Phase-Matching Quantum Cryptographic Conferencing

Shuai Zhao,[1,2] Pei Zeng,[3] Wen-Fei Cao,[1,2] Xin-Yu Xu,[1,2] Yi-Zheng Zhen,[4,1,2] Xiongfeng Ma,[3,*]
Li Li,[1,2,†] 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 Anhui, People's Republic of China*
[2] *CAS Center for Excellence and Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, 230026 Anhui, People's Republic of China*
[3] *Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, 100084 Beijing, People's Republic of China*
[4] *Institute for Quantum Science and Engineering, Southern University of Science and Technology, Shenzhen, 518055 Guangdong, People's Republic of China*

(Received 2 December 2019; revised 28 April 2020; accepted 25 June 2020; published 5 August 2020)

Quantum cryptographic conferencing (QCC) holds promise for distributing information-theoretic secure keys among multiple users over a long distance. Limited by the fragility of Greenberger-Horne-Zeilinger (GHZ) states, QCC networks based on directly distributing GHZ states over a long distance still face a big challenge. Another two potential approaches are measurement device-independent QCC and conference-key agreement with single-photon interference, which were proposed on the basis of the postselection of GHZ states and the postselection of the W state, respectively. However, implementations of the former protocol are still heavily constrained by the transmission rate η of optical channels and the complexity of the setups for postselecting GHZ states. Meanwhile, the latter protocol cannot be cast as a measurement device-independent prepare-and-measure scheme. Combining the idea of postselecting GHZ states and recently proposed twin-field quantum-key-distribution protocols, we report a QCC protocol based on weak coherent-state interferences named "phase-matching quantum cryptographic conferencing," which is immune to all detector side-channel attacks. The proposed protocol can improve the key-generation rate from $O(\eta^N)$ to $O(\eta^{N-1})$ compared with the measurement device-independent QCC protocols. Meanwhile, it can be easily scaled up to multiple parties due to its simple setup.

DOI: 10.1103/PhysRevApplied.14.024010

I. INTRODUCTION

Quantum networks [1–10], aimed at realizing quantum-information tasks among multiple parties, are playing more and more important roles in burgeoning quantum-information processing, including quantum computing [11], quantum communication [12], and quantum metrology [13]. A quantum-cryptographic-conferencing (QCC) network [14–19], which distributes information-theoretic secure keys among multiple parties over a long distance, is one of the most-promising applications in quantum-information science. With the rapid development of quantum-information processing, a QCC network has great potential to improve the security of the communications in networks. For example, a QCC network can be used to broadcast a message to users securely. So far, several protocols have been proposed to realize QCC networks. The first protocol is based on the predistribution of multiparty entanglement states [14–16]. These presentations require the predistribution of a Greenberger-Horne-Zeilinger (GHZ) entanglement state [20], which was initially introduced to verify Bell's theorem [21,22]. Although great endeavors have been made to improve preparation of multiparty GHZ states [23–28], the low intensity and fragility of the GHZ states make their application to a practical QCC network a big challenge with current technology. The second protocol is measurement device-independent (MDI) QCC, which is based on the postselection of a GHZ state [17]. Once a successful detection event occurs, a GHZ state is shared among multiple parties [29]. Thus, multiple parties can distribute secret-key bits among themselves by the postselected entanglement states. Furthermore, the measurement device can be controlled by an untrusted third party, Eve. Therefore, according to the MDI-quantum-key-distribution (QKD) idea [30] (see also Ref. [31]), it is immune to all detector side-channel attacks. Combined

[*] xma@tsinghua.edu.cn
[†] eidos@ustc.edu.cn
[‡] nlliu@ustc.edu.cn
[§] kaichen@ustc.edu.cn

with the decoy-state method [32], a MDI-QCC network is more likely to be realized in experiments with current technology. The third protocol is the conference-key agreement with single-photon interference (single-photon CKA) [18], which is based on postselection of the W state [33]. However, the single-photon-CKA protocol cannot be cast as a MDI prepare-and-measure scheme. Meanwhile, the signal pulses cannot be substituted by coherent states, and the local qubits have to resort to quantum memories. Thus, the feasibility of single-photon CKA requires further investigation [18].

Recently, twin-field (TF) QKD and phase-matching (PM) QKD [34–43] were reported to overcome the repeaterless rate-distance limit [44] of QKD. By introducing single-photon interference, these protocols achieve key-generation rates scaling with the square root of the channel transmittance $O(\sqrt{\eta})$, which exceeds the rate-distance limit without quantum repeaters. Here η is the transmission rate of the optical channel between two users. At the same time, their measurement device can be controlled by an untrusted third party, which is also immune to all detector side-channel attacks [30]. These types of QKD protocols have also been realized [45–49] and shown to extend the distance of repeaterless fiber QKD to more than 500 km [49].

In this paper, we present a QCC-network protocol by combining the ideas of phase-matching weak-coherent-pulse (WCP) interference and postselecting GHZ states, named “phase-matching quantum cryptographic conferencing (PM QCC).” As shown in Appendixes A and B, successful WCP-interference events imply successful postselection of multiparty GHZ states within the GHZ-state basis:

$$|\psi_{j,i_1i_2\cdots i_{N-1}}\rangle = \frac{1}{\sqrt{2}}[|0i_1i_2\cdots i_{N-1}\rangle + (-1)^j|1\bar{i}_1\bar{i}_2\cdots\bar{i}_{N-1}\rangle], \quad (1)$$

where j $(i_m) \in \{0,1\}$ is called the “phase (amplitude) bit,” $1 \le m \le N-1$, and $\bar{i}_m$ is the logical negation of i_m. With use of the entanglement-distillation protocol [50], one can distill the perfect N-qubit GHZ state:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\cdots 0\rangle + |11\cdots 1\rangle)_N, \quad (2)$$

which can be used to generate secret-key bits among N parties.

In terms of the PM-QCC network presented, since the measurement device can be untrusted, it is immune to all detector side-channel attacks. Owing to its simpler setup structure compared with MDI-QCC networks based on a GHZ analyzer [29,51], one can extend PM QCC to more users easily. Similarly to the TF-QKD protocol, the key-generation rate of the PM-QCC network presented can be improved to scale with η^{N-1}, whereas that of the MDI-QCC network scales with η^N. Here η is the transmission rate of the optical channel from each party to the untrusted third party, Eve. Practically, there might be small-scale interference between N' parties (N' parties are near-neighbor connected, and $2 \le N' \le N$) instead of perfect interference of N parties. It is demonstrated that the small-scale N'-party PM QCC can still be realized securely with key-generation rates scaling with $\eta^{N'-1}$.

