entropy

MDPI

Article

Open-Destination Measurement-Device-Independent Quantum Key Distribution Network

Wen-Fei Cao [1,2], Yi-Zheng Zhen [1,2], Yu-Lin Zheng [1,2], Shuai Zhao [1,2], Feihu Xu [1,2,*], Li Li [1,2,*], Zeng-Bing Chen [3,*], Nai-Le Liu [1,2,*] and Kai Chen [1,2,*]

[1] Hefei National Laboratory for Physical Sciences at Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei 230026, China; caowf@mail.ustc.edu.cn (W.-F.C.); yizheng@mail.ustc.edu.cn (Y.-Z.Z.); ylzheng@mail.ustc.edu.cn (Y.-L.Z.); zssa@mail.ustc.edu.cn (S.Z.)

[2] CAS Center for Excellence and Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei 230026, China

[3] National Laboratory of Solid State Microstructures and School of Physics, Nanjing University, Nanjing 210093, China

[*] Correspondence: feihuxu@ustc.edu.cn (F.X.); eidos@ustc.edu.cn(L.L.); zbchen@nju.edu.cn(Z.-B.C.); nlliu@ustc.edu.cn(N.-L.L.); kaichen@ustc.edu.cn(K.C.)

Received: 16 August 2020; Accepted: 22 September 2020; Published: 26 September 2020

Abstract: Quantum key distribution (QKD) networks hold promise for sharing secure randomness over multi-parties. Most existing QKD network schemes and demonstrations are based on trusted relays or limited to point-to-point scenario. Here, we propose a flexible and extensible scheme named as open-destination measurement-device-independent QKD network. The scheme enjoys security against untrusted relays and all detector side-channel attacks. Particularly, any users can accomplish key distribution under assistance of others in the network. As an illustration, we show in detail a four-user network where two users establish secure communication and present realistic simulations by taking into account imperfections of both sources and detectors.

Keywords: quantum cryptography; quantum key distribution; quantum network; measurement-device-independent

PACS: 03.67.Dd; 03.67.Hk

1. Introduction

Quantum key distribution (QKD) [1–4] provides unconditional security between distant communication parties based on the fundamental laws of quantum physics. In the last three decades, QKD has achieved tremendous progress in both theoretical developments and experimental demonstrations. To extend to a large scale, the QKD network holds promise to establish an unconditionally secure global network. Different topologies for QKD network have been demonstrated experimentally during the past decades [5–11]. However, due to high demanding on security and the relatively low detection efficiency, the realization of large-scale QKD networks is still challenging.

On the one hand, many previous demonstrations of quantum networks heavily rely on the assumption of trusted measurement devices. From security point of view, however, such assumption is challenging in realistic situations, as various kinds of detector side-channel attacks are found due to the imperfections of practical devices [12–16]. Fortunately, measurement-device-independent QKD (MDI-QKD) protocol [17,18] can remove all kinds of attacks in the detector side-channel. Since its security does not rely on any assumptions on measurement devices, MDI-QKD networks are expected to close the security loophole existing in the previous QKD networks. The MDI-QKD network has been discussed theoretically in Ref. [19,20], and a preliminary experimental MDI-QKD network demonstration was realized very recently [21].

On the other hand, most of the existing QKD networks are limited to point-to-point QKD. When expanded to multi-partite QKD case, the complexity increases, and the efficiency decreases significantly. Recent study shows that multi-partite entanglement can speed up QKD in networks [22]. Therefore, it is highly desirable to develop variously novel schemes of QKD networks if assisted by multi-partite entanglement source. Then, an immediate problem comes out: how to design a QKD network enjoying security against untrusted measurement devices and simultaneously offer practical applicability for arbitrary scalability? This is exactly the purpose of this work.

In this paper, we propose a flexible and extensible protocol named as open-destination MDI-QKD network, by combining the idea of open-destination teleportation [23] and MDI-QKD [17,18]. In this protocol, secure communication between any two users in the network can be accomplished under assistance of others. The open-destination feature allows these two-party users share secure keys simultaneously, where we also generalize to the case of C communication users. Remarkably, this feature allows communication users not to be specified before the measurement step, which makes the network flexible and extendable. Furthermore, the MDI feature enables this scheme to be secure against untrusted relays and all detector side-channel attacks. Specially, all users need only trusted state-preparation devices at hand, while the untrusted relay section is made by entangled resources and measurement devices.

2. Open-Destination MDI-QKD Network

Consider an N-party quantum network. We are particularly interested in the case where arbitrary two users want to share secure keys. This scenario is denoted as $(N, 2)$ for convenience. To simplify the discussion, here we focus on the star-type network, where both the user and a central source emit quantum signals. The signals are measured by untrusted relays located between each user and the central source.

2.1. Protocol

The $(N, 2)$ open-destination MDI-QKD runs as follows. An illustration of the $(4, 2)$ example is shown in Figure 1.

Step. 1 **Preparation**: A third party, which may be untrusted, prepares N-partite GHZ state

$$|GHZ\rangle_N = \frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N}), \tag{1}$$

where $|0\rangle$ and $|1\rangle$ denote two eigenstates of the computational basis Z. All users prepare BB84 polarization states, i.e., $|0\rangle$, $|1\rangle$, $|+\rangle$, and $|-\rangle$ with $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ being the two eigenstates of the basis X. The third party and all users distribute the prepared quantum states to their relays, which may also be untrusted.

Step. 2 **Measurement**: The relays perform Bell state measurements (BSMs). When using linear optical setups, only two outcomes related to projections on $|\psi^{\pm}\rangle = (|01\rangle \pm |10\rangle)/\sqrt{2}$ can be distinguished.

Step. 3 **Announcement**: All relays announce their successful BSM results among a public classical authenticated channel. The two communication users announce their photons bases, and other users announce their states prepared in the X basis.

Step. 4 **Sifting**: The two communication user keep the strings where all the relays get successful BSM results and other users use X bases. Then, they discard the strings where different preparation bases are used. To guarantee their strings to be correctly correlated, one of the two users flip or not flip his/her bit according to the corresponding BSM results and other users' prepared states (see Appendix A for details). Then, the two users obtain the raw key bits.

Step. 5 **Post-processing**: The two communication users estimate the quantum phase error and quantum bit error rate (QBER) in Z and X bases, according to which they further perform error correction and privacy amplification to extract correct and secure keys.

In this protocol, the multi-partite GHZ state between distant users can also be established through a prior distributed singlets, following the scheme of Bose *et al.* [24]. In fact, the open-destination feature allows arbitrary two users in the network to share secure keys based on the same experiment statistics. To accomplish the task of MDI-QKD among arbitrary two users, a natural scheme is to establish direct MDI-QKD between each two users. This requires either the central source to adjust his devices such that EPR pairs (the maximally entangled quantum states of a two qubit system, named after Einsetin, Podolski and Rosen Paradox [25]) are sent along desired directions, or a number $N(N-1)/2$ of two-user combinations to establish direct MDI-QKD using the same number of untrusted relays. The open-destination scheme is an alternative scheme. It does not require the central source to adjust his devices according to the demand of communications, at the same time involve only N untrusted relays. In a practical scenario, all the users can use weak coherent pulses to reduce experimental cost and apply decoy-state techniques [26–28] to avoid photon-number-splitting attack, as well as to estimate the gain and the error rate.

