Equitable Multiparty Quantum Communication Without a Trusted Third Party

Tanumoy Pramanik,[1,2,†] Dong-Hwa Lee,[1,3,†] Young-Wook Cho,[1] Hyang-Tag Lim,[1] Sang-Wook Han,[1,3] Hojoong Jung,[1] Sung Moon,[1,3] Kwang Jo Lee,[4] and Yong-Su Kim[1,3,*]

[1] *Center for Quantum Information, Korea Institute of Science and Technology (KIST), Seoul 02792, Republic of Korea*

[2] *Currently with State Key Laboratory for Mesoscopic Physics & Collaborative Innovation Center of Quantum Matter, Peking University, Beijing 100871, China*

[3] *Division of Nano & Information Technology, KIST School, Korea University of Science and Technology, Seoul 02792, Republic of Korea*

[4] *Department of Applied Physics, Kyung Hee University, Yongin 17104, Republic of Korea*

(Received 26 March 2020; revised 5 November 2020; accepted 1 December 2020; published 29 December 2020)

Multiparty quantum communication provides delightful applications, including quantum cryptographic communication and quantum secret sharing. Quantum communication based on the Greenberg-Horne-Zeilinger (GHZ) state measurement provides a practical way to implement multiparty quantum communication. With the standard *spatially localized* GHZ state measurement, however, information can be imbalanced among the communication parties that can cause significant problems in some applications of multiparty cryptographic communication, e.g., secret sharing. Here, we propose an equitable multiparty quantum communication where information balance among the communication parties is achieved without a trusted third party. Our scheme is based on the GHZ state measurement that is not spatially localized but implemented in a way that all the distant communication parties symmetrically participate. We also verify the feasibility of our scheme by presenting the proof-of-principle experimental demonstration of informationally balanced three-party quantum communication using weak coherent pulses.

DOI: 10.1103/PhysRevApplied.14.064074

I. INTRODUCTION

Quantum key distribution (QKD) provides the information-theoretically secure way to share random bit strings between two remote parties [1,2]. Significant theoretical and experimental efforts have been dedicated to improving the security and practicality of QKD. For instance, measurement-device-independent QKD (MDI QKD), which is based on the entanglement detection in the middle of two communication parties, provides higher security than other ordinary QKD protocols since it is immune to all quantum hacking attempts to the measurement devices [3–6]. Recently, MDI QKD has been further improved to twin-field QKD (TF QKD) that enables much longer communication distance [7–11]. These remarkable works, however, are focused on the secret communication between two parties.

There are delightful multiparty quantum communication applications, such as quantum cryptographic conferencing [12,13] and quantum secret sharing [14–16]. These multiparty quantum communication protocols are usually based on distributing multipartite entanglement, e.g., the Greenberger-Horne-Zeilinger (GHZ) state. However, due to the difficulty in generating the multipartite GHZ state, it is challenging to implement multiparty quantum communication. Indeed, there exists only a few proof-of-principle experiments of multiparty quantum communication [17–19] and the long distance GHZ state distribution [20]. Remarkably, one can circumvent this difficulty by employing the idea of the MDI protocol based on the GHZ state measurement [21]. Despite the compromising performance, quantum communication based on the GHZ state measurement can be implemented using weak coherent pulses with decoy states [22]. Therefore, it provides a more practical solution for multiparty quantum communication than those based on the GHZ state generation.

In order to fully enjoy the benefits of multiparty cryptographic communication, it is significant to retain information equitability among the communication parties [23,24]. For instance, in secret sharing, each party has the same size of random bits p_i as a private key and the secret is encoded as $s = p_1 \oplus p_2 \oplus \cdots \oplus p_N$. Here, "$\oplus$" and the subscript N denote the bitwise exclusive OR and the number of communication parties, respectively. The secret s can be restored only when all N parties cooperate. If, however, one knows the private keys of the other parties, the secret can be reconstructed by less than N parties. Therefore, for the

*yong-su.kim@kist.re.kr

†These authors contributed equally to this work.

security of secret sharing, information equitability among the communication parties should be guaranteed. Information equitability should also be maintained when quantum communication is applied to multiparty cryptographic communication for information-theoretical security.

In ordinary multiparty quantum communication based on the GHZ state measurement, it is assumed that the GHZ state measurement is performed by one of the communication parties or a third party [21]. This assumption is reasonable since entanglement detection cannot be performed via local operation and classical communication [25]. Note that the security of this scheme is based on the measurement-induced entanglement, and, thus, the third party can be considered as an eavesdropper. However, information imbalance among the communication parties follows if one of the parties cooperates with the third party in secret. Considering the importance of information equitability in multiparty cryptographic communication, it is critical to rule out this information imbalance possibility.

In this paper, we propose an equitable multiparty quantum communication protocol where information balance among the communication parties is achieved without a trusted third party. Our protocol is based on the GHZ state measurement that is not exclusively performed by one of the communication parties or a third party, but equally shared by all communication parties. We also show the feasibility of our protocol by presenting the proof-of-principle experimental demonstration using weak coherent pulses.

II. THEORY

A. Standard multiparty quantum communication

1. Quantum communication with honest parties

Let us introduce the multiparty quantum communication protocol based on the GHZ state measurement shown in Fig. 1(a) [21]. Standard three-party quantum communication can be performed via the following steps. Here, for simplicity, we assume that the communication parties utilize single-photon states.

Step 1. Each communication party generates single-photon states that are randomly encoded as one of the four states used in the Bennett-Brassard 84 (BB84) protocol [1], i.e., $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and then transmits them to an honest third party, David. Here, $|\pm\rangle = (1/\sqrt{2})(|0\rangle \pm |1\rangle)$.

Step 2. David performs the GHZ state measurement and announces the results.

Step 3. The communication parties reveal their basis. If they have chosen the same basis, keep the cases for generating sifted keys. If not, discard the cases.

Step 4. Using Table I, each communication party can generate sifted keys with her (his) own state and the GHZ state measurement result.

Step 4(a): quantum cryptographic conference. If the single-photon states are prepared in the Z basis, i.e., either $|0\rangle$ or $|1\rangle$, the successful GHZ state