II. PM-QCC NETWORK

Suppose that N parties $P_1, P_2, \ldots, P_N$ plan to conduct a quantum-cryptographic-conferencing task, see Fig. 1. They can encode their random bits in their phase-randomized coherent pulses. The encoded coherent pulses are sent to the untrusted third party, Eve, who is supposed to perform interference measurements. The N-party PM-QCC network works as follows:

Step 1. Preparation. Party P_1 randomly generates one bit $k_1 \in \{0,1\}$ and one coherent pulse with a random phase $\phi_1 \in [0, 2\pi)$. Then, he encodes the random bit in the coherent pulse and gets a phase-randomized coherent pulse $|e^{i(\phi_1+\pi k_1)}\sqrt{\mu_1}\rangle$. Similarly, parties $P_2, \ldots, P_N$ prepare their phase-randomized coherent pulses $|e^{i(\phi_2+\pi k_2)}\sqrt{\mu_2}\rangle, \ldots, |e^{i(\phi_N+\pi k_N)}\sqrt{\mu_N}\rangle$, respectively.

As shown in Fig. 1, the settings for P_1 and P_N are different from those for $P_2, \ldots, P_{N-1}$ in the experimental setup. Thus, the intensities of the weak coherent pulses used by parties P_1 and P_N are set to be μ_1 and $\mu_N \in \{\mu/2 > \nu/2 > \omega/2 > \tau/2 > \cdots > 0\}$, while the intensities for parties $P_2, \ldots, P_{N-1}$ are set to be $\mu_t \in \{\mu > \nu > \omega > \tau > \cdots > 0\}$ $(2 \le t \le N-1)$. The pulses with intensity μ are used as signal pulses and the pulses with intensities $\{\nu, \omega, \tau, \ldots, 0\}$ are used as decoy pulses.

Step 2. Measurement. All the parties send their pulses directly to the untrusted third party, Eve. By design, an honest Eve splits each pulse of parties $P_2, \ldots, P_{N-1}$ into two separated coherent pulses using 50:50 beam splitters (BS1 in Fig. 1) to perform interference measurements as shown in Fig. 1. Eve measures the received pulses and records the measurement results. Here successful detection events are defined as coincidence clicks of $N-1$ measurement branches, within which only one detector clicks.

Step 3. Announcement. Eve announces measurement results for successful detection events. Then, all the parties announce their random phases $\phi_1, \phi_2, \ldots, \phi_N$ and their randomly chosen intensities $\mu_1, \mu_2, \ldots, \mu_N$, respectively.

Step 4. Sifting. When a successful detection event is announced by Eve, the N parties P_1, $P_2, \ldots, P_N$

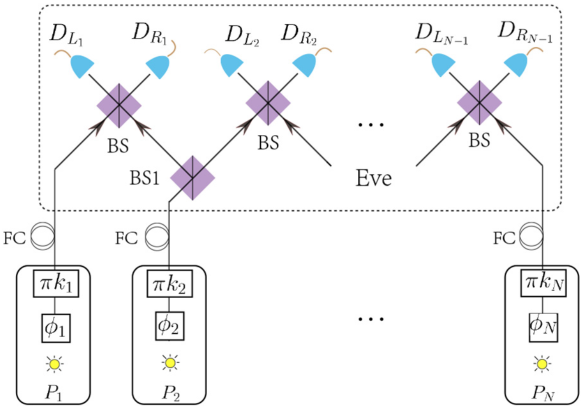

FIG. 1. Setup for a N-party PM-QCC network. ϕ_1, ϕ_2, and $\phi_N \in [0, 2\pi)$ label the random phases for parties P_1, P_2, and P_N, respectively. k_1, k_2, and $k_N \in \{0, 1\}$ label the random bits for parties P_1, P_2, and P_N, respectively. D_{L_1} (D_{R_1}) is the left (right) detector of the first measurement branch. D_{L_2} (D_{R_2}) is left (right) detector of the second measurement branch. $D_{L_{N-1}}$ ($D_{R_{N-1}}$) is the left (right) detector of the $(N-1)$th measurement branch. BS, beam splitter; FC, fiber channel.

keep their random bits $k_1, k_2, \ldots, k_N$, respectively. A successful detection event is one of 2^{N-1} coincident click events in the set $\{D_{L_1}D_{L_2}\cdots D_{L_{N-1}}, D_{R_1}D_{L_2}\cdots D_{L_{N-1}}, \ldots, D_{R_1}D_{R_2}\cdots D_{R_{N-1}}\}$. Here D_{L_l} [$D_{(R_l)}$] means that only the detector D_{L_l} (D_{R_l}) clicks in the lth measurement branch. According to Eve's announcements, they cooperate to flip theirs bits to make their encoded phases the same as those of the events $D_{L_1}D_{L_2}\cdots D_{L_{N-1}}$. Then, $P_1, P_2, \ldots, P_N$ keep their random bits only when the phase-matching conditions are satisfied: $|\phi_1 - \phi_2| = 0$ or π, $|\phi_2 - \phi_3| = 0$ or $\pi, \ldots, |\phi_{N-1} - \phi_N| = 0$ or π and their intensities are $2\mu_1 = \mu_t = 2\mu_N$ $(2 \leq t \leq N-1)$. Then, according to their phase announcements, they cooperate to flip their retained random bits to be the same as those of $|\phi_1 - \phi_2| = 0$, $|\phi_2 - \phi_3| = 0, \ldots, |\phi_{N-1} - \phi_N| = 0$ if this is not the case.

Step 5. Parameter estimation and key distillation. The above steps are repeated enough times to distill the raw-key bits. From the data set generated by the signal pulses, the users can directly estimate the gain Q_μ and marginal quantum bit error rates (QBERs) $E^Z_{\mu,P_1P_2}, E^Z_{\mu,P_1P_3}, \ldots, E^Z_{\mu,P_1P_N}$ from the measurement results. From the data set generated by the decoy pulses, the users can estimate the phase error E^X_μ according to decoy-state methods (see Appendix D for details). Finally, they distill private key bits by performing error correction and privacy amplification on the raw key.