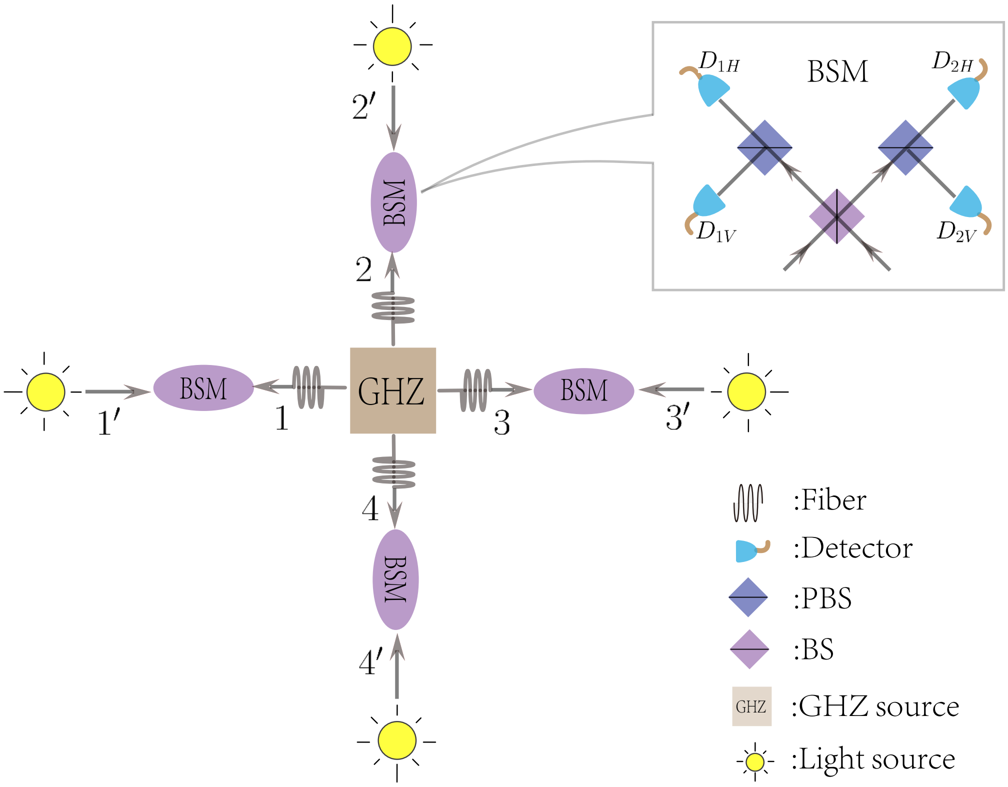

Figure 1. An optical diagram for the polarization-encoding $(4,2)$ open-destination measurement-device-independent quantum key distribution (MDI-QKD) network. The GHZ source outputs 4-partite GHZ entangled state in polarization and the light source outputs BB84 polarization state. The BSM represents the Bell state measurement, where BS is the 50:50 beam splitter, PBS is the polarization beam splitter, and D_{1H}, D_{2H}, D_{1V}, and D_{2V} are single-photon detectors. A click in D_{1H} and D_{2V}, or in D_{1V} and D_{2H}, indicates a projection into the Bell state $|\psi^-\rangle = (|01\rangle - |10\rangle)/\sqrt{2}$, and a click in D_{1H} and D_{1V}, or in D_{2H} and D_{2V}, indicates a projection into the Bell state $|\psi^+\rangle = (|01\rangle + |10\rangle)/\sqrt{2}$.

2.2. Correctness and Security Analysis

We will show the correctness and security of the open-destination MDI-QKD protocol, i.e., the communication users end up with sharing a common key in an honest run and any eavesdropper can only obtain limited information of the final key. The following analysis applies for the $(N,2)$ case. As an illustration, we show a detailed derivation of the $(4,2)$ in Appendix A.

For the correctness of the protocol, we show that after successful BSMs and other users announce the X-basis states, the two communication users can perform flip their bits locally to obtain perfectly correlated sifted keys. We start from rewriting the GHZ state as

$$|GHZ\rangle_N = \frac{1}{\sqrt{2}}\left[|00\rangle_{12}\bigotimes_{k=3\ldots N}\frac{|+\rangle_k+|-\rangle_k}{\sqrt{2}}+|11\rangle_{12}\bigotimes_{k=3\ldots N}\frac{|+\rangle_k-|-\rangle_k}{\sqrt{2}}\right], \tag{2}$$

$$= \left(\frac{1}{\sqrt{2}}\right)^{N-1}\sum_{\chi}\left(|00\rangle_{12}+(-1)^{\sigma_\chi}|11\rangle_{12}\right)|\chi\rangle_{3\ldots N}. \tag{3}$$

Here, $\chi \in \{+,-\}^{N-2}$ is a string of $N-2$ bits with bit value "+" or "−" and $\sigma_\chi = 0(1)$ if the number of "−" is even (odd).

We label each user by $1', 2', \ldots, N'$ and let the two communication users be $1'$ and $2'$. In a successful run of the protocol, suppose that users $1'$ and $2'$ prepare states $|\alpha\rangle, |\beta\rangle \in \{0,1,+,-\}$, respectively, and other users $3', \ldots, N'$ prepare state in the X basis, denoted as a string $\chi' \in \{+,-\}^{N-2}$. In addition, denote the successful BSM results as a string $v \in \{+,-\}^N$, with the kth bit v_k denoting the BSM outcome on the state prepared by the user k' and the k-th particle of the GHZ state. Here, $v_k = \pm$ corresponds to projections $|\psi^\pm\rangle\langle\psi^\pm|$, respectively. Then, when other users send states denoted by $|\chi'\rangle$ and when all untrusted relays announce successful BSM results v, the equivalent measurement $M_{12}^{\chi',v}$ on $1'$ and $2'$ is

$$\sqrt{M_{1'2'}^{\chi',v}}\,|\alpha\beta\rangle_{1'2'} = \left(\bigotimes_k \langle\psi^{v_k}|_{kk'}\right)|GHZ\rangle_N \otimes |\alpha\beta\rangle_{1'2'}\,|\chi'\rangle_{3'\ldots N'}, \tag{4}$$

$$= \left(\frac{1}{\sqrt{2}}\right)^{N-1}\sum_{\chi}\langle\psi^{v_1}|_{11'}\langle\psi^{v_2}|_{22'}\left(|00\rangle_{12}+(-1)^{\sigma_\chi}|11\rangle_{12}\right)|\alpha\beta\rangle_{1'2'}$$
$$\times\prod_{k=3\ldots N}\langle\psi^{v_k}|_{kk'}\,|\chi\rangle_k\,|\chi'\rangle_{k'}, \tag{5}$$

$$\propto \left(\langle 00|_{1'2'}+(-1)^{\tau}\langle 11|_{1'2'}\right)|\alpha\beta\rangle_{1'2'}. \tag{6}$$

Here, $\tau = \sigma_{\chi'\oplus\tilde{v}} \oplus v_1 \oplus v_2$ with $\tilde{v} = v_3 v_4 \ldots v_N \in \{+,-\}^{N-2}$ and $\sigma_{\chi'\oplus\tilde{v}} = +(-)$ if the number of "−" in $\chi' \oplus \tilde{v}$ is even (odd). Therefore, when the user $1'$ and $2'$ both prepare Z-basis states, or when they both prepare X-basis states with $\tau = 0$, the corresponding strings are correctly correlated; otherwise, when they both prepare X-basis states but $\tau = 1$, their strings are anticorrelated, and one party needs to flip all his/her bits.

For the security of the protocol, here we show that an open-destination MDI-QKD can be equivalent to a standard bipartite MDI-QKD if we only focus on the two communication users. Recall that, in the standard MDI-QKD, two parties, Alice and Bob, prepare and send quantum signals to a remote untrusted relay, which announces a successful BSM result or not. In our scheme, one can treat all parts outside the two users $1'$ and $2'$ as an untrusted relay [29]. That is, the GHZ source, the BSM setups and all other users serve as a big untrusted relay, and the successful BSM results in the standard MDI-QKD corresponds to all BSMs announcing successful measurements together with all other users announcing X-basis states (see Figure A1 as an example of the $(4,2)$ case). In this sense, our scheme is reduced to the MDI-QKD and the two has the same security. Additionally, although we require the preparation device of each user to be trusted in the protocol, the two communication users need not to trust these preparation devices of other users.