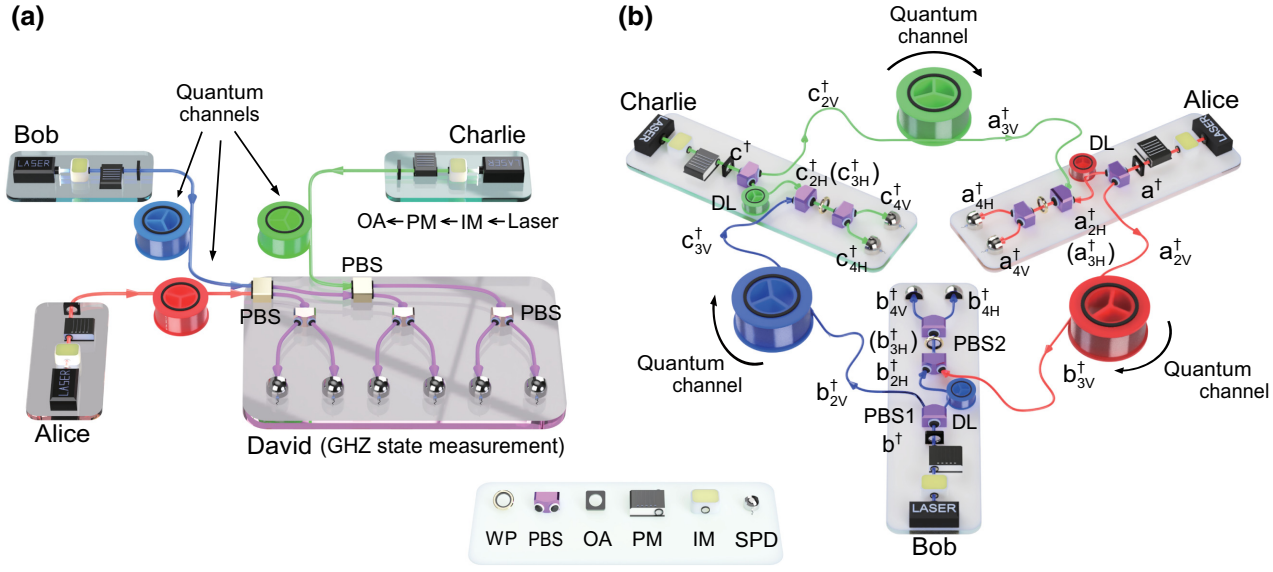

FIG. 1. Schematics of (a) ordinary multiparty quantum communication based on the GHZ state measurement and (b) equitable multiparty quantum communication without a trusted third party. In ordinary multiparty quantum communication, the communication parties send optical pulses to David, who performs the GHZ state measurement. In equitable multiparty quantum communication, the GHZ state measurement is not performed *locally*, but all the communication parties equally participate in the GHZ state measurement. Here SPD is the single-photon detector, IM is the intensity modulator, PM is the polarization modulator, OA is the optical attenuator, PBS is the polarization beamsplitter, WP is the waveplate, and DL is the delay line.

TABLE I. The probability of the GHZ state measurement result according to the encoded input state. The columns labeled single photons and coherent pulses denote for the optical pulses of single photons and weak coherent pulses, respectively.

Encoded input states			GHZ state measurement probability			
			Single photons		Coherent pulses	
Alice	Bob	Charlie	$\|\mathrm{GHZ}^+\rangle$	$\|\mathrm{GHZ}^-\rangle$	$\|\mathrm{GHZ}^+\rangle$	$\|\mathrm{GHZ}^-\rangle$
$\|0\rangle$	$\|0\rangle$	$\|0\rangle$	1/2	1/2	1/2	1/2
$\|0\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	0	0
$\|0\rangle$	$\|1\rangle$	$\|0\rangle$	0	0	0	0
$\|0\rangle$	$\|1\rangle$	$\|1\rangle$	0	0	0	0
$\|1\rangle$	$\|0\rangle$	$\|0\rangle$	0	0	0	0
$\|1\rangle$	$\|0\rangle$	$\|1\rangle$	0	0	0	0
$\|1\rangle$	$\|1\rangle$	$\|0\rangle$	0	0	0	0
$\|1\rangle$	$\|1\rangle$	$\|1\rangle$	1/2	1/2	1/2	1/2
$\|+\rangle$	$\|+\rangle$	$\|+\rangle$	1	0	5/8	3/8
$\|+\rangle$	$\|-\rangle$	$\|-\rangle$	1	0	5/8	3/8
$\|-\rangle$	$\|+\rangle$	$\|-\rangle$	1	0	5/8	3/8
$\|-\rangle$	$\|-\rangle$	$\|+\rangle$	1	0	5/8	3/8
$\|-\rangle$	$\|-\rangle$	$\|-\rangle$	0	1	3/8	5/8
$\|-\rangle$	$\|+\rangle$	$\|+\rangle$	0	1	3/8	5/8
$\|+\rangle$	$\|-\rangle$	$\|+\rangle$	0	1	3/8	5/8
$\|+\rangle$	$\|+\rangle$	$\|-\rangle$	0	1	3/8	5/8

measurement result implies that all communication parties transmit the same states, either $|000\rangle$ or $|111\rangle$. Therefore, all communication parties can share the same bit information.

Step 4(b): quantum secret sharing. If the single-photon states are prepared in the X basis, i.e., either $|+\rangle$ or $|-\rangle$, each communication party cannot note the bit information of the other parties but can note their correlation. For example, if the $|\mathrm{GHZ}^+\rangle = (1/\sqrt{2})(|000\rangle + |111\rangle)$ measurement result is announced and Alice has transmitted $|+\rangle$ ($|-\rangle$), she can note that Bob's and Charlie's bits are the same (different), i.e., $X_B = X_C$ ($X_B = X_C + 1$).

Step 5. The communication parties utilize some parts of the sifted keys to calculate the quantum bit error rate (QBER). If the QBER is sufficiently small, they conclude that they successfully share sifted keys, and perform error correction and privacy amplification for generating secret keys. If the QBER is too high, they interrupt the protocol.

Note that the number of communication parties can be further increased since the GHZ state measurement scheme can be generalized with an arbitrary number of photons [26]. It is also remarkable that this protocol can be implemented using weak coherent pulses with decoy states. The intrinsic QBER with the weak coherent pulses, as shown in Table I, are $Q_Z = 0$ and $Q_X = \frac{3}{8}$ for the Z and X bases, respectively. We note that the nonzero QBER for the X basis can be mitigated by postselecting the phase of weak coherent pulses [21,27,28].

2. Quantum communication with a dishonest party

In the aforementioned multiparty quantum communication scenario, David can be assumed to be an eavesdropper since his eavesdropping can be revealed with the cooperation of all communication parties [21]. This assumption is valid when Alice, Bob, and Charlie are honest and cooperate for the cryptographic communication. If, however, one of the communication parties is dishonest and wants to obtain more information than the other parties, the assumption is no longer valid. In order to investigate the information imbalance in the standard quantum communication scenario, let us assume that David is secretly cooperating with Alice, who wants to get more information than the others. Equivalently, one can simply consider that David belongs to Alice, so the GHZ state measurement is simply performed by Alice. In this case, Alice has more information than Bob and Charlie; see the procedure below.

Step 1. Each communication party generates single-photon states that are randomly encoded as one of the BB84 states, i.e., $\{|0\rangle, |1\rangle, |+\rangle, |-\rangle\}$, and then transmits them to David.

Step 2. Instead of performing the GHZ state measurement, David performs a simple projective measurement on the same bases according to Alice's encoding state. For example, if Alice sends $|0\rangle$ ($|+\rangle$), David projects all the photons on the Z (X) basis. Note that David can know Alice's encoding state before he gets the photons since they have a secret collaboration.

Step 3. Based on the projective measurement results, David announces the (fake) GHZ state measurement result according to Table I.