For the coherent-pulse interference measurement on the lth $(1 \leq l \leq N-1)$ measurement branch, there would be only one detector click if the encoded phases of two pulses with equal intensities are matched; that is, D_{L_l} (or D_{R_l}) would click if $\Delta\phi_l = |\phi_l + \pi k_l - (\phi_{l+1} + \pi k_{l+1})| = 0$ (or π). This is vital in the security of the PM-QCC network.

In the N-party PM-QCC network described above, the random phases $\phi_1, \phi_2, \ldots, \phi_N$ that $P_1, P_2, \ldots, P_N$ attach to their pulses are continuous. Thus, the precise phase-matching condition $|\phi_m - \phi_{m+1}| = 0$ or π is hard to realize. Moreover, we suppose that the lasers of P_1, $P_2, \ldots, P_N$ are perfectly locked, which is also impractical in experiments. To overcome these problems, we introduce the phase-compensation method [34,35] that can help to conduct phase matching and phase reference. For an arbitrary party P_m, the phase interval $[0, 2\pi)$ is cut into M slices $\{\Delta_{j_m}\}$, with $0 \leq j_m \leq M-1$, $\Delta_{j_m} = [(2\pi/M)j_m, (2\pi/M)(j_m+1)]$. In the announcement step, what N parties $P_1, P_2, \ldots, P_N$ announce are their phase-slice indexes $j_1, j_2, \ldots, j_N$ instead of their exact phases $\phi_1, \phi_2, \ldots, \phi_N$, respectively. Then, in the sifting step, parties P_m and P_{m+1} need to compare only their slices indexes, $|j_m + j^a_m - j_{m+1}| \mod M = 0$ or $M/2$, where $j^a_m \in \{0, 1, \ldots, M-1\}$ is an adjusted slice index to compensate for the deviation of phase reference for parties P_m and P_{m+1}. In practice, j^a_m can be determined in the parameter-estimation step by minimizing the QBER. Although there will be intrinsic misalignment errors in the sifting induced by the coarse split of the phase interval, this makes phase sifting practical without affecting the security [35].

III. SECURITY ANALYSIS

Without loss of generality, we consider an entanglement-based protocol whereby party P_m prepares entanglement states between his virtual qubits and his WCPs instead of directly preparing WCPs (see Appendix B for details). Thus, its security analysis applies to the entanglement-distillation argument [16,52,53]. Following the entanglement-distillation argument [52,53], to generate a sequence of almost perfect secure key bits, parties P_1, $P_2, \ldots, P_N$ need to share only a sequence of almost perfect GHZ states in terms of monogamy of entanglement [54,55]. Therefore, what we are facing now is to distill almost-perfect GHZ states [50].

As described in step 4, when the phase-matching condition is satisfied, encoded random bits are kept. Without loss of generality, the phases are supposed to be $\phi_1 = \phi_2 = \cdots = \phi$. In Fig. 2(a), the WCP with random phase ϕ of party P_2 arriving at the 50:50 beam splitter BS1 is split into two WCPs with the same encoded phases:

$$|e^{i(\phi+\pi k_2)}\sqrt{\mu}\rangle \xrightarrow{\text{BS1}} |e^{i(\phi+\pi k_2)}\sqrt{\mu/2}\rangle|e^{i(\phi+\pi k_2)}\sqrt{\mu/2}\rangle, \quad (3)$$

where $\phi + \pi k_2$ is the encoded phase of party P_2. The WCPs from party P_2 are split into two branches to interfere

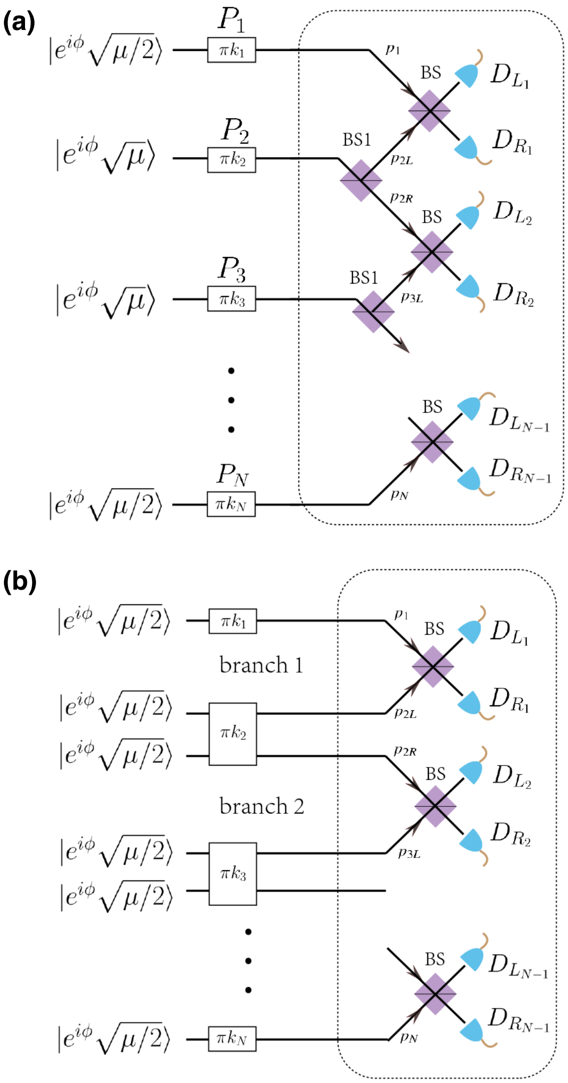

FIG. 2. (a) The PM-QCC protocol with phase-matching condition $\phi_1 = \phi_2 = \cdots = \phi_N = \phi$ satisfied. (b) Equivalent PM-QCC protocol after Eve's splitting with phase-matching condition $\phi_1 = \phi_2 = \cdots \phi_N = \phi$ satisfied. Eve splits each pulse of parties $P_2, \ldots, P_{N-1}$ into two separated coherent pulses using a beam splitter (BS1) to perform interference measurements. Once a successful detection event is achieved, the encoded phases of N parties are correlated with each other. $p_1, p_{2L}, \ldots, p_N$ are the path modes after Eve's splitting. D_{L_1} (D_{R_1}) is the left (right) detector of the first measurement branch. D_{L_2} (D_{R_2}) is the left (right) detector of the second measurement branch. $D_{L_{N-1}}$ ($D_{R_{N-1}}$) is the left (right) detector of the $(N-1)$th measurement branch.

with P_1 and P_3, respectively. Similarly, WCPs from parties $P_3, \ldots, P_{N-1}$ are split. The third party, Eve, performs interference measurement for all N parties. Now, the protocol is equivalent to that in Fig. 2(b).