2.3. Key Generation Rate

The key generation rate for open-destination MDI-QKD can be derived similarly as the standard MDI-QKD, i.e., by converting it to an entanglement purification scheme. Suppose that the two communication users both have virtual singlets at their hands and then send one particle to the untrusted relays. In a successful run of the protocol, the remaining virtual particles of the two communication users will be entangled. When the entanglement between the virtual particles is sufficiently strong, the monogamy property of entanglement [30–32] guarantees the extraction of information-theoretically secure key bits between the two users. In this sense, the secret key rate can be roughly viewed as the gains of entanglement purification in the asymptotic case. Taking account of imperfections, such as basis misalignment, channel loss, and dark counts of the detectors, the key generation rate is given by the GLLP method [33]

$$R_2 = Q^{ZZ}\left[1 - H\left(e^{XX}\right) - fH\left(e^{ZZ}\right)\right]. \tag{7}$$

Here, we have assumed that the user $1'$ and $2'$ use Z basis to generate keys and use X basis to estimate phase errors. In the equation, Q^{ZZ} denotes the overall gain in the Z basis, and e^{XX} (e^{ZZ}) denotes the phase (bit) error rate, $f > 1$ is the error correction inefficiency for the error correction process, and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. In a realistic experiment, if using weak coherent pulses and adopting decoy-state techniques, Q^{ZZ}, e^{ZZ}, and e^{XX} can be efficiently estimated [27,28].

2.4. Comparison with the Standard MDI-QKD

The open-destination MDI-QKD network is different from the conventional MDI-QKD. The main difference comes from the open-destination feature, which in fact allows the all 2-party users in the network generate their own secure keys independently and simultaneously. There are in fact $N(N-1)/2$ combinations of such two-party users. If one uses the conventional MDI-QKD scheme, the same number of untrusted relays are required. To increase the communication distance, one may further add the same number of relays and EPR sources to construct the user-relay-EPR source-relay-user structure. Such construction of quantum network could be expensive considering the number of devices required. One could also use the optical switches to reduce the number of relays; however, in this case the communication would be arranged in time order and some users have to wait. In the open-destination scheme, N untrusted relays are sufficient to connect each other supplied with good-quality GHZ central source. Although the distribution of GHZ states may lead to other technological challenges, the open-destination scheme can reduce the number of devices significantly in constructing the network. As for the performance, the two schemes in fact have similar performance in the ideal case. The difference is that the open-destination scheme generates secure keys for any two-party users in one round of implementation while the bipartite MDI-QKD scheme costs $N(N-1)/2$ rounds. Furthermore, the open-destination scheme also establishes conference key agreements among arbitrary users, which can not be accomplished directly via the bipartite MDI-QKD. We will discuss this case in the next section.

3. Numerical Simulation

As an example, we will analyze the secure key rate for the $(4,2)$ open-destination MDI-QKD (see Appendices B and C for details). For simplicity, the single-photon source and the asymptotic approximations are assumed. We let the BSM setups be located in each user's side, although, in a realistic experiment, the BSM setups can be located in anywhere to increase the communication distance. We suppose that quantum channels are identically depolarizing such that untrusted relays receive the GHZ state in a mixture form [34]:

$$\rho = p\,|GHZ\rangle\,\langle GHZ|_4 + \frac{1-p}{16}\mathbb{I}_{16}, \tag{8}$$

where $0 \leq p \leq 1$. We also assume that all detectors are identical, i.e., they have the same dark count rates and the same detection efficiencies. After numerical simulation, the lower bound of secure key rates with respective to communication distance between user and central source are shown in Figure 2.

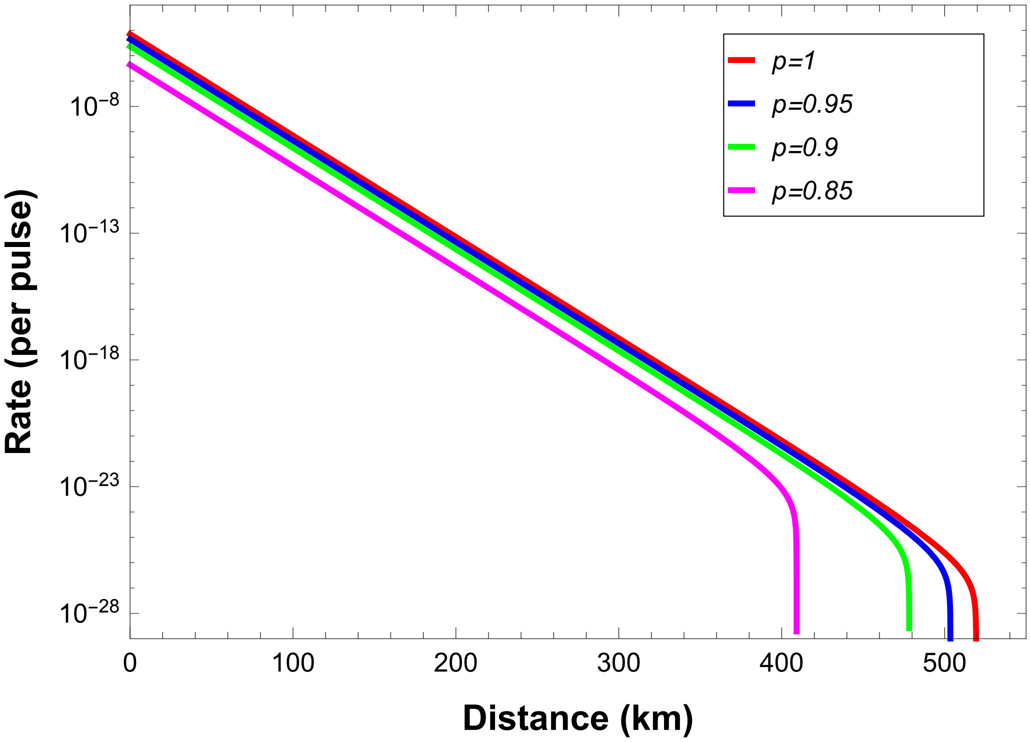

Figure 2. Lower bound on the secret key rate R versus communication distance between communication users using Werner-like states source. The red line denotes $p = 1$, i.e., the perfect GHZ source. The parameters are chosen according to experiments [35] : the detection efficiency $\eta_d = 40\%$, the misalignment-error probability of the system $e_d = 2\%$, the dark count rate of the detector $p_d = 8 \times 10^{-8}$, the error correction efficiency $f = 1.16$, the intrinsic loss coefficient of the standard telecom fiber channel $\alpha = 0.2$ dB/km.

The simulation shows that the secure key rate and the largest communication distance decrease when p decreases. To implement open-destination MDI-QKD efficiently, good-quality GHZ sources and single-photon sources are necessary. If such requirements are satisfied, our scheme can tolerate a high loss of more than 500 km of optical fibers, i.e., 100 dB, using perfect GHZ source and single-photon source, even when the BSM setups are located in every user's side. One can double the communication distance by putting the BSM setups in the middle of the users and the GHZ source, which is similar with the case in MDI-QKD [17,18]. For the realistic case where weak coherent pulses are used, our analysis can be generalized by considering the decoy state method [27,28] and following the procedures in Refs. [36,37].

4. Generalization to The (N,C) Case

As aforementioned, the complete analysis has been focused on the $(N, 2)$ open-destination MDI-QKD case. Here, we show that the case of two communication users can also generalized to the case of C communication users. Note that the open-destination feature enables any C users to generate secure keys at the same time.