Step 3(a): the Z-basis projection measurement. If David measures $|000\rangle$ or $|111\rangle$, he randomly announces either the result $|\mathrm{GHZ}^{+}\rangle$ or $|\mathrm{GHZ}^{-}\rangle$. If he measures other states, e.g., $|001\rangle$, he says that he failed to measure the case.

Step 3(b): the X-basis projection measurement. If David measures $|++{+}\rangle$, $|+{-}{-}\rangle$, $|{-}+{-}\rangle$, or $|{-}{-}{+}\rangle$, he announces the result $|\mathrm{GHZ}^{+}\rangle$. For the other measurement results $|{-}{-}{-}\rangle$, $|{-}{+}{+}\rangle$, $|+{-}{+}\rangle$, and $|+{+}{-}\rangle$, he says that he got $|\mathrm{GHZ}^{-}\rangle$.

Step 4. When the successful GHZ state measurement results are announced, Alice, Bob, and Charlie reveal their bases. The sifted keys are generated when all three communication parties have utilized the same basis. In other words, the sifted keys are generated when Bob's and Charlie's bases are the same as that of Alice.

Step 5. Since David performed a simple projection measurement based on Alice's state, he has full information about all the communication parties' keys when the sifted keys are successfully generated. For example, in the case of the X-basis projection measurement, David (equivalently, Alice) knows not only the correlation between Bob's and Charlie's bits but also their individual bits. Note that David's measurement does not have any error since he always chose the right basis with the help of Alice. On the other hand, Bob (Charlie) only knows the correlation between Alice's and Charlie's (Bob's) bits. This information imbalance among communication parties is not appropriate in the secret sharing scenario [23,24].

Step 6. The communication parties utilize some part of the sifted key to calculate the QBER. If the QBER is sufficiently small, they conclude that they successfully share sifted keys, and perform error correction and privacy amplification for generating secret keys. If the QBER is too high, they interrupt the protocol. Note, however, that the QBER cannot detect the hidden cooperation between Alice and David.

The above procedure clearly shows that standard multiparty quantum communication can cause information imbalance among the communication parties, and it cannot be detected by the other parties. This is because the third party, who exclusively possesses the GHZ state measurement, is cooperating with one of the communication parties in secret, and the other parties cannot discern this hidden cooperation. If one can implement the GHZ state measurement in such a way that all communication parties equally participate, we can rule out hidden collaboration between the third party and one of the communication parties. Therefore, it is essential to implement the symmetrical GHZ state measurement among all communication parties for information balance in multiparty quantum cryptographic communication.

B. Equitable multiparty quantum communication

For information balance among communication parties, the GHZ state measurement should be implemented in a way that all communication parties equally participate. Implementation of the symmetrical GHZ state measurement among distant parties without a third party is not straightforward since entanglement cannot be increased by local operation and classical communication.

In linear optical quantum information processing, two-qubit interaction can be implemented using two-photon interference and postselection. It is remarkable that the origin of two-photon interference is not through particle-particle interaction at a *localized* region, but through interference between indistinguishable probability amplitudes [29–31]. Recently, we have shown that two-photon entanglement generation and measurement can be implemented without the two photons overlapping at a localized region [32,33]. By applying this principle to the multiple photon case, we can implement equitable multiparty quantum communication.

In Fig. 1(b) we present a schematic of our proposed equitable multiparty quantum communication. Likewise, in standard quantum communication, Alice, Bob, and Charlie prepare optical pulses in an eigenstate of either the X or Z basis. Then, they send the probability amplitude $|1\rangle$ to the next party, e.g., Alice $\rightarrow$ Bob, Bob $\rightarrow$ Charlie, and Charlie $\rightarrow$ Alice, while keeping the probability amplitude $|0\rangle$. Then, they combine the receiving $|1\rangle$ state with their own $|0\rangle$ state and measure it in the X basis. The successful GHZ state measurement results are registered when each communication party receives a single-photon counting click, and thus a threefold coincidence count is measured among Alice, Bob, and Charlie. It is remarkable that the GHZ state measurement is not performed in a spatially localized region, but equally shared by the communication parties, Alice, Bob, and Charlie.

Let us describe how Fig. 1(b) performs the GHZ state measurement among distant parties. To prove the GHZ state measurement, let us consider the polarization GHZ input states of

$$\begin{aligned}|\mathrm{GHZ}^{\pm}\rangle &= \frac{1}{\sqrt{2}}(|HHH\rangle \pm |VVV\rangle)\\ &= \frac{1}{\sqrt{2}}(a_{1H}^{\dagger}b_{1H}^{\dagger}c_{1H}^{\dagger} \pm a_{1V}^{\dagger}b_{1V}^{\dagger}c_{1V}^{\dagger})|0\rangle, \qquad (1)\end{aligned}$$

where $|H\rangle$ and $|V\rangle$ denote the horizontal and vertical polarization states that correspond to the logical states of $|0\rangle$

and $|1\rangle$, respectively. The operators $a^\dagger$, $b^\dagger$, and $c^\dagger$ are the creation operators at Alice, Bob, and Charlie, respectively, and the subscript nP refers to spatial mode n with polarization state P. After the PBS1, the states evolve to

$$|\mathrm{GHZ}^{\pm}\rangle \rightarrow \frac{1}{\sqrt{2}}(a^\dagger_{2H}b^\dagger_{2H}c^\dagger_{2H} \pm a^\dagger_{2V}b^\dagger_{2V}c^\dagger_{2V})|0\rangle. \quad (2)$$

The probability amplitude exchange, i.e., keeping the probability amplitude $|0\rangle$ (equivalently, $|H\rangle$) while sending the probability amplitude $|1\rangle$ (equivalently, $|V\rangle$) to the next party, is presented as

$$a^\dagger_{2H} \rightarrow e^{i\theta_1}a^\dagger_{3H}, \qquad b^\dagger_{2H} \rightarrow e^{i\theta_2}b^\dagger_{3H}, \qquad c^\dagger_{2H} \rightarrow e^{i\theta_3}c^\dagger_{3H}, \quad (3)$$

$$a^\dagger_{2V} \rightarrow e^{i\phi_1}b^\dagger_{3V}, \qquad b^\dagger_{2V} \rightarrow e^{i\phi_2}c^\dagger_{3V}, \qquad c^\dagger_{2V} \rightarrow e^{i\phi_3}a^\dagger_{3V}, \quad (4)$$

where θ_j and ϕ_j $(j = 1, 2, 3)$ are the phases obtained during the probability amplitude exchange. Note that Eq. (3) takes place via DLs that belong to the communication parties, whereas Eq. (4) happens via quantum channels (QCs) that can be accessed by eavesdroppers. After the PBS2 that combines two orthogonal polarization states into the same spatial mode, the states become

$$|\mathrm{GHZ}^{\pm}\rangle \rightarrow \frac{1}{\sqrt{2}}(a^\dagger_{4H}b^\dagger_{4H}c^\dagger_{4H} \pm e^{i\Phi}a^\dagger_{4V}b^\dagger_{4V}c^\dagger_{4V})|0\rangle, \quad (5)$$

where $\Phi = \Sigma_j(\phi_j - \theta_j)$. Note that we can set $\Phi = 0$ by adjusting the phase of the interferometer.

