2015**, *47*, 1809–1817. [CrossRef]
10. Chen, Y.A.; Zhang, Q.; Chen, T.Y.; Cai, W.Q.; Liao, S.K.; Zhang, J.; Chen, K.; Yin, J.; Ren, J.G.; Chen, Z.; et al. An integrated space-to-ground quantum communication network over 4,600 kilometres. *Nature* **2021**, *589*, 214–219. [CrossRef]
11. Greenberger, D.M.; Horne, M.A.; Zeilinger, A. Going Beyond Bell's Theorem. In *Bell's Theorem, Quantum Theory and Conceptions of the Universe*; Kafatos, M., Ed.; Springer: Dordrecht, The Netherlands, 1989; pp. 69–72._10. [CrossRef]
12. Multi-partite quantum cryptographic protocols with noisy ghz states. *Quantum Inf. Comput.* **2007**, *7*, 689–715. [CrossRef]
13. Zhang, L.; Hu, M.; Ran, P.; Zeng, H.; Li, J.; Guo, B. Fuzzy Greenberger–Horne–Zeilinger state analyzer and multiparty measurement-device-independent quantum key distribution network. *Opt. Eng.* **2019**, *58*, 016113. [CrossRef]
14. Cao, X.Y.; Gu, J.; Lu, Y.S.; Yin, H.L.; Chen, Z.B. Coherent one-way quantum conference key agreement based on twin field. *New J. Phys.* **2021**, *23*, 043002. [CrossRef]
15. Grasselli, F.; Kampermann, H.; Bruß, D. Conference key agreement with single-photon interference. *New J. Phys.* **2019**, *21*, 123002. [CrossRef]
16. Epping, M.; Kampermann, H.; Macchiavello, C.; Bruß, D. Multi-partite entanglement can speed up quantum key distribution in networks. *New J. Phys.* **2017**, *19*, 093012. [CrossRef]
17. Cao, X.Y.; Lu, Y.S.; Li, Z.; Gu, J.; Yin, H.L.; Chen, Z.B. High Key Rate Quantum Conference Key Agreement with Unconditional Security. *IEEE Access* **2021**, *9*, 128870–128876. [CrossRef]
18. Xu, F.; Qi, B.; Liao, Z.; Lo, H.K. Long distance measurement-device-independent quantum key distribution with entangled photon sources. *Appl. Phys. Lett.* **2013**, *103*, 061101. [CrossRef]
19. Zhao, S.; Zeng, P.; Cao, W.F.; Xu, X.Y.; Zhen, Y.Z.; Ma, X.; Li, L.; Liu, N.L.; Chen, K. Phase-Matching Quantum Cryptographic Conferencing. *Phys. Rev. Appl.* **2020**, *14*, 024010. [CrossRef]
20. Hong, C.K.; Ou, Z.Y.; Mandel, L. Measurement of subpicosecond time intervals between two photons by interference. *Phys. Rev. Lett.* **1987**, *59*, 2044–2046. [CrossRef]
21. Bose, S.; Vedral, V.; Knight, P.L. Multiparticle generalization of entanglement swapping. *Phys. Rev. A At. Mol. Opt. Phys.* **1998**, *57*, 822–829. [CrossRef]
22. Gottesman, D.; Hoi-Kwonglo, L.O.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **2004**, *4*, 325–360. [CrossRef]
23. Cao, W.F.; Zhen, Y.Z.; Zheng, Y.L.; Zhao, S.; Xu, F.; Li, L.; Chen, Z.B.; Liu, N.L.; Chen, K. Open-destination measurement-device-independent quantum key distribution network. *Entropy* **2020**, *22*, 1083. [CrossRef] [PubMed]
24. Marsili, F.; Verma, V.B.; Stern, J.A.; Harrington, S.; Lita, A.E.; Gerrits, T.; Vayshenker, I.; Baek, B.; Shaw, M.D.; Mirin, R.P.; et al. Detecting single infrared photons with 93% system efficiency. *Nat. Photonics* **2013**, *7*, 210–214. [CrossRef]

25. Ma, X.; Qi, B.; Zhao, Y.; Lo, H.K. Practical decoy state for quantum key distribution. *Phys. Rev. A* **2005**, *72*, 012326. [CrossRef]
26. Fu, Y.; Yin, H.L.; Chen, T.Y.; Chen, Z.B. Long-distance measurement-device-independent multiparty quantum communication. *Phys. Rev. Lett.* **2015**, *114*, 090501. [CrossRef]
27. Xu, F.; Curty, M.; Qi, B.; Lo, H.K. Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **2013**, *15*, 113007. [CrossRef]
28. Lütkenhaus, N.; Jahma, M. Quantum key distribution with realistic states: Photon-number statistics in the photon-number splitting attack. *New J. Phys.* **2002**, *4*, 44. [CrossRef]
29. Ma, X.; Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Phys. Rev. A* **2012**, *86*, 062319. [CrossRef]
30. Yin, H.L.; Chen, T.Y.; Yu, Z.W.; Liu, H.; You, L.X.; Zhou, Y.H.; Chen, S.J.; Mao, Y.; Huang, M.Q.; Zhang, W.J.; et al. Measurement-Device-Independent Quantum Key Distribution over a 404 km Optical Fiber. *Phys. Rev. Lett.* **2016**, *117*, 190501. [CrossRef]
31. Zhu, C.; Xu, F.; Pei, C. W-state Analyzer and Multi-party Measurement-device-independent Quantum Key Distribution. *Sci. Rep.* **2015**, *5*, 17449. [CrossRef]
32. Li, Z.; Cao, X.Y.; Li, C.L.; Weng, C.X.; Gu, J.; Yin, H.L.; Chen, Z.B. Finite-key analysis for quantum conference key agreement with asymmetric channels. *Quantum Sci. Technol.* **2021**, *6*, 045019. [CrossRef]
33. Lucamarini, M.; Yuan, Z.L.; Dynes, J.F.; Shields, A.J. Overcoming the rate-distance limit of quantum key distribution without quantum repeaters. *Nature* **2018**, *557*, 400–403. [CrossRef] [PubMed]
34. Xie, Y.M.; Lu, Y.S.; Weng, C.X.; Cao, X.Y.; Jia, Z.Y.; Bao, Y.; Wang, Y.; Fu, Y.; Yin, H.L.; Chen, Z.B. Breaking the Rate-Loss Bound of Quantum Key Distribution with Asynchronous Two-Photon Interference. *Phys. Rev. Appl.* **2021**, *10*, 020315. [CrossRef]
35. Zeng, P.; Zhou, H.; Wu, W.; Ma, X. Quantum key distribution surpassing the repeaterless rate-transmittance bound without global phase locking. *arXiv* **2022**, arXiv:2201.04300.
36. Azuma, K.; Tamaki, K.; Munro, W.J. All-photonic intercity quantum key distribution. *Nat. Commun.* **2015**, *6*, 10171. [CrossRef] [PubMed]