Suppose that, in an N-party quantum network with users $1, 2, \cdots, N$, the communication users are denoted by the subset $\mathcal{C} = \{i_1, i_2, \ldots, i_C\}$, where $C = |\mathcal{C}|$. The auxiliary set denoted by $\mathcal{A}$ consists of auxiliary users, i.e., users that assist communication users to generate secure keys, with $A = |\mathcal{A}| = N - C$ users. According to Equation (3), for a general C communication users case, the GHZ state can be rewritten as

$$|GHZ\rangle_N = \frac{1}{\sqrt{2}}\left[|00\cdots0\rangle_{12\cdots C} \bigotimes_{k=C+1\ldots N} \frac{|+\rangle_k + |-\rangle_k}{\sqrt{2}} + |11\cdots1\rangle_{12\cdots C} \bigotimes_{k=C+1\ldots N} \frac{|+\rangle_k - |-\rangle_k}{\sqrt{2}}\right], \tag{9}$$

$$= \left(\frac{1}{\sqrt{2}}\right)^{N-1} \sum_{\chi} \left(|00\cdots0\rangle_{12\cdots C} + (-1)^{\sigma_\chi} |11\cdots1\rangle_{12\cdots C}\right) |\chi\rangle_{C+1\ldots N} \,. \tag{10}$$

Here, $\chi \in \{+,-\}^{N-C}$ is a string of $N - C$ bits with bit value "$+$" or "$-$" and $\sigma_\chi = 0(1)$ if the number of "$-$" is even (odd). Intuitively, with the assistance of $N - C$ auxiliary users, C-qubit GHZ states are shared among arbitrary C communication users. Meanwhile, based on the C-qubit GHZ state, the communication users can complete different quantum information tasks with the merit of open destination, such as quantum conference key agreement [24,34,38–40] and quantum secret sharing [39,41–43]. In general, we call it the (N, C) open-destination quantum communication task. When $C = 2$, and the aim is to establish QKD, the task is reduced to the $(N, 2)$ open-destination MDI-QKD network discussed above.

For instance, in the general case of (N, C) open-destination quantum conference key agreement, all users prepares and sends BB84 states to their respective untrusted relays. The central source simultaneously distribute the GHZ state, which is measured together with the state from user on the untrusted relay. When the relays announce successful BSM outcomes and when all auxiliary users announce their prepared states in X-basis, the communication users virtually share a multipartite entangled state, as the same of the $(N, 2)$ case. After suitable local operations of bit flips, all communication users share correctly correlated bits.

By slightly modifying the scheme, the experimental cost, especially the number of detectors can be reduced significantly. For instance, when all users announce their preparation basis X for assisting others while keep the bits corresponding to Z basis for distill the key, any C users can share secure keys simultaneously. This is because their respective sifted keys corresponds to different portions of the raw data. If one insists on using the conventional two-party QKD and multi-party conference key agreement scheme to realize the same function of the open-destination scheme under discussion, about $(2^N - 2)N$ detectors are required. In the open-destination scheme, the number of detectors is reduced to $4N$, which only increases linearly with the user number N.

As an example, we consider the case of $(N, 3)$ open-destination quantum conference key agreement. From Equation (10), the post-selected 3-party GHZ state is $|\phi^{\pm}_{\text{3-party}}\rangle = (|000\rangle \pm |111\rangle)/\sqrt{2}$ according to the announcements of the states and the BSM results related with auxiliary users. Meanwhile, as shown in Table 1, an equivalent GHZ analyzer among three communication users can be obtained according to the post-selected GHZ state $|\phi^{\pm}_{\text{3-party}}\rangle$ and the BSM results of their corresponding relays. Then, according to the MDI-QCC protocol in Ref. [39], $(N, 3)$ open-destination quantum conference key agreement can be directly conducted based on the equivalent GHZ analyzer.

Table 1. The equivalent GHZ analyzer measurement results of three communication users. Here, GHZ^A denotes the post-selected GHZ state from the GHZ source; BSM result 1(2,3) denotes the BSM results of three relays nearby the communication users' side; GHZ analyzer^C denotes the results of corresponding GHZ analyzer among three communication users.

GHZ^A	BSM Result 1	BSM Result 2	BSM Result 3	GHZ Analyzer^C
$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$	$\lvert\psi^+\rangle$	$\lvert\psi^+\rangle$	$\lvert\psi^+\rangle$	$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$
$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$	$\lvert\psi^+\rangle$	$\lvert\psi^+\rangle$	$\lvert\psi^-\rangle$	$\lvert\phi^-_{3\text{-party}}\rangle$ $(\lvert\phi^+_{3\text{-party}}\rangle)$
$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$	$\lvert\psi^+\rangle$	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$	$\lvert\phi^-_{3\text{-party}}\rangle$ $(\lvert\phi^+_{3\text{-party}}\rangle)$
$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$	$\lvert\psi^+\rangle$	$\lvert\psi^-\rangle$	$\lvert\psi^-\rangle$	$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$
$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$	$\lvert\psi^+\rangle$	$\lvert\phi^-_{3\text{-party}}\rangle$ $(\lvert\phi^+_{3\text{-party}}\rangle)$
$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$	$\lvert\psi^-\rangle$	$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$
$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$	$\lvert\psi^-\rangle$	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$	$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$
$\lvert\phi^+_{3\text{-party}}\rangle$ $(\lvert\phi^-_{3\text{-party}}\rangle)$	$\lvert\psi^-\rangle$	$\lvert\psi^-\rangle$	$\lvert\psi^-\rangle$	$\lvert\phi^-_{3\text{-party}}\rangle$ $(\lvert\phi^+_{3\text{-party}}\rangle)$

Similar to the open-destination MDI-QKD in Section (2) of the $(N, 2)$ case, the security of the $(N, 3)$ open-destination quantum conference key agreement is also based on the entanglement purification discussion [39,44,45]. According to the multi-partite entanglement purification scheme [46], the secret key rate can be written as follows [34,39,40]:

$$R_3 = Q^Z\{1 - f \cdot \max[H(E^Z_{12}), H(E^Z_{13})] - H(E^X)\}, \tag{11}$$

where Q^Z is the overall gains when three communication users send out quantum states in Z basis, E^Z_{12} (E^Z_{13}) is the marginal quantum bit error rate between user 1 and user 2 (3) in Z basis, E^X is the overall quantum bit error rate in X basis, f is the error correction efficiency, and $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. Q^Z, E^X, E^Z_{12}, and E^Z_{13} can be gotten directly from the experimental results. Meanwhile, the estimation of key rate can be slightly different if the sources of users are weak coherent states [33].

5. Conclusions

As a conclusion, we proposed a flexible and extensible scheme of the $(N, 2)$ open-destination MDI-QKD network. We proved the correctness and security of the protocol, and derived practical key generation rate formula. For an illustration, we studied a specific network where two of four users want to distill quantum secure keys. For the scenario, we presented a polarization-encoding scheme for experimental implementation and offered in detail a simulation by taking the imperfections in both source and detectors into account. The simulation results show that the scheme enjoys a promising structure and performance in real-life situation.

A significant virtue of our scheme is the security against untrustful relays and all detector side-channel attacks. Moreover, the open-destination feature enables any two users to establish MDI-QKD without changing the network structures. In fact, one can establish MDI-QKD among arbitrary users even after the entangled source have been distributed and all the measurements have been completed. Furthermore, following the multi-entanglement swapping scheme, the network can be extended into a large scale by adding shared multi-partite GHZ states.

We would like to remark that currently the efficiency was relatively low (seen from Figure 2). This can be overcome by taking optimization in network topology, basis selections, and measurements for both the auxiliary and communication parties, as well as considering asymmetric loss for various channels, etc., like techniques adopted in Ref. [47]. Any future improvement on distributing multipartite entanglement efficiently and effectively will definitely benefit the proposed scheme and push it forward practical applications.