By transforming the polarization states using half waveplates (HWPs) at 22.5°, the states become

$$\begin{aligned}|\mathrm{GHZ}^{+}\rangle \rightarrow{}& \tfrac{1}{2}(a^\dagger_{4H}b^\dagger_{4H}c^\dagger_{4H} + a^\dagger_{4H}b^\dagger_{4V}c^\dagger_{4V} \\ &+ a^\dagger_{4V}b^\dagger_{4H}c^\dagger_{4V} + a^\dagger_{4V}b^\dagger_{4V}c^\dagger_{4H})|0\rangle, \\ |\mathrm{GHZ}^{-}\rangle \rightarrow{}& \tfrac{1}{2}(a^\dagger_{4H}b^\dagger_{4H}c^\dagger_{4V} + a^\dagger_{4H}b^\dagger_{4V}c^\dagger_{4H} \\ &+ a^\dagger_{4V}b^\dagger_{4H}c^\dagger_{4H} + a^\dagger_{4V}b^\dagger_{4V}c^\dagger_{4V})|0\rangle.\end{aligned}$$

Thus, the $|\mathrm{GHZ}^{+}\rangle$ state is registered as coincidences D_{HHH}, D_{HVV}, D_{VHV}, and D_{VVH}, while $|\mathrm{GHZ}^{-}\rangle$ corresponds to the coincidences D_{HHV}, D_{HVH}, D_{VHH}, and D_{VVV}, where D_{ijk} denotes threefold coincidences of the i, j, and k states at Alice, Bob, and Charlie.

In order to verify the GHZ state measurement, it is essential that the basis states other than the GHZ states do not provide the same coincidence results. For three qubit states, there are six other basis states: $|HHV\rangle$, $|HVH\rangle$, $|HVV\rangle$, $|VHH\rangle$, $|VHV\rangle$, and $|VVH\rangle$. It is remarkable that these states does not provide threefold coincidence among Alice, Bob, and Charlie due to the probability exchange transformation, Eqs. (3) and (4). Therefore, the proposed scheme successfully performs the GHZ state measurement. Note that this GHZ state measurement scheme can be implemented with an arbitrary number of qubits, so equitable multiparty quantum communication can be implemented with an arbitrary number of communication parties.

The schematic of the present multiparty quantum communication scheme is inherently symmetrical without a third party. All communication parties keep the probability amplitude $|0\rangle$ and send the probability amplitude $|1\rangle$ to the next party. The successful GHZ state measurement result is registered only when all communication parties have photon counting clicks; therefore, all communication parties should cooperate in order to determine the GHZ state measurement result. These features provide information balance among communication parties without introducing a third party.

Although our protocol utilizes the GHZ state measurement, unlike standard multiparty quantum communication based on the GHZ state measurement [21], it does not provide the MDI feature. Therefore, similar to the ordinary QKD protocols such as the BB84 protocol, the whole communication party, including the measurement setup, should be protected from quantum hacking attempts by, for instance, monitoring the radiation towards the communication parties [34,35]. We note that, in standard multiparty quantum communication based on the GHZ state measurement, the measurement devices do not need to be protected, but the transmitters should be protected.

It is worth noting that the QCs, which eavesdroppers can access freely in the quantum communication scenario, deliver very limited information, i.e., they only deliver $|V\rangle$ all the time. Therefore, it is undesirable for eavesdroppers to tap meaningful information via quantum channels without knowing the whole interferometer, including DLs that belong to the communication parties. Note also that Eqs. (3) and (4) imply that the individual transformations have no losses, or, equivalently, have identical losses. We remark that the loss imbalance between individual transformations can be balanced without introducing additional loss. Moreover, the loss analysis shows that any attempts to alter the quantum channel loss increases the QBER in the X basis. We further discuss the effect of imbalanced channel losses in Appendix A.

III. EXPERIMENT

The equitable multiparty quantum communication scheme of Fig. 1(b) requires synchronization and phase stabilization between photons traveling through different optical paths. We note that these technical demands have been realized with current technology even when the optical paths are a few hundred kilometers in order to implement TF QKD [9,11]; see also Appendix B for a proposed experimental setup to stabilize polarization and phase.

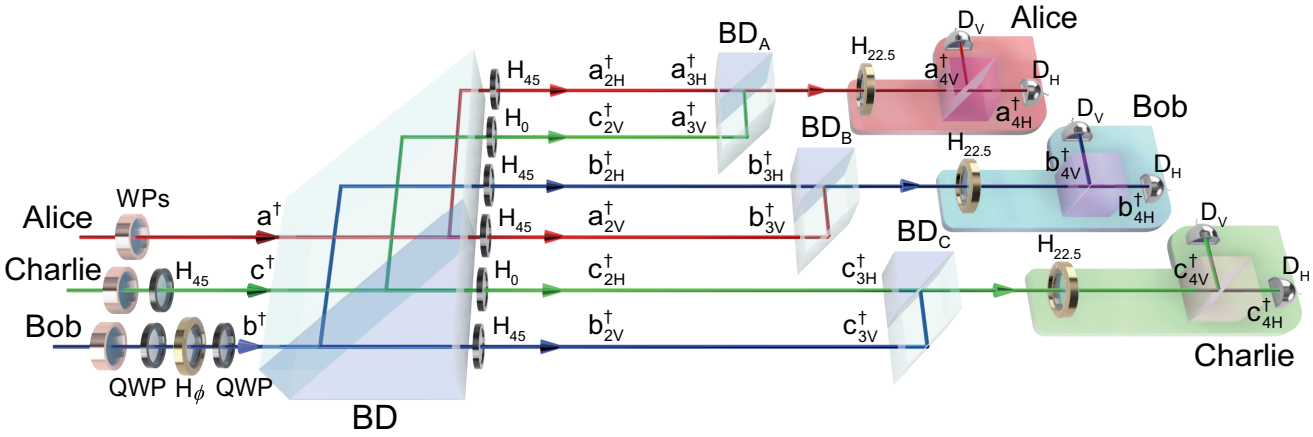

FIG. 2. The proof-of-principle experimental setup of equitable three-party quantum communication. Here BD is the beam displacer, H_ϕ is the half waveplate at θ (in degrees), and QWP is the quarter waveplate.

Here, in order to verify the feasibility and practicality of equitable multiparty quantum communication, we present the proof-of-principle experiment of three-party quantum communication on the optical table using the polarization state of weak coherent pulses.

The proof-of-principle experimental setup for equitable three-party quantum communication is depicted in Fig. 2. The optical pulses should be indistinguishable in spectrum and timing while they are mutually incoherent so as not to have first-order interference. In order to obtain such pulses, we divide a femtosecond laser pulse into three pulses and modulate them using three independent acousto-optic modulators [30,31,36]. The optical pulses are then attenuated to the average photon number per pulse of $\mu = 0.1$, and sent to the proof-of-principle experimental setup for equitable three-party quantum communication; see Fig. 2.