Let us consider the entanglement-based protocol of PM QCC (see Appendix B). Once there is a successful detection event, virtual qubits in N parties are entangled together. After the distillation protocol (see Appendix A), perfect GHZ states are shared between N parties. Finally, they can generate secret-key bits from the distillation of the GHZ state [15–17]. The corresponding key-generation rate is

$$R_{N\text{-party}} = \left(\frac{2}{M}\right)^{N-1} Q_\mu\{1 - f \times \max[H(E^Z_{\mu,P_1P_2}), H(E^Z_{\mu,P_1P_3}), \ldots, H(E^Z_{\mu,P_1P_N})] - H(E^X_\mu)\}, \quad (4)$$

where $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function, E^Z_{μ,P_1P_m} $(2 \leq m \leq N)$ is the marginal QBER of parties P_1 and P_m and can be estimated from Eve's measurement results directly, E^X_μ is the phase error rate, which is an intrinsic error of the protocol and can be estimated with the help of the decoy-state method in experiments (see Appendixes C and D), Q_μ is the overall gain, and $\frac{2}{M}$ is induced by phase postselection in the phase-compensation method, which can be optimized according to the experimental parameters [34,35].

As shown in Eq. (4), there is a prefactor $(2/M)^{N-1}$ that is induced by the phase postselection process in the key-generation rate. It might cause a decrease in the key-generation rate when the number of user increases. According to Appendix B, the PM-QCC protocol is still secure even when the phase choices for the signal pulses are announced before Eve's measurement if one can estimate the phase error accurately. Thus, the phase-compensation method provides a practical and secure way to align the phases for signal pulses. Then, if one can realize an accurate and secure phase reference the laboratory, the PM-QCC protocol can be improved to a version PM-QCC* without phase postselection in signal pulses (see Appendix E for details). It has also been demonstrated in variants of the TF-QKD and PM-QKD protocols [37,38,41–43]. In the PM-QCC* protocol, the factor $(2/M)^{N-1}$ can be improved to 1, and the key-generation rate is

$$R^*_{N\text{-party}} = Q^*_\mu\{1 - f \times \max[H(E^{Z*}_{\mu,P_1P_2}), H(E^{Z*}_{\mu,P_1P_3}), \ldots, H(E^{Z*}_{\mu,P_1P_N})] - H(E^{X*}_\mu)\}. \quad (5)$$

where Q^*_μ is the overall gain, E^{Z*}_{μ,P_1P_2}, E^{Z*}_{μ,P_1P_2}, and E^{Z*}_{μ,P_1P_2} are marginal QBERs, and E^{X*}_μ is the phase error rate. The signal pulses from the parties can no longer be regarded as photon-number states since the phase randomization for signal pulses has been canceled out in the PM-QCC* protocol. Thus, the preceding discussion of decoy states for the PM-QCC protocol becomes unsuitable for the PM-QCC* protocol, and a more-delicate decoy-state method is required to evaluate the phase error rate for the signals (see Appendix E) [39,41,42]. For example, as in Ref. [41], the estimation of the phase error rate is converted to the estimation of the yields for the photon-number state, which can be estimated using phase-randomized decoy states. Thus, the phase-randomized decoy states with different intensities can, in principle, be used to constrain the phase error rate E_{μ}^{X} tightly, and we leave this for further studies.

IV. PERFORMANCE OF THE PM-QCC NETWORK

Without loss of generality, the channels between party P_m and the measurement station are supposed to be symmetric. To show the performance of the PM-QCC network, we consider the three-party PM-QCC network and the three-party PM-QCC* network and compare these two protocols with the MDI-QCC network [17] using the following experimental parameters: intrinsic fiber-channel loss $\alpha = 0.2$ dB/km, detection efficiency of the threshold single-photon detector $\eta_d = 93\%$, dark-count rate $p_d = 10^{-7}$, error-correction efficiency $f = 1.16$, misalignment error for MDI QCC $e_d^{\text{MDI}} = 1.5\%$, and phase error for PM QCC* $e_\delta^{\text{PM QCC*}} = 1.5\%$. As shown in Fig. 3, one can see that the key-generation rate of the PM-QCC network is much greater than that of the MDI-QCC network around $L = 80$ km. The key-generation rate is increased by approximately 2 orders of magnitude around $L = 200$ km. For the PM-QCC* network without the phase-matching condition in signal pulses, the key-generation rate greatly exceeds that of the MDI-QCC network around $L = 12$ km. This increase is mainly because the key-generation rate of the PM-QCC network can be improved to scale with η^{N-1}, whereas that of the MDI-QCC network scales with η^N (see Appendix F).

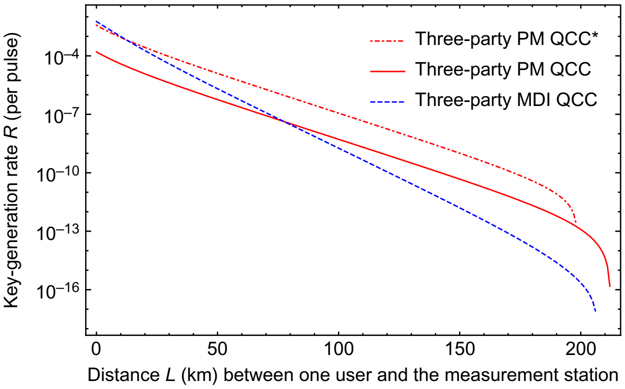

FIG. 3. Key-generation rate R of three-party PM-QCC, three-party PM-QCC* (without phase postselection in signal pulses), and three party MDI-QCC networks versus transmission distance L. The simulation results are obtained with parameters from Ref. [17]: dark-count rate $p_d = 1 \times 10^{-7}$, loss rate of the channel $\alpha = 0.2$ dB/km, detection efficiency $\eta_d = 93\%$, error-correction efficiency $f = 1.16$, misalignment error for MDI QCC $e_d^{\text{MDI}} = 1.5\%$, and phase misalignment error for PM QCC* $e_\delta = 1.5\%$. The number of phase slices M for PM QCC is optimized at different transmission distances.