Author Contributions: Conceptualization, K.C.; methodology, F.X., L.L., N.-L.L., and K.C.; software, W.-F.C. and Y.-L.Z.; validation, Y.-Z.Z., Y.-L.Z., and K.C.; investigation, W.-F.C., Y.-Z.Z.; Writing—Original draft preparation, W.-F.C., Z.-Y.Z., and S.Z.; Writing—Review and editing, F.X., L.L., Z.-B.C., N.-L.L., and K.C.; visualization, W.-F.C., N.-L.L., and K.C.; supervision, F.X., L.L., Z.-B.C., N.-L.L., and K.C.; All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Chinese Academy of Science, the National Fundamental Research Program, the National Natural Science Foundation of China (Grants No. 11575174, No. 11374287, No. 61125502, No. 11574297, and No. 61771443), as well as the Fundamental Research Funds for the Central Universities (WK2340000083).

Acknowledgments: We thank Yu-Ao Chen and Qiang Zhang for valuable and enlightening discussions.

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

Appendix A. Sifting Procedure of The (4,2) Case

In this section, we describe the sifting procedure of open-destination MDI-QKD in detail for the $(4,2)$ case. We will show that such scenario can be reduced to the standard MDI-QKD scenario. The general case can be proved in a similar way, as shown in the main text. The schematic diagram is depicted in Figure A1a.

We start by writing the GHZ state as

$$\begin{aligned} |GHZ\rangle_4 =& \frac{1}{2\sqrt{2}}[(|00\rangle + |11\rangle)(|{++}\rangle + |{--}\rangle) \\ &+ (|00\rangle - |11\rangle)(|{+-}\rangle + |{-+}\rangle)]. \end{aligned} \tag{A1}$$

Up to the announcement of the quantum state of users $3'$ and $4'$, the BSM(s) of relays 3 and 4 on the received quantum state from GHZ source and quantum state from users $3'(4')$ can be treated as an equivalent projective measurement on the whole GHZ state. Specifically, if the relays 3 and 4 perform the BSM and obtain equivalent projective measurement results $|00\rangle$ or $|11\rangle$ ($|01\rangle$ or $|10\rangle$), the photons received by relays 1 and 2 will be projected into state $|\phi^+\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ ($|\phi^-\rangle = (|00\rangle - |11\rangle)\sqrt{2}$) according to Equation (A1). After announcement of the successful BSM results and the quantum states of auxiliary users $3'$ and $4'$, the projected state received by relays 1 and 2 can be determined. So, one can treat the GHZ source, the BSM setups of relays 3 and 4 and the quantum state of auxiliary user $3'$ and $4'$ as an virtual entanglement source, which outputs different Bell states. The protocol is thus directly equivalent to MDI-QKD with an entangled source in the middle [29] as illustrated in Figure A1b. Since the virtual Bell state with two BSMs along each side can be equivalent to a virtual BSM, the scheme is finally equivalent to implement MDI-QKD between users $1'$ and $2'$ as showed in Figure A1c. Therefore, in an honest run, the protocol is reduced to the honest standard MDI-QKD scenario, and the parties will end up with sharing a common key.

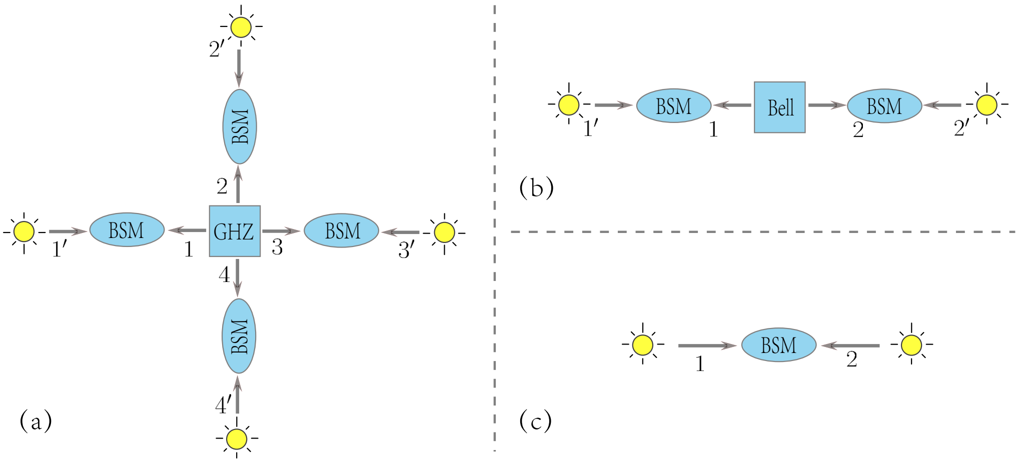

Figure A1. (**a**) The schematic diagram for the $(4, 2)$ open-destination MDI-QKD scheme. Users $1'$ and $2'$ denote communication users, while users $3'$ and $4'$ denote auxiliary users. (**b**) The equivalent topological schematic diagram when users $1'$ and $2'$ communicate with each other. According to BSM results of relays 3 and 4 and quantum states of auxiliary users $3'$ and $4'$, the GHZ state is projected to a virtual Bell state. (**c**) The final equivalent topological schematic diagram that users $1'$ and $2'$ perform MDI-QKD, according to the BSM results and the virtual Bell state.

Firstly, notice that the projection measurement of two systems onto one Bell state can be viewed as a POVM (positive operator valued measure) on one system if one knows the state of the other system. For example, as shown in Figure A1a, a successful BSM result of $|\psi^-\rangle$ of the relay 3 with auxiliary photons from auxiliary $3'$ in the state $|\alpha\rangle_3^{\prime}$ can be viewed as a POVM $\mathrm{tr}_{3'}\left[|\psi^-\rangle\langle\psi^-|_{33'}\,|\alpha\rangle\langle\alpha|_{3'}\right]$ on the state 3. In the open-destination scheme, we have $|\alpha\rangle \in \{|+\rangle, |-\rangle\}$ and the BSM results $\{|\psi^+\rangle, |\psi^-\rangle\}$. The correspondence between the POVM on the system k and the untrusted relay announces a successful BSM together with auxiliary state are listed in Table A1.

Table A1. The correspondence between the POVM on state labeled k and the BSM result labeled by kk' with auxiliary state labeled by k'.

State of System k'	**BSM Result on Systems kk'**	**POVM on System k**
$\|+\rangle$	$\|\psi^-\rangle$	$\|-\rangle\langle-\|/2$
$\|-\rangle$	$\|\psi^-\rangle$	$\|+\rangle\langle+\|/2$
$\|+\rangle$	$\|\psi^+\rangle$	$\|+\rangle\langle+\|/2$
$\|-\rangle$	$\|\psi^+\rangle$	$\|-\rangle\langle-\|/2$

Secondly, when the two auxiliary users prepare X-basis photons and the corresponding relays get successful BSM results, according to Table A1, the total GHZ state collapses into one of the maximally entangled states $|\phi^\pm\rangle = \frac{1}{\sqrt{2}}(|HH\rangle \pm |VV\rangle)$ at the side of two communication users.

Thirdly, at the sides of the two communication users, according to the post-selected Bell state $|\phi^\pm\rangle$ and the BSM results of their corresponding relays, a BSM between two communication users can be obtained. Such correspondence is listed in Table A2.

Table A2. The equivalent BSM results of two communication users. Here, Bell^A denotes the post-selected Bell state from the GHZ source; BSM result 1(2) denotes the BSM results of the two relays nearby the communication users' side; BSM^C denotes the results of corresponding BSM between two communication users.