The polarization states of Alice, Bob, and Charlie are encoded using WPs. For convenience, Charlie flips his qubit using a HWP at 45° (H_{45}). The probability amplitudes $|H\rangle$ and $|V\rangle$ of incoming photons A, B, and C are divided by a BD that transmits and reflects horizontal and vertical polarization states, respectively. The divided probability amplitudes interfere at BD_A, BD_B, and BD_C in such a way that the necessary probability amplitude exchange of Eqs. (3) and (4) happens during the interference. To this end, the polarization states from Alice and Bob are converted from horizontal (vertical) to vertical (horizontal) by HWPs at 45°, while those from Charlie remain the same with HWPs at 0°. Note that the redundant HWPs at 0° are inserted to match the optical path lengths of the interferometers. The photons are detected by SPDs after passing through a HWP at 22.5° and a PBS. This experimental scheme provides automatic temporal synchronization and excellent phase stability without active stabilization [32,33].

In order to adjust the phase $\Phi = \Sigma_j(\phi_j - \theta_j)$, we insert a set of waveplates at the input of Bob, as shown in Fig. 2. By changing the angle H_ϕ of a HWP between two QWPs at 45°, we can tune the phase $\Phi \sim 4H_\phi$ [37]. In Fig. 3 we present the threefold coincidences between Alice, Bob, and Charlie while changing Φ with the input $|DDD\rangle$. Here, the red circles (blue squares) are the $|\mathrm{GHZ}^+\rangle$ ($|\mathrm{GHZ}^-\rangle$) projections for $\Phi = 0$ that correspond to the coincidences D_{HHH}, D_{HVV}, D_{VHV}, and D_{VVH} (D_{HHV}, D_{HVH}, D_{VHH}, and D_{VVV}). The sinusoidal fitting curves show the visibility $V = (20.5 \pm 0.2)\%$ for both the $|\mathrm{GHZ}^+\rangle$ and $|\mathrm{GHZ}^-\rangle$ projections. The limited visibility of the three-photon interference with the coherent pulses input is related to the limited QBER with weak coherent pulses [21]. During the proof-of-principle experiment of equitable three-party quantum communication, we set $\Phi = 0$.

We summarize the GHZ state measurement results with respect to various input states in Figs. 4(a) and 4(b) for the Z-basis and X-basis inputs, respectively. During the data acquisition, the phase is kept at $\Phi = 0$. For the Z-basis

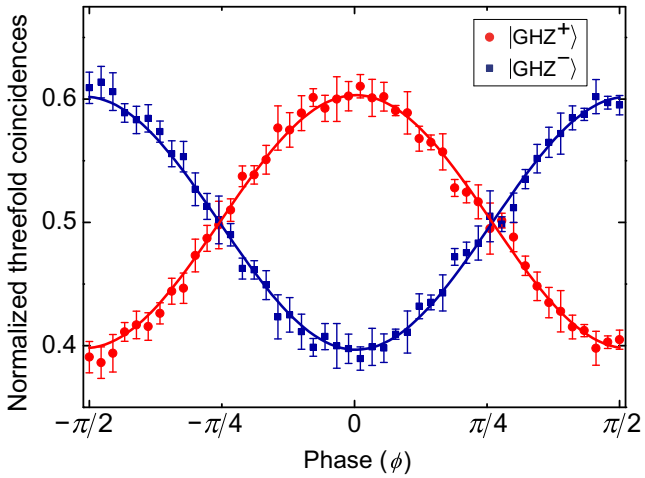

FIG. 3. Three-photon interference with respect to the phase ϕ with $|DDD\rangle$ input.

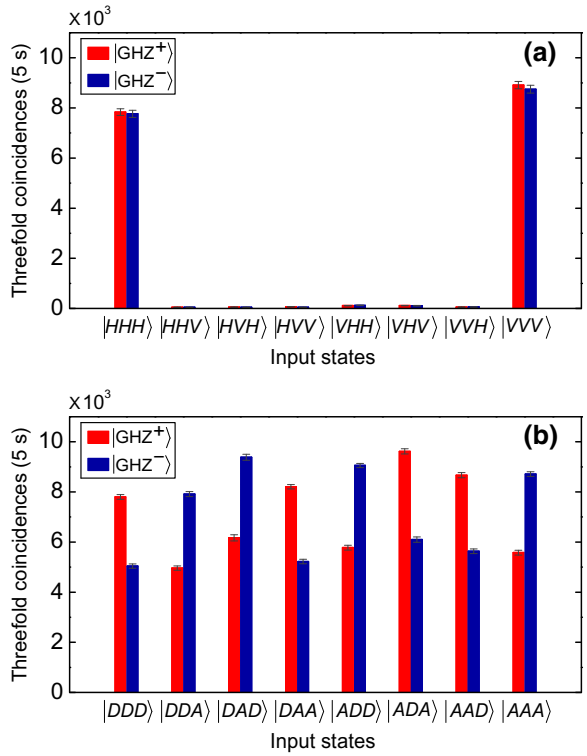

FIG. 4. The GHZ state measurement results with various input states of the (a) Z basis and (b) X basis. For Z-basis inputs, only the $|HHH\rangle$ and $|VVV\rangle$ inputs provide the GHZ state measurement outputs. On the other hand, all the X-basis inputs give biased $|\mathrm{GHZ}^{\pm}\rangle$. The experimentally obtained QBER for the Z and X bases are $Q_Z = (2.56 \pm 0.32)\%$ and $Q_X = (39.1 \pm 0.34)\%$, respectively.

inputs, only the $|HHH\rangle$ and $|VVV\rangle$ inputs are registered as $|\mathrm{GHZ}^{\pm}\rangle$, while all other input states do not provide threefold coincidences. The QBER

$$Q_Z = 1 - \frac{N_{HHH} + N_{VVV}}{\sum_{i,j,k=H,V} N_{ijk}},$$

where N_{ijk} denotes the GHZ measurement output count with $|ijk\rangle$ input, is measured as $Q_Z = (2.56 \pm 0.32)\%$. In Fig. 4(b) we show the GHZ state measurement results with X-basis input states. As theoretically expected, the inputs $|DDD\rangle$, $|DAA\rangle$, $|ADA\rangle$, and $|AAD\rangle$ provide the biased result towards $|\mathrm{GHZ}^{+}\rangle$, while the other states are biased to $|\mathrm{GHZ}^{-}\rangle$. The nonzero erroneous measurement results come from using weak coherent pulses instead of single-photon inputs. The average QBER in the X basis is $Q_X = (39.1 \pm 0.34)\%$. Here, the QBER is calculated as $Q_X = N_-/(N_+ + N_-)$ for $|DDD\rangle$, $|DAA\rangle$, $|ADA\rangle$, and $|AAD\rangle$ inputs and $Q_X = N_+/(N_+ + N_-)$ for the other inputs, where $N_\pm$ refers to the number of $|\mathrm{GHZ}^{\pm}\rangle$ measurement outcomes. Note that the experimentally obtained Q_X is about 2% higher than its theoretical value of $Q_X = 37.5\%$ with weak coherent pulse inputs [21].