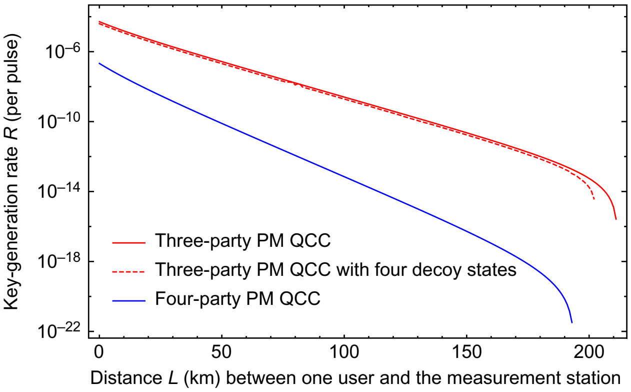

FIG. 4. Key-generation rate R for three-party PM QCC, three-party PM QCC with four decoy states (ν, ω, τ, and 0), and four-party PM QCC versus transmission distance L. Parameters used in the simulation are obtained from Ref. [56]: dark-count rate $p_d = 7.2 \times 10^{-8}$, loss rate of the channel $\alpha = 0.2$ dB/km, detection efficiency $\eta_d = 65\%$, and error-correction efficiency $f = 1.16$.

To demonstrate the scalability and the decoy-state method of the PM-QCC network, we simulate the PM-QCC network for $N = 3$ parties with infinite decoy states and four decoy states ($\nu > \omega > \tau > 0$). With the experimental parameters given in Ref. [56] (detection efficiency $\eta_d = 65\%$ and dark-count rate $p_d = 7.2 \times 10^{-8}$), the performance of PM-QCC network for $N = 3$ parties is presented in Fig. 4. The longest transmission distance between one user and the measurement station of the PM-QCC network is more than 200 km for $N = 3$ parties. Remarkably, the longest transmission distance between two users is more than 400 km by special arrangement. The optimized weak coherent states μ and phase-slice numbers M for given parameters for $N = 3$ are presented in Table I. Meanwhile, the key-generation rate for the three-party PM-QCC network with four decoy states is optimized over μ, ν, ω, and τ for given parameters and $M = 13$. For example, the key-generation rate $R = 1.7327 \times 10^{-11}$ (bits per pulse) at $L = 150$ (km) with $\mu = 0.104815$, $\nu = 0.0204583$, $\omega = 0.0182017$, and $\tau = 9.27216 \times 10^{-5}$. Furthermore, we simulate the PM-QCC network for $N = 4$ parties; the simulation results are presented in Fig. 4.

According to the above discussion, it is feasible to realize the PM-QCC network for three and even more parties with current experimental technology. Meanwhile, the PM-QCC* network (without phase postselection in signal pulses) (see Appendix E) can be realized with further optimization and an accurate phase reference over a long distance.

Practically, there might be interferences of only N' parties (N' parties are near-neighbor connected, and $2 \leq N' \leq N$) instead of perfect interference of N parties. In this case, according to step 1 of the PM-QCC network, the

TABLE I. Performance of the PM-QCC network at $N = 3$. The key-generation rate R, mean photon number μ, and phase-slice number M are optimized with $p_d = 7.2 \times 10^{-8}$, $\eta_d = 65\%$, $f = 1.16$, and $\alpha = 0.2$ dB/km at different transmission distances L.

R (bits per pulse)	L (km)	μ	M
2.6989×10^{-7}	50	0.1333	13
1.6227×10^{-8}	80	0.1299	13
2.5332×10^{-9}	100	0.1291	13
2.2928×10^{-11}	150	0.1263	13
2.6206×10^{-14}	200	0.1239	17

weak coherent pulses prepared by parties at broken points are $|\sqrt{\mu}\rangle$ instead of $|\sqrt{\mu/2}\rangle$ (the encoded phase is omitted here). As shown in Fig. 1, the intensities of weak coherent pulses arriving at the third party are equal in an inference branch. Therefore, higher numbers of weak coherent pulses are lost during transmission for broken points compared with unbroken points. It is demonstrated that secure reduced small-scale PM-QCC networks can also be constructed among N' parties with key-generation rate $R_{\text{reduced PM QCC}} \propto \eta^{N'-1}$ (see Appendix G for detail).

V. CONCLUSION AND OUTLOOK

Based on multiparty weak-coherent-pulse interference, we present a protocol named a "phase-matching quantum cryptographic conferencing network" that can distribute information-theoretic secure keys among N parties. With the merit of a simple setup, the PM-QCC network can be conveniently generalized to N parties and can go beyond the existing QCC networks. Firstly, similarly to the MDI-QCC network, the PM-QCC network is immune to all detector side-channel attacks since the measurement device can be untrusted. Secondly, compared with the MDI-QCC networks based on a GHZ analyzer, the PM-QCC network can be more-easily extended to multiple users due to its simpler setup structure. Thirdly, the key-generation rate of the PM-QCC network can be improved to scale with η^{N-1}, whereas that of the MDI-QCC network scales with η^{N}. Fourthly, considering practical cases where there are small-scale interferences between N' parties instead of perfect interferences of N parties, the small-scale N'-party PM-QCC network can still be realized. Finally, on the basis of the setup of the PM-QCC network, GHZ-state distribution networks can be constructed directly, which may have great potential for other implementations in quantum-information science.

During the preparation of this paper, related work based on postselection of the W state [33] was reported [18], which is named "conference-key agreement with single-photon interference" (single-photon CKA). Compared with single-photon CKA, the proposed protocol is essentially a different protocol. Specifically, the proposed protocol is a MDI prepare-and-measure scheme, while the single-photon-CKA protocol cannot be cast as a MDI prepare-and-measure scheme, in which all parties have to measure their local qubits and trust the measurement results. Meanwhile, the signal qubits sent to the measurement station cannot be replaced by coherent states, and the local qubits have to resort to quantum memories in the single-photon-CKA protocol. Thus, the feasibility of the single-photon-CKA protocol requires further investigation [18].