Bell^A	**BSM Result 1**	**BSM Result 2**	**BSM^C**
$\lvert\phi^+\rangle$	$\lvert\psi^+\rangle$	$\lvert\psi^+\rangle$	$\lvert\phi^+\rangle$
$\lvert\phi^+\rangle$	$\lvert\psi^+\rangle$	$\lvert\psi^-\rangle$	$\lvert\phi^-\rangle$
$\lvert\phi^+\rangle$	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$	$\lvert\phi^-\rangle$
$\lvert\phi^+\rangle$	$\lvert\psi^-\rangle$	$\lvert\psi^-\rangle$	$\lvert\phi^+\rangle$
$\lvert\phi^-\rangle$	$\lvert\psi^+\rangle$	$\lvert\psi^+\rangle$	$\lvert\phi^-\rangle$
$\lvert\phi^-\rangle$	$\lvert\psi^+\rangle$	$\lvert\psi^-\rangle$	$\lvert\phi^+\rangle$
$\lvert\phi^-\rangle$	$\lvert\psi^-\rangle$	$\lvert\psi^+\rangle$	$\lvert\phi^+\rangle$
$\lvert\phi^-\rangle$	$\lvert\psi^-\rangle$	$\lvert\psi^-\rangle$	$\lvert\phi^-\rangle$

Finally, as shown in Table A3, according to the final equivalent BSM result and the preparation bases, one of the communication users apply a bit flip or not such that their keys can be correlated. In fact, only when both communication users select X basis and the final equivalent BSM result is $|\phi^-\rangle$, one of them needs to apply a bit flip. After many rounds, they obtain enough raw key bits that can be used in the following data post-processing process.

Table A3. Flip table according to the preparation bases and the equivalent BSM result at communication users side.

Basis	$\lvert\boldsymbol{\phi}^+\rangle$	$\lvert\boldsymbol{\phi}^-\rangle$
Z-basis	No Flip	No Flip
X-basis	No Flip	Flip

Appendix B. Detector Analysis

Since the BSM with the auxiliary photon is equivalent to an probabilistic projective measurement, one can use an equivalent detector to replace the BSM device with the corresponding light source in the key rate analysis. Here, we develop a method to derive the equivalent detector parameters, i.e., the detection efficiency and the dark count of the equivalent detector. We use the BSM setup with polarization encoding as illustrated in Figure A2.

In H/V basis, suppose that Alice and Bob encode the same polarization states; then, the state becomes as follows after the BS:

$$a_H^\dagger b_H^\dagger \left|vac\right\rangle \to (a_{1H}^{\dagger 2} - a_{2H}^{\dagger 2}) \left|vac\right\rangle , \tag{A2}$$

where $a^\dagger$ ($b^\dagger$) denotes creation operators, and $|vac\rangle$ denotes vacuum state. The probability of the successful BSM when the input states are $|H\rangle$ and $|H\rangle$, is given by

$$P_{HH} = 2p_d(1-p_d)^2(1-(1-p_d)(1-\eta_d)^2), \tag{A3}$$

where η_d is the detection efficiency, and p_d is the dark count. Suppose that Alice and Bob encode different polarization state; then, after the BS, the state becomes as follows:

$$\begin{aligned} a_H^\dagger b_V^\dagger \left|vac\right\rangle \to &(a_{1H}^\dagger a_{1V}^\dagger - a_{2H}^\dagger a_{2V}^\dagger) \left|vac\right\rangle \\ &+ (a_{2H}^\dagger a_{1V}^\dagger - a_{1H}^\dagger a_{2V}^\dagger) \left|vac\right\rangle . \end{aligned} \tag{A4}$$

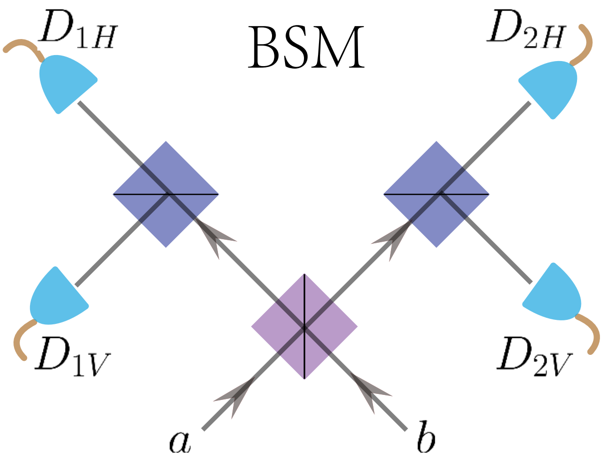

Figure A2. The BSM setup with polarization encoding. BS denotes beam splitter, PBS denotes polarization beam splitter, and H and V denote, respectively, horizontal and vertical linear polarizations, and D_{1H}, D_{2H}, D_{1V}, D_{2V} denote single-photon detectors. A click in D_{1H} and D_{2V}, or in D_{1V} and D_{2H}, indicates a projection into the Bell state $|\psi^-\rangle = (|HV\rangle - |VH\rangle)/\sqrt{2}$, and a click in D_{1H} and D_{1V}, or in D_{2H} and D_{2V}, indicates a projection into the Bell state $|\psi^+\rangle = (|HV\rangle + |VH\rangle)/\sqrt{2}$.

The probability of the successful BSM when the input states are $|H\rangle$ and $|V\rangle$ is given by

$$P_{HV} = (1-p_d)^2(1-(1-p_d)(1-\eta_d))^2. \tag{A5}$$

Thus, the equivalent detection probability when the input state is $|H\rangle$ is given by

$$\begin{aligned}\eta_H^{'} =&\frac{1}{2}(1-p_d)^2[2p_d(1-(1-p_d)(1-\eta_d)^2)\\&+(1-(1-p_d)(1-\eta_d))^2].\end{aligned} \tag{A6}$$

Due to symmetry, the equivalent detection probability when the input state is $|V\rangle$ has the same form with the case that the input state is $|H\rangle$, i.e., one has $\eta_V^{'} = \eta_H^{'}$. Similarly, by using the transformation relation under $\{+,-\}$ basis

$$\begin{aligned}a_+^\dagger b_+^\dagger\,|vac\rangle &\rightarrow (a_{1H}^\dagger a_{1V}^\dagger - a_{2H}^\dagger a_{2V}^\dagger)\,|vac\rangle\\ a_+^\dagger b_-^\dagger\,|vac\rangle &\rightarrow (a_{1H}^\dagger a_{2V}^\dagger - a_{1V}^\dagger a_{2H}^\dagger)\,|vac\rangle\,,\end{aligned} \tag{A7}$$

one can ontain the equivalent detection probability when the input state is $|+\rangle$ as follows:

$$\eta_+^{'} =(1-p_d)^2(1-(1-p_d)(1-\eta_d))^2. \tag{A8}$$

Due to symmetry, one has $\eta_-^{'} = \eta_+^{'}$.

We consider practical experimental parameters, which are listed in Table A4. For the experimental parameters, one arrives at

$$\eta_d^{'Z} = 0.08, \quad \eta_d^{'X} = 0.16, \tag{A9}$$

where $\eta_d^{'Z}$ denotes the equivalent detection efficiency for H/V basis, i.e., Z basis, and $\eta_d^{'X}$ denotes the equivalent detection efficiency for $+/-$ basis, i.e., X basis.

Table A4. List of experimental parameters used for simulation. η_d is the detection efficiency; e_d is the misalignment-error probability of the system; p_d is the dark count rate of the detector; f is error correction efficiency; α is the intrinsic loss coefficient of the standard telecom fiber channel.

η_d	e_d	p_d	f	α(dB/km)
40%	2%	8×10^{-8}	1.16	0.2

To calculate the parameters for equivalent dark count, one should consider the case in which there was no incoming photon. Suppose the local photon being $|H\rangle$, and the incoming photon being vacumm state, the states become as follows after the BS:

$$b_H^\dagger |vac\rangle \to \frac{i}{\sqrt{2}} a_{1H}^\dagger + \frac{1}{\sqrt{2}} a_{2H}^\dagger, \tag{A10}$$

where $b_H^\dagger$ denotes the creation operator of local photon. So, one can get the probability of the successful BSM as follows:

$$P_H = 2p_d(1-p_d)^2\eta_d. \tag{A11}$$

Due to symmetry, one has that $P_+ = P_- = P_V = P_H$. Here, P_x denotes the probability of the successful BSM result when the local photon is $|x\rangle$ and there is no incoming photon. So, one can get the equivalent dark count as

$$p_d^{'} = 2p_d(1-p_d)^2\eta_d. \tag{A12}$$

For the experimental parameters given in Table A4, one arrives at

$$p_d^{'} = 6.4 \times 10^{-8}. \tag{A13}$$

Finally, one can achieve the parameters for the equivalent detectors shown in Table A5.