IV. CONCLUSION

In multiparty cryptographic communication, all communication parties should have the same amount of information. Similarly, information balance is essential for multiparty quantum communication. Here, we show that exclusive possession of the GHZ state measurement in multiparty quantum communication by one party causes information imbalance among the communication parties. In order to guarantee information balance in multiparty quantum communication, we propose equitable multiparty quantum communication based on the GHZ state measurement that is symmetrically shared by all communication parties. We also verify the feasibility and practicality of the scheme by performing the proof-of-principle experiment using weak coherent pulses.

ACKNOWLEDGMENT

The authors thank Y. Shin for experimental assistance. This work is supported by the National Research Foundation of Korea (Grants No. 2019M3E4A1079777, No. 2019R1A2C2006381, and No. 2019M3E4A107866011), MSIT/IITP (Grants No. 2020-0-00972, and 2020-0-00947), and a KIST research program (Grant No. 2E30620).

Tanumoy Pramanik and Donghwa Lee contributed equally to this work.

APPENDIX A: EQUITABLE MULTIPARTY QUANTUM COMMUNICATION WITH IMBALANCED CHANNEL LOSSES

In the main text, we have assumed that all probability amplitude exchange transformations, Eqs. (3) and (4), have no losses, or, equivalently, have identical losses. In a real-world implementation, each transformation can have different losses, and can be represented in the more general forms

$$\begin{aligned} &a_{2H}^\dagger \to \xi_1 e^{i\theta_1} a_{3H}^\dagger, \quad b_{2H}^\dagger \to \xi_2 e^{i\theta_2} b_{3H}^\dagger, \quad c_{2H}^\dagger \to \xi_3 e^{i\theta_3} c_{3H}^\dagger, \\ &a_{2V}^\dagger \to \eta_1 e^{i\phi_1} b_{3V}^\dagger, \quad b_{2V}^\dagger \to \eta_2 e^{i\phi_2} c_{3V}^\dagger, \quad c_{2V}^\dagger \to \eta_3 e^{i\phi_3} a_{3V}^\dagger, \end{aligned} \tag{A1}$$

where $0 \le \xi_i, \eta_i \le 1$ $(i \in \{1,2,3\})$ are the efficiencies of the individual transformations. After the PBS2, the GHZ input states become

$$|\mathrm{GHZ}^{\pm}\rangle \to \frac{1}{\sqrt{\xi^2 + \eta^2}} (\xi a_{4H}^\dagger b_{4H}^\dagger c_{4H}^\dagger \pm \eta e^{i\Phi} a_{4V}^\dagger b_{4V}^\dagger c_{4V}^\dagger)|0\rangle, \tag{A2}$$

where $\xi = \xi_1\xi_2\xi_3$ and $\eta = \eta_1\eta_2\eta_3$. In equitable quantum communication, ξ and η are the transmission efficiencies of kept and sent probability amplitudes, respectively. The HWP at 22.5° transforms the states as, with $\Phi = 0$,

$$|\mathrm{GHZ}^{\pm}\rangle \rightarrow \frac{1}{2\sqrt{2(\xi^2+\eta^2)}}\left\{(\xi\pm\eta)\left(a_{4H}^{\dagger}b_{4H}^{\dagger}c_{4H}^{\dagger}+a_{4H}^{\dagger}b_{4V}^{\dagger}c_{4V}^{\dagger}+a_{4V}^{\dagger}b_{4H}^{\dagger}c_{4V}^{\dagger}+a_{4V}^{\dagger}b_{4V}^{\dagger}c_{4H}^{\dagger}\right)\right.$$
$$\left.+(\xi\mp\eta)\left(a_{4H}^{\dagger}b_{4H}^{\dagger}c_{4V}^{\dagger}+a_{4H}^{\dagger}b_{4V}^{\dagger}c_{4H}^{\dagger}+a_{4V}^{\dagger}b_{4H}^{\dagger}c_{4H}^{\dagger}+a_{4V}^{\dagger}b_{4V}^{\dagger}c_{4V}^{\dagger}\right)\right\}|0\rangle. \quad \text{(A3)}$$

Equation (A3) implies that the $|\mathrm{GHZ}^{+}\rangle$ and $|\mathrm{GHZ}^{-}\rangle$ states cannot be distinguished by means of threefold coincidences unless $\xi=\eta$. Therefore, in equitable multiparty quantum communication, the overall transmission efficiency between kept and sent probability amplitudes should be balanced, i.e., $\xi=\eta$. Note, however, that the individual transformation efficiencies of ξ_j and η_j do not have to be identical.

The simplest way to balance the transmission efficiencies is to introduce additional losses on the kept probability amplitudes with DLs of the same length as the QCs. Note that the DLs belong to the communication parties and do not cause additional losses since a single photon effectively travels along either the QC or DL, similar to the dual rail encoding in MDI QKD [27]. The transmission efficiency imbalance between QCs and DLs can be compensated at the state preparation stage.

In equitable multiparty quantum communication, secret key generation in the Z basis does not require distinguishing the $|\mathrm{GHZ}^{+}\rangle$ and $|\mathrm{GHZ}^{-}\rangle$ states, and, thus, the quantum communication protocol can be performed without modification in the Z basis despite the transmission efficiency imbalance. On the other hand, it is necessary to distinguish the $|\mathrm{GHZ}^{+}\rangle$ and $|\mathrm{GHZ}^{-}\rangle$ states to generate secret keys in the X basis. In order to compensate the transmission efficiency imbalance, the transmitters can prepare biased X-basis states as $|\widetilde{\pm}\rangle_i=|\widetilde{D}/\widetilde{A}\rangle_i=(\eta_i|H\rangle\pm\xi_i|V\rangle)/(\sqrt{\xi_i^2+\eta_i^2})$ instead of the ordinary states $|\pm\rangle=|D/A\rangle=(|H\rangle+|V\rangle)/\sqrt{2}$. The imbalances in the probability amplitudes of biased states and the transmission efficiency are canceled out, and, thus, the overall system works as if the transmitters transmit $|D/A\rangle$ states via balanced transmission efficiency channels. Meanwhile, Eq. (A3) shows that any eavesdropping attempt to alter the quantum channel transmission efficiency can be captured by increasing the QBER in the X basis.

It is worth remarking on the expected key generation rate in a lossy quantum channel. Equitable quantum communication requires threefold coincidence counts while injecting weak coherent pulses with a low-mean photon number. We note, however, that it can provide a reasonable amount of keys in a realistic situation. For instance, taking the mean photon number per pulse $\mu=0.5$ and the system efficiency $\eta_{\mathrm{sys}}=0.5$ (which are typical values in quantum communication), and 50 km of three quantum channels (10 dB loss for each quantum channel), the threefold coincidence probability is given as $P_3\sim 10^{-4}$. Considering the key sifting efficiency of $p=\frac{1}{4}$, one can expect more than 1000 sifted keys per second with 100 MHz of laser pulse repetition rate.