ACKNOWLEDGMENTS

We acknowledge Feihu Xu for insightful discussion. This work was supported by the Chinese Academy of Science, the National Fundamental Research Program, the National Natural Science Foundation of China (Grants No. 11575174, No. 11374287, No. 11574297, No. 11875173, and No. 11674193), the National Key R&D Program of China (Grants No. 2017YFA0303900 and No. 2017YFA0304004), the Anhui Initiative in Quantum Information Technologies, and the Zhongguancun Haihua Institute for Frontier Information Technology.

APPENDIX A: DISTILLATION OF THE GHZ STATE

Inspired by the quantum-key-distribution protocol based on entanglement distillation [52,53], multiparty quantum-conference-key-distribution protocols based on entanglement distillation are proposed to securely distribute random bits between multiple users [15–17]. The security of the PM-QCC network is based on the distillation of the N-qubit GHZ state [50]:

$$|\Phi^+\rangle = \frac{1}{\sqrt{2}}(|00\cdots 0\rangle + |11\cdots 1\rangle)_N, \tag{A1}$$

which is stabilized by a group of stabilizer generators,

$$\begin{aligned} S_0 &= XXXX\cdots X,\\ S_1 &= ZZII\cdots I,\\ S_2 &= ZIZI\cdots I,\\ S_3 &= ZIIZ\cdots I,\\ &\vdots\\ S_{N-1} &= ZIII\cdots Z, \end{aligned} \tag{A2}$$

where $X = \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$, $Z = \left(\begin{smallmatrix}1&0\\0&-1\end{smallmatrix}\right)$, and $I = \left(\begin{smallmatrix}1&0\\0&1\end{smallmatrix}\right)$ are Pauli matrices. The corresponding N-qubit-GHZ-state basis is

$$\begin{aligned}|\psi_{j,i_1 i_2\cdots i_{N-1}}\rangle = \frac{1}{\sqrt{2}}[&|0 i_1 i_2\cdots i_{N-1}\rangle\\ &+(-1)^j|1\bar{i}_1\bar{i}_2\cdots\bar{i}_{N-1}\rangle],\end{aligned} \tag{A3}$$

where $j, i_m \in \{0,1\}$, $1 \leq m \leq N-1$, and $\bar{i}_m$ is the logical negation of i_m. If $j = 1$ ($i_m = 1$), the basis vector is the -1 eigenvalue of S_0 (S_m). This means that there is a phase error (bit error) to the original GHZ state. Thus, j (or i_m) is also called the "phase (or amplitude) bit." With us eof the multipartite-hashing method [50], the yield of distillation of the pure N-qubit GHZ state is

$$D = 1 - \max[H(E^Z_{\mu,P_1P_2}), H(E^Z_{\mu,P_1P_3}), \ldots, H(E^Z_{\mu,P_1P_N})] - H(E^X_\mu), \tag{A4}$$

where E^Z_{μ,P_1P_m} represents the bit-flip error rate of parties P_1 and P_m corresponding to the stabilizer S_{m-1}, E^X_μ is the phase-flip error corresponding to the stabilizer S_0, and $H(x) = -x\log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function.

APPENDIX B: SECURITY ANALYSIS FOR PM QCC

Without loss of generality, we consider an entanglement-based version whereby party P_m ($1 \leq m \leq N$) prepares entanglement states between virtual qubits and his WCPs instead of directly preparing WCPs. Thus, its security analysis applies to the entanglement-distillation argument [16,52,53]. As shown in Fig. 5(a), there is a virtual qubit at each party:

$$|+\rangle = \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle).$$

Party P_m prepares an entanglement state using a controlled phase gate $C_\pi = |0\rangle\langle 0|U_o + |1\rangle\langle 1|U_\pi$ between the virtual qubit and the WCP:

$$|\Psi\rangle_m = \frac{1}{\sqrt{2}}[|0\rangle|e^{i\phi}\sqrt{\mu_m}\rangle + |1\rangle|e^{i(\phi+\pi)}\sqrt{\mu_m}\rangle], \tag{B1}$$

where $U_{0(\pi)}$ will attach a phase of 0 (π) to the WCP. Without loss of generality, the phases of parties $P_1, P_2, \ldots, P_N$ are supposed to be $\phi_1 = \phi_2 = \cdots = \phi_N = \phi$. The WCPs are sent to an untrusted third party, Eve, to perform interference measurements with other parties, while the virtual qubits are kept at each party. As stated in the main text, the WCP with random phase ϕ of party P_m passing through the 50:50 beam splitter BS1 is split into two WCPs with the same encoded phases:

$$|e^{i(\phi+\pi k_m)}\sqrt{\mu}\rangle \xrightarrow{\text{BS1}} |e^{i(\phi+\pi k_m)}\sqrt{\mu/2}\rangle \otimes |e^{i(\phi+\pi k_m)}\sqrt{\mu/2}\rangle, \tag{B2}$$

where $\phi + \pi k_m$ is the encoded phase of party P_m. The protocol is equivalent to entanglement-based protocol in Fig. 2(b). Since the neighbor WCPs are of the same intensity, the only difference is their phases. Thus, the WCPs in each branch can be regarded as being from one virtual WCP source $|e^{i\phi}\sqrt{\mu}\rangle$, and the protocol is straightforwardly equivalent to that in Fig. 5(b). In the protocol in Fig. 5(b), the N-party state evolves as