Table A5. List of the parameters for the equivalent detectors. $\eta_d^{'Z}$ ($\eta_d^{'X}$) denotes the equivalent detection efficiency for Z (X) basis, and $p_d^{'}$ denotes the equivalent dark count.

$\eta_d^{'Z}$	$\eta_d^{'X}$	$p_d^{'}$
8%	16%	6.4×10^{-8}

Appendix C. Simulation for (4,2)-Scenario

For simulation purposes, one can assume practically that the source has the form of Werner-like states

$$\rho = p\,|GHZ\rangle\,\langle GHZ|_4 + \frac{1-p}{16}\mathbb{I}, \tag{A14}$$

in which $|GHZ\rangle_4 = (|HHHH\rangle + |VVVV\rangle)/\sqrt{2}$ is the 4-partite GHZ states, $\mathbb{I}/16$ is the 4-partite maximal mixed states, and $0 \le p \le 1$. As proven in the previous section, according to the measurement results of auxiliary side, the photons received by communication side will be projected into different Bell states. Here, we consider the case in which auxiliary side get the $|+\rangle \otimes |+\rangle$ results, due to the symmetry. When auxiliary side get the $|+\rangle \otimes |+\rangle$ result, the particles received by communication side will collapse into

$$\rho_{\mathrm{AB}} = p\,|\phi^+\rangle\,\langle\phi^+| + \frac{1-p}{4}\mathbb{I}, \tag{A15}$$

where $\phi^+ = (|HH\rangle + |VV\rangle)/\sqrt{2}$ is one of the Bell states. So, it is equivalent with the case in which the two communication users (denoted by Alice and Bob) perform an entanglement-based QKD using the two-qubit Werner states ρ_{AB} as a source and the equivalent detectors as detection device, as illustrated in Figure A3, from the perspective of key rate analysis.

Taking these imperfections of the source and detectors into account, the key generation rate in a realistic setup will be given by

$$R = Q_{11}^{ZZ}(1 - H(e_{11}^{XX})) - Q_{\mu\nu}^{ZZ} \cdot f \cdot H(E_{\mu\nu}^{ZZ}). \tag{A16}$$

In the following, we discuss how one can derive each quantity in this key rate formula, i.e., Q_{11}^{ZZ}, e_{11}^{XX}, $Q_{\mu\nu}^{ZZ}$, and $E_{\mu\nu}^{ZZ}$.

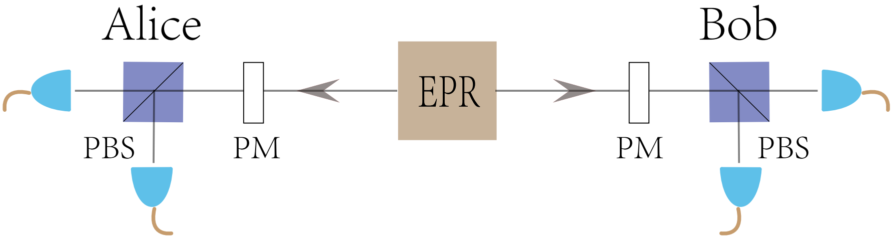

Figure A3. Equivalent setup for Alice and Bob when tracing the BSM results of the auxiliary users. PBS denotes polarization beam splitter, PM denotes polarization modulator, and EPR denotes EPR source.

Yield. Denote the yield of single-photon pair as Y_{11}, i.e., the conditional probability of a coincidence detection event given that the entanglement source emits an single-photon pair. Then, Y_{11} is given by

$$Y_{11} = [1 - (1 - Y_{0A})(1 - \eta_A)][1 - (1 - Y_{0B})(1 - \eta_B)], \tag{A17}$$

where $Y_{0A} = Y_{0B} = p_d^{'}$ are the background count rates on Alice's and Bob's sides in the Z basis, and $\eta_A = \eta_B = \eta_d^{'Z} \times 10^{-\alpha L/20}$ denotes the total detection efficiency considering the channel loss. Equation (A17) is also applicable to the X basis. Then, the gain of the single photon part and the overall gain are given by

$$Q_{\mu\nu}^{ZZ} = Q_{11}^{ZZ} = Y_{11}. \tag{A18}$$

Error Rate. The error rate of single-photon pair in the X basis e_{11}^{XX} has three main contributions taking some imperfections into account: (i) *The imperfections of entanglement source*, i.e., the maximal mixed states component, which brings 50% error rate $e_0 = 1/2$; (ii) *Background counts*, which are random noises $e_0 = 1/2$; (iii) *Intrinsic detector error e_d*, which characterizes the alignment and stability of the optical system. So, the error rate of single-photon pair e_{11}^{XX} is given as follows:

$$e_{11}^{XX} Y_{11} = pe_0(Y_{11} - \eta_A\eta_B) + pe_d\eta_A\eta_B + (1 - p)e_0 Y_{11}, \tag{A19}$$

where the first item comes from background counts, the second term comes from intrinsic errors, and the third term comes from the mixed part of the source. So, one achieves the error rate of single-photon pair e_{11}^{XX} as follows:

$$e_{11}^{XX} = e_0 - \frac{p\eta_A\eta_B(e_0 - e_d)}{Y_{11}}. \tag{A20}$$

Similarly, the error rate in the Z basis is given by

$$E_{\mu\nu}^{ZZ} = e_0 - \frac{p\eta_A\eta_B(e_0 - e_d)}{Y_{11}}. \tag{A21}$$

Reference

1. Bennett, C.H.; Brassard, G. Quantum cryptography: Public key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computer System and Signal Processing*; IEEE: New York, NY, USA, 1984; p. 175.
2. Ekert, A.K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **1991**, *67*, 661–663. [CrossRef] [PubMed]
3. Gisin, N.; Ribordy, G.; Tittel, W.; Zbinden, H. Quantum cryptography. *Rev. Mod. Phys.* **2002**, *74*, 145–195. [CrossRef]
4. Scarani, V.; Bechmann-Pasquinucci, H.; Cerf, N.J.; Dušek, M.; Lütkenhaus, N.; Peev, M. The security of practical quantum key distribution. *Rev. Mod. Phys.* **2009**, *81*, 1301–1350. [CrossRef]
5. Elliott, C. The DARPA quantum network. In *Quantum Communications and Cryptography*; CRC Press: Boca Raton, FL, USA, 2005; pp. 83–102.
6. Peev, M.; Pacher, C.; Alléaume, R.; Barreiro, C.; Bouda, J.; Boxleitner, W.; Debuisschert, T.; Diamanti, E.; Dianati, M.; Dynes, J.; et al. The SECOQC quantum key distribution network in Vienna. *New J. Phys.* **2009**, *11*, 075001. [CrossRef]
7. Chen, T.Y.; Wang, J.; Liang, H.; Liu, W.Y.; Liu, Y.; Jiang, X.; Wang, Y.; Wan, X.; Cai, W.Q.; Ju, L.; et al. Metropolitan all-pass and inter-city quantum communication network. *Opt. Express* **2010**, *18*, 27217–27225. [CrossRef]
8. Sasaki, M.; Fujiwara, M.; Ishizuka, H.; Klaus, W.; Wakui, K.; Takeoka, M.; Miki, S.; Yamashita, T.; Wang, Z.; Tanaka, A.; et al. Field test of quantum key distribution in the Tokyo QKD Network. *Opt. Express* **2011**, *19*, 10387–10409. [CrossRef]
9. Fröhlich, B.; Dynes, J.F.; Lucamarini, M.; Sharpe, A.W.; Yuan, Z.; Shields, A.J. A quantum access network. *Nature* **2013**, *501*, 69. [CrossRef]
10. Qiu, J. Quantum communications leap out of the lab. *Nature (London)* **2014**, *508*, 441. [CrossRef]
11. Liao, S.K.; Cai, W.Q.; Handsteiner, J.; Liu, B.; Yin, J.; Zhang, L.; Rauch, D.; Fink, M.; Ren, J.G.; Liu, W.Y.; et al. Satellite-Relayed Intercontinental Quantum Network. *Phys. Rev. Lett.* **2018**, *120*, 030501. [CrossRef]
12. Qi, B.; Fung, C.H.F.; Lo, H.K.; Ma, X. Time-shift Attack in Practical Quantum Cryptosystems. *Quantum Inf. Comput.* **2007**, *7*, 073.
13. Zhao, Y.; Fung, C.H.F.; Qi, B.; Chen, C.; Lo, H.K. Quantum hacking: Experimental demonstration of time-shift attack against practical quantum-key-distribution systems. *Phys. Rev. A* **2008**, *78*, 042333. [CrossRef]
14. Lydersen, L.; Wiechers, C.; Wittmann, C.; Elser, D.; Skaar, J.; Makarov, V. Hacking commercial quantum cryptography systems by tailored bright illumination. *Nat. Photonics* **2010**, *4*, 686–689. [CrossRef]
15. Gerhardt, I.; Liu, Q.; Lamas-Linares, A.; Skaar, J.; Kurtsiefer, C.; Makarov, V. Full-field implementation of a perfect eavesdropper on a quantum cryptography system. *Nat. Commun.* **2011**, *2*, 349. [CrossRef] [PubMed]
16. Weier, H.; Krauss, H.; Rau, M.; Fürst, M.; Nauerth, S.; Weinfurter, H. Quantum eavesdropping without interception: An attack exploiting the dead time of single-photon detectors. *New J. Phys.* **2011**, *13*, 073024. [CrossRef]
17. Lo, H.K.; Curty, M.; Qi, B. Measurement-Device-Independent Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130503. [CrossRef]
18. Braunstein, S.L.; Pirandola, S. Side-Channel-Free Quantum Key Distribution. *Phys. Rev. Lett.* **2012**, *108*, 130502. [CrossRef]
19. Xu, F.; Curty, M.; Qi, B.; Qian, L.; Lo, H.K. Discrete and continuous variables for measurement-device-independent quantum cryptography. *Nat. Photonics* **2015**, *9*, 772. [CrossRef]
20. Pirandola, S.; Ottaviani, C.; Spedalieri, G.; Weedbrook, C.; Braunstein, S.L.; Lloyd, S.; Gehring, T.; Jacobsen, C.S.; Andersen, U.L. Reply to Discrete and continuous variables for measurement-device-independent quantum cryptography. *Nat. Photonics* **2015**, *9*, 773. [CrossRef]
21. Tang, Z.; Wei, K.; Bedroya, O.; Qian, L.; Lo, H.K. Experimental measurement-device-independent quantum key distribution with imperfect sources. *Phys. Rev. A* **2016**, *93*, 042308. [CrossRef]
22. 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]

23. Zhao, Z.; Chen, Y.A.; Zhang, A.N.; Yang, T.; Briegel, H.J.; Pan, J.W. Experimental demonstration of five-photon entanglement and open-destination teleportation. *Nature* **2004**, *430*, 54–58. [CrossRef] [PubMed]
24. Bose, S.; Vedral, V.; Knight, P.L. Multiparticle generalization of entanglement swapping. *Phys. Rev. A* **1998**, *57*, 822–829. [CrossRef]
25. Einstein, A.; Podolsky, B.; Rosen, N. Can Quantum-Mechanical Description of Physical Reality Be Considered Complete? *Phys. Rev.* **1935**, *47*, 777. [CrossRef]
26. Hwang, W.Y. Quantum Key Distribution with High Loss: Toward Global Secure Communication. *Phys. Rev. Lett.* **2003**, *91*, 057901. [CrossRef]
27. Lo, H.K.; Ma, X.; Chen, K. Decoy State Quantum Key Distribution. *Phys. Rev. Lett.* **2005**, *94*, 230504. [CrossRef]
28. Wang, X.B. Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *94*, 230503. [CrossRef]
29. 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]
30. Koashi, M.; Winter, A. Monogamy of quantum entanglement and other correlations. *Phys. Rev. A* **2004**, *69*, 022309. [CrossRef]
31. Osborne, T.J.; Verstraete, F. General Monogamy Inequality for Bipartite Qubit Entanglement. *Phys. Rev. Lett.* **2006**, *96*, 220503. [CrossRef]
32. Ou, Y.C.; Fan, H.; Fei, S.M. Proper monogamy inequality for arbitrary pure quantum states. *Phys. Rev. A* **2008**, *78*, 012311. [CrossRef]
33. Gottesman, D.; Lo, H.K.; Lütkenhaus, N.; Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **2004**, *4*, 325.
34. Chen, K.; Lo, H.K. Multi-partite quantum cryptographic protocols with noisy GHZ states. *Quantum Inf. Comput.* **2007**, *7*, 689.
35. Tang, Y.L.; Yin, H.L.; Chen, S.J.; Liu, Y.; Zhang, W.J.; Jiang, X.; Zhang, L.; Wang, J.; You, L.X.; Guan, J.Y.; et al. Measurement-Device-Independent Quantum Key Distribution over 200 km. *Phys. Rev. Lett.* **2014**, *113*, 190501. [CrossRef] [PubMed]
36. Curty, M.; Xu, F.; Cui, W.; Lim, C.C.W.; Tamaki, K.; Lo, H.K. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **2014**, *5*, 3732. [CrossRef]
37. Xu, F.; Xu, H.; Lo, H.K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **2014**, *89*, 052333. [CrossRef]
38. Chen, K.; Lo, H.K. Conference key agreement and quantum sharing of classical secrets with noisy GHZ states. In Proceedings of the International Symposium on Information Theory (ISIT 2005), Adelaide, SA, Australia, 4–9 September 2005; pp. 1607–1611. [CrossRef]
39. 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]
40. 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]
41. Hillery, M.; Bužek, V.; Berthiaume, A. Quantum secret sharing. *Phys. Rev. A* **1999**, *59*, 1829–1834. [CrossRef]
42. Cleve, R.; Gottesman, D.; Lo, H.K. How to Share a Quantum Secret. *Phys. Rev. Lett.* **1999**, *83*, 648–651. [CrossRef]
43. Chen, Y.A.; Zhang, A.N.; Zhao, Z.; Zhou, X.Q.; Lu, C.Y.; Peng, C.Z.; Yang, T.; Pan, J.W. Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography. *Phys. Rev. Lett.* **2005**, *95*, 200502. [CrossRef]
44. Lo, H.K.; Chau, H.F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **1999**, *283*, 2050–2056. [CrossRef] [PubMed]
45. Shor, P.W.; Preskill, J. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.* **2000**, *85*, 441. [CrossRef] [PubMed]

46. Maneva, E.N.; Smolin, J.A. Improved two-party and multi-party purification protocols. *Contemp. Math.* **2002**, *305*, 203–212.
47. Wang, W.; Xu, F.; Lo, H.K. Asymmetric Protocols for Scalable High-Rate Measurement-Device-Independent Quantum Key Distribution Networks. *Phys. Rev. X* **2019**, *9*, 041012. [CrossRef]

© 2020 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (http://creativecommons.org/licenses/by/4.0/).