APPENDIX B: A PROPOSED EXPERIMENTAL SETUP TO STABILIZE POLARIZATION AND PHASE

The implementation of equitable multiparty quantum communication requires polarization and phase stabilization as well as temporal synchronization among the communication parties. These technical demands are similar to those of the recently proposed and implemented TF QKD [7,11]. Note that the phase stabilization of a large interferometer with an arm length of a few hundred kilometers has been implemented in the context of TF QKD [11]. In this section, based on this technique, we present a practical setup to stabilize polarization and phase and achieve temporal synchronization.

In Fig. 5 we show the proposed setup for equitable multiparty quantum communication. Each communication party utilizes two lasers with different wavelengths (LD1 and LD2). LD1 and LD2 are used for quantum communication and polarization and phase stabilization, respectively. Two laser pulses from LD1 and LD2 can be combined and split by wavelength division multiplexers, so one can make them take the same optical channel without loss.

Let us first present how Alice performs polarization and phase stabilization. She transmits the laser pulses from LD2 with polarization state $|D\rangle$. Then, they are split by a polarizing beamsplitter, and the horizontal and vertical polarization states are kept and sent to the next party (Bob), respectively. The horizontal and vertical polarization states acquire phases of θ_i and ϕ_i during the transmission via a delay line (DL1) and a quantum channel (QC1), respectively. The polarization drift during the transmission via QC1 can be monitored and mitigated by a feedback system at Bob using a photodiode and a polarization controller. The laser pulses are reflected by mirrors and sent back to Alice. During the reverse propagation, the phases θ_i and ϕ_i are acquired for the horizontal and vertical polarization states. Two laser pulses are combined by a PBS, and the polarization state becomes $|\psi\rangle=(|H\rangle+e^{i(2\phi_1-2\theta_1)}|V\rangle)/\sqrt{2}$ since the whole traveling of the

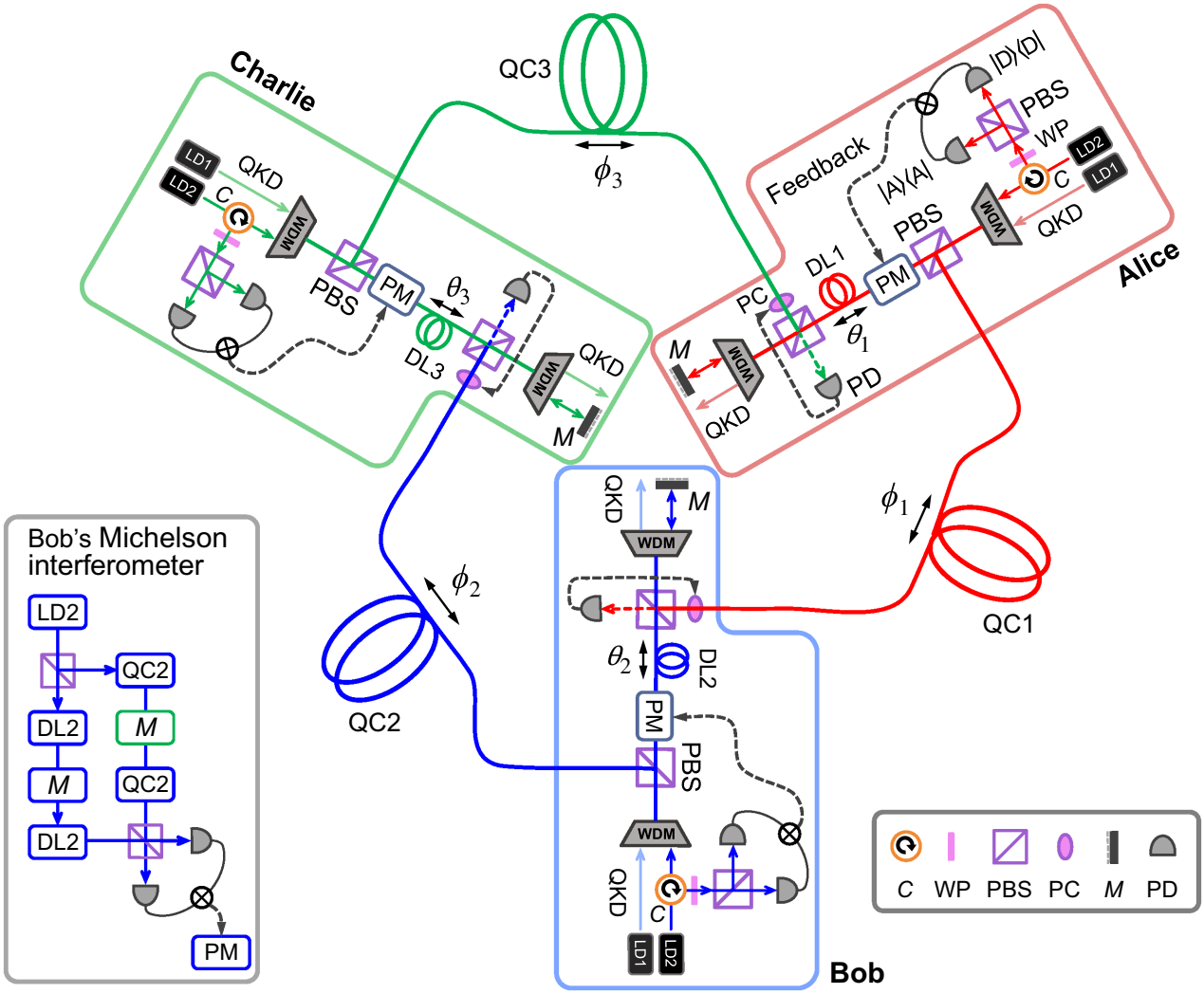

FIG. 5. A proposed experimental setup to stabilize polarization and phase. Two laser diodes (LD1 and LD2) are utilized for the quantum communication and stabilization system. As shown in the inset, each communication party can stabilize the phase by forming a Michelson interferometer with the arms of QCs and DLs; see the text for details. Here C is the circulator, WDM is the wavelength division multiplexer, PM is the phase modulator, PD is the photodiode, PC is the polarization controller, and M is the mirror.

laser pulses corresponds to a Michelson interferometer with arms QC1 and DL1. Here, we assume that the transmission efficiencies of the delay line and quantum channel are identical. Therefore, one can monitor and stabilize the phase difference between DL1 and QC1 by measuring the polarization state of LD2 pulses and the feedback system with a phase modulator. Bob and Charlie can employ the same system, then they can stabilize the overall phase, i.e., $\Phi = \Sigma_j (\phi_j - \theta_j)$ becomes constant. Note that the optical delay drift (which is much slower than that of the phase) can also be monitored with the purity of the polarization state and compensated with a variable optical delay (not shown in Fig. 5).

Note that the wavelength mismatch between LD1 and LD2 can cause a stabilization system error. This error can be mitigated by utilizing the same lasers with different timings for system stabilization and quantum communication. Note that Wang *et al.* [11] successfully demonstrated TF QKD with a few hundred kilometers of quantum channel using this time-multiplexing technique.