$$\begin{aligned}
&|+\rangle_{P_1}|+\rangle_{P_2}\cdots|+\rangle_{P_N}\sum_{n_1=0}^{\infty} e^{-\mu/2}\frac{(e^{i\phi}\sqrt{\mu}C_1^\dagger)^{n_1}}{n_1!}\sum_{n_2=0}^{\infty} e^{-\mu/2}\frac{(e^{i\phi}\sqrt{\mu}C_2^\dagger)^{n_2}}{n_2!}\cdots\sum_{n_{N-1}=0}^{\infty} e^{-\mu/2}\frac{(e^{i\phi}\sqrt{\mu}C_{N-1}^\dagger)^{n_{N-1}}}{n_{N-1}!}|\text{vac}\rangle\\
&\xrightarrow{\text{BS}} \sum_{n_1,n_2,\ldots,n_{N-1}=0}^{\infty} |+\rangle_{P_1}|+\rangle_{P_2}\cdots|+\rangle_{P_N}\frac{e^{-\mu/2}(\mu)^{\frac{n_1}{2}}}{n_1!}\left(\frac{e^{i\phi}p_1^\dagger + e^{i\phi}p_{2L}^\dagger}{\sqrt{2}}\right)^{n_1}\frac{e^{-\mu/2}(\mu)^{\frac{n_2}{2}}}{n_2!}\left(\frac{e^{i\phi}p_{2R}^\dagger + e^{i\phi}p_{3L}^\dagger}{\sqrt{2}}\right)^{n_2}\cdots\\
&\frac{e^{-\mu/2}(\mu)^{n_{N-1}/2}}{n_{N-1}!}\left(\frac{e^{i\phi}p_{(N-1)R}^\dagger + e^{i\phi}p_N^\dagger}{\sqrt{2}}\right)^{n_{N-1}}|\text{vac}\rangle\\
&\xrightarrow{C_\pi} \frac{1}{2^{N/2}}\sum_{n_1,n_2,\ldots,n_{N-1}=0}^{\infty}\frac{e^{-(N-1)\mu/2}(\mu)^{(n_1+n_2+\cdots+n_{N-1})/2}}{n_1!n_2!\cdots n_{N-1}!}\left[|0\rangle|0\rangle\cdots|0\rangle\left(\frac{e^{i\phi}p_1^\dagger + e^{i\phi}p_{2L}^\dagger}{\sqrt{2}}\right)^{n_1}\left(\frac{e^{i\phi}p_{2R}^\dagger + e^{i\phi}p_{3L}^\dagger}{\sqrt{2}}\right)^{n_2}\cdots\right.\\
&\left(\frac{e^{i\phi}p_{(N-1)R}^\dagger + e^{i\phi}p_N^\dagger}{\sqrt{2}}\right)^{n_{N-1}} + \cdots\\
&\left.+\ |1\rangle|1\rangle\cdots|1\rangle\left(\frac{-e^{i\phi}p_1^\dagger - e^{i\phi}p_{2L}^\dagger}{\sqrt{2}}\right)^{n_1}\left(\frac{-e^{i\phi}p_{2R}^\dagger - e^{i\phi}p_{3L}^\dagger}{\sqrt{2}}\right)^{n_2}\cdots\left(\frac{-e^{i\phi}p_{(N-1)R}^\dagger - e^{i\phi}p_N^\dagger}{\sqrt{2}}\right)^{n_{N-1}}\right]|\text{vac}\rangle\\
&= \frac{1}{2^{(N-1)/2}}\sum_{n_1,n_2,\ldots,n_{N-1}=0}^{\infty}\frac{e^{-(N-1)\mu/2}(\mu)^{(n_1+n_2+\cdots+n_{N-1})/2}}{n_1!n_2!\cdots n_{N-1}!}
\end{aligned}$$

$$\times\Bigg\{\sum_{i_1,i_2,\ldots,i_{N-1}\in\{0,1\}}\frac{1}{\sqrt{2}}[|0i_1i_2\cdots i_{N-1}\rangle+(-1)^{n_1+n_2+\cdots+n_{N-1}}|1\bar{i}_1\bar{i}_2\cdots\bar{i}_{N-1}\rangle]$$

$$\left[\frac{e^{i\phi}p_1^\dagger+(-1)^{i_1}e^{i\phi}p_{2L}^\dagger}{\sqrt{2}}\right]^{n_1}\left[\frac{(-1)^{i_1}e^{i\phi}p_{2R}^\dagger+(-1)^{i_2}e^{i\phi}p_{3L}^\dagger}{\sqrt{2}}\right]^{n_2}\cdots\left[\frac{(-1)^{i_{N-2}}e^{i\phi}p_{(N-1)R}^\dagger+(-1)^{i_{N-1}}e^{i\phi}p_N^\dagger}{\sqrt{2}}\right]^{n_{N-1}}\Bigg\}|\mathrm{vac}\rangle$$

$$=\frac{1}{2^{(N-1)/2}}\times\sum_{i_1,i_2,\ldots,i_{N-1}\in\{0,1\}}\Bigg\{\frac{1}{\sqrt{2}}[|0i_1i_2\cdots i_{N-1}\rangle+|1\bar{i}_1\bar{i}_2\cdots\bar{i}_{N-1}\rangle]\sqrt{p_{\mathrm{even}}}|\mathrm{even}\rangle_\mu$$

$$+\frac{1}{\sqrt{2}}[|0i_1i_2\cdots i_{N-1}\rangle-|1\bar{i}_1\bar{i}_2\cdots\bar{i}_{N-1}\rangle]\sqrt{p_{\mathrm{odd}}}|\mathrm{odd}\rangle_\mu\Bigg\}, \tag{B3}$$

where $C_i^\dagger$ is the creation operator of the ith virtual source, $|\mathrm{vac}\rangle$ is the vacuum state, $\sqrt{p_{\mathrm{even}}}$ and $\sqrt{p_{\mathrm{odd}}}$ are normalized coefficients of pure states $|\mathrm{even}\rangle_\mu$ and $|\mathrm{odd}\rangle_\mu$ [see Eqs. (B11)–(B12)], and $p_1^\dagger, p_{2L}^\dagger, p_{2R}^\dagger, \ldots$ are the creation operators of the corresponding path mode after beam splitters BS1. The beam splitters act as

$$T_{\mathrm{BS}}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}.$$

For example, consider the beams interfere at the second beam splitter shown in the first branch in Fig. 5(b). For input-beam optical modes $p_1^\dagger$ and $p_{2L}^\dagger$, the output modes $L_1^\dagger$ and $R_1^\dagger$ are

$$\begin{pmatrix}L_1^\dagger\\ R_1^\dagger\end{pmatrix}=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\ 1 & -1\end{pmatrix}\begin{pmatrix}p_1^\dagger\\ p_{2L}^\dagger\end{pmatrix}, \tag{B4}$$

where $L_1^\dagger$ ($R_1^\dagger$) means the output-path mode to detector $D_{L_1}^\dagger$ ($D_{R_1}^\dagger$) for branch 1 in Fig. 5(b). Then, we have

$$\frac{p_1^\dagger+(-1)^{i_1}p_{2L}^\dagger}{\sqrt{2}}\xrightarrow{\mathrm{BS}}\begin{cases}L_1^\dagger & \text{if } i_1=0,\\ R_1^\dagger & \text{if } i_1=1.\end{cases} \tag{B5}$$