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, Piscataway, 1984), p. 175.
[2] A. Ekert, Quantum Cryptography Based on Bell's Theorem, Phys. Rev. Lett. **67**, 661 (1991).
[3] S. L. Braunstein and S. Pirandola, Side-Channel Free Quantum key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).
[4] H. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[5] Y. Choi, O. Kwon, M. Woo, K. Oh, S.-W. Han, Y.-S. Kim, and S. Moon, Plug-and-play measurement-device-independent quantum key distribution, Phys. Rev. A **93**, 032319 (2016).

[6] C. H. Park, B. K. Park, M. S. Lee, Y.-S. Kim, Y.-W. Cho, S. Kim, S.-W. Han, and S. Moon, Practical plug-and-play measurement-device- independent quantum key distribution with polarization division multiplexing, IEEE Access **6**, 58587 (2018).

[7] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate?distance limit of quantum key distribution without quantum repeaters, Nature **557**, 400 (2018).

[8] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, Nat. Photon. **13**, 334 (2019).

[9] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, J. Lin, T.-Y. Chen, L. You, Z. Wang, X.-B. Wang, Q. Zhang, and J.-W. Pan, Experimental Twin-Field Quantum Key Distribution Through Sending-Or-Not-Sending, Phys. Rev. Lett. **123**, 100505 (2019).

[10] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Proof-Of-Principle Experimental Demonstration of Twin-Field Type Quantum key Distribution, Phys. Rev. Lett. **123**, 100506 (2019).

[11] S. Wang, D.-Y. He, Z.-Q. Yin, F.-Y. Lu, C.-H. Cui, W. Chen, Z. Zhou, G.-C. Guo, and Z.-F. Han, Beating the Fundamental Rate-Distance Limit in a Proof-Of-Principle Quantum key Distribution System, Phys. Rev. X **9**, 021046 (2019).

[12] S. Bose, V. Vedral, and P. L. Knight, Multiparticle generalization of entanglement swapping, Phys. Rev. A **57**, 822 (1998).

[13] K. Chen and H.-K. Lo, Multi-partite quantum cryptographic protocols with noisy GHZ states, Quantum Inf. Comput. **7**, 689 (2007).

[14] M. Hillery, V. Bužek, and A. Berthiaume, Quantum secret sharing, Phys. Rev. A **59**, 1829 (1999).

[15] R. Cleve, D. Gottesman, and H.-K. Lo, How to Share a Quantum Secret, Phys. Rev. Lett. **83**, 648 (1999).

[16] B. Bell, D. Markham, D. A. Herrera-Marti, A. Marin, W. J. Wadsworth, J. G. Rarity, and M. S. Tame, Experimental demonstration of graph-state quantum secret sharing, Nat. Commun. **5**, 5480 (2014).

[17] W. Tittel, H. Zbinden, and N. Gisin, Experimental demonstration of quantum secret sharing, Phys. Rev. A **63**, 042301 (2001).

[18] Y.-A. Chen, A.-N. Zhang, Z. Z. X.-Q. Zhou, C.-Y. Lu, C.-Z. Peng, T. Yang, and J.-W. Pan, Experimental Quantum Secret Sharing and Third-Man Quantum Cryptography, Phys. Rev. Lett. **95**, 200502 (2005).

[19] S. Gaertner, C. Kurtsiefer, M. Bourennane, and H. Weinfurter, Experimental Demonstration of Four-Party Quantum Secret Sharing, Phys. Rev. Lett. **97**, 020503 (2007).

[20] C. Erven, E. Meyer-Scott, K. Fisher, J. Lavoie, B. L. Higgins, Z. Yan, C. J. Pugh, J.-P. Bourgoin, R. Prevedel, L. K. Shalm, L. Richards, N. Gigov, R. Laflamme, G. Weihs, T. Jennewein, and K. J. Resch, Experimental three-photon quantum nonlocality under strict locality conditions, Nat. Photonics **8**, 292 (2014).

[21] Y. Fu, H.-L. Yin, T.-Y. Chen, and Z.-B. Chen, Long-Distance Measurement-Device-Independent Multiparty Quantum Communication, Phys. Rev. Lett. **114**, 090501 (2015).

[22] W.-Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).

[23] A. Shamir, How to share a secret, Comm. ACM **22**, 612 (1979).

[24] W. Mao, *Modern Cryptography* (Prentice Hall PTR, Upper Saddle River, New Jersey, 2004).

[25] R. Horodecki, P. Horodecki, M. Horodecki, and K. Horodecki, Quantum entanglement, Rev. Mod. Phys. **81**, 865 (2008).

[26] J.-W. Pan and A. Zeilinger, Greenberger-horne-zeilinger-state analyzer, Phys. Rev. A **57**, 2208 (1998).

[27] X. Ma and M. Ravavi, Alternative schemes for measurement-device-independent quantum key distribution, Phys. Rev. A **86**, 062319 (2012).

[28] X. Ma and N. Lütkenhaus, Improved data post-processing in quantum key distribution and application to loss thresholds in device independent QKD, Quantum Inf. Comput. **12**, 0203 (2012).

[29] T. B. Pittman, D. V. Strekalov, A. Migdall, M. H. Rubin, A. V. Sergienko, and Y. H. Shih, Can Two-Photon Interference be Considered the Interference of Two Photons?, Phys. Rev. Lett. **77**, 1917 (1996).

[30] Y.-S. Kim, O. Slattery, P. S. Kuo, and X. Tang, Conditions for two-photon interference with coherent pulses, Phys. Rev. A **87**, 063843 (2013).

[31] Y.-S. Kim, O. Slattery, P. S. Kuo, and X. Tang, Two-photon interference with continuous-wave multi-mode coherent light, Opt. Express **22**, 3611 (2014).

[32] Y.-S. Kim, T. Pramanik, Y.-W. Cho, M. Yang, S.-W. Han, S.-Y. Lee, M.-S. Kang, and S. Moon, nformationally symmetrical bell state preparation and measurement, Opt. Express **26**, 29539 (2018).

[33] M. R. Barros, S. Chin, T. Pramanik, H.-T. Lim, Y.-W. Cho, J. Huh, and Y.-S. Kim, Entangling bosons through particle indistinguishability and spatial overlap, Opt. Express **28**, 38083 (2020).

[34] L. Lydersen, C. Wiechers, C. Wittmann, D. Elser, J. Skaar, and V. Makarov, Hacking commercial quantum cryptography systems by tailored bright illumination, Nat. Photon. **4**, 686 (2010).

[35] S. Sajeed, A. Huang, S. Sun, F. Xu, V. Makarov, and M. Curty, Insecurity of Detector-Device-Independent Quantum key Distribution, Phys. Rev. Lett. **117**, 250505 (2016).

[36] Y. Choi, K.-H. Hong, H.-T. Lim, J. Yune, O. Kwon, S.-W. Han, K. Oh, Y.-H. Kim, Y.-S. Kim, and S. Moon, Generation of a non-zero discord bipartite state with classical second-order interference, Opt. Express **25**, 2540 (2017).

[37] J. Yoon, T. Pramanik, B. K. Park, S.-W. Han, S. Kim, Y.-S. Kim, and S. Moon, Experimental comparison of various quantum key distribution protocols under reference frame rotation and fluctuation, Opt. Comm. **441**, 64 (2019).