Thus, when $i_1=0$, only detector D_{L_1} clicks, while when $i_1=1$, only detector D_{R_1} clicks. From Eq. (B3), once there is a successful coincidence event whereby only one detector clicks in each branch, a GHZ state of N parties is postselected successfully such that

$$|\Psi_{j,i_1i_2\cdots i_{N-1}}\rangle=\frac{1}{\sqrt{2}}[|0i_1i_2\cdots i_{N-1}\rangle+(-1)^j|1\bar{i}_1\bar{i}_2\cdots\bar{i}_{N-1}\rangle], \tag{B6}$$

where $j=n_1+n_2+\cdots+n_{N-1}$. One can obtain the phase-error correlation immediately:

$$e^X_{n_1,n_2,\ldots,n_{N-1}}=\begin{cases}1 & \text{for } j\in \text{odd},\\ 0 & \text{for } j\in \text{even}.\end{cases} \tag{B7}$$

The phase error rate is determined by different photon-number components. A similar phase-error property is shown in a improved analysis of the PM-QKD protocol [57]. When $n_1+n_2+\cdots+n_{N-1}\in$ odd, $e^X_{n_1,n_2,\ldots,n_{N-1}}=1$ and when $n_1+n_2+\cdots+n_{N-1}\in$ even, $e^X_{n_1,n_2,\ldots,n_{N-1}}=0$. Using the correlation of Eqs. (B7) and (B3), we can estimate the total phase error rate E^X_μ as

$$E^X_\mu=p_{\mathrm{odd}}\frac{Y^{\mathrm{odd}}_\mu}{Q_\mu}, \tag{B8}$$

where Y^{odd}_μ is the overall yield for odd-number components, and Q_μ is the overall gain of signal pulses.

Following the entanglement-distillation argument [52, 53], to generate a sequence of almost-perfectly-secure key bits, P_1, $P_2, \ldots, P_N$ need to share only a sequence of almost-perfect GHZ states in terms of monogamy of entanglement [54,55]. From Eq. (A4), the key-generation rate of the PM-QCC network is

$$R_{N\text{-party}}=\left(\frac{2}{M}\right)^{N-1}Q_\mu\{1-f\times\max[H(E^Z_{\mu,P_1P_2}),$$
$$H(E^Z_{\mu,P_1P_3}),\ldots,H(E^Z_{\mu,P_1P_N})]-H(E^X_\mu)\}, \tag{B9}$$

where $(2/M)^{N-1}$ is the prefactor induced by phase postselection, which can be optimized according to the experimental parameters [34,35].

What is counterintuitive in the security analysis of the phase-matching protocol is that parties $P_1, P_2, \ldots, P_N$ will announce their random phases ϕ_1, $\phi_2, \ldots, \phi_N$ after Eve's announcements of her measurement results. If the phases are not announced by P_1, $P_2, \ldots, P_N$, the weak coherent

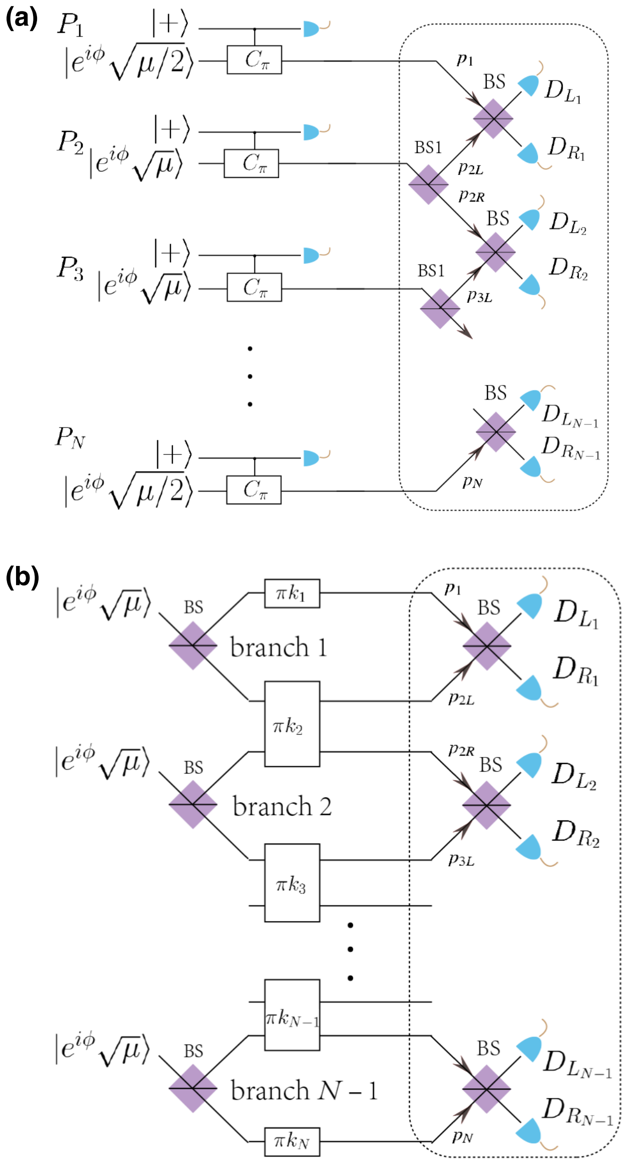

FIG. 5. (a) The entanglement-based version of the N-party PM-QCC network. (b) The equivalent entanglement-based version of the N-party PM-QCC network with virtual sources after Eve's splitting. In 5(a),5(b), random phases are supposed to be $\phi_1=\phi_2=\cdots=\phi$. Here we omit the virtual qubits for simplicity in (b). $p_1, p_{2L}, \ldots, p_N$ are path modes after Eve's splitting. D_{L_1} (D_{R_1}) is the left (right) detector of the first measurement branch. D_{L_2} (D_{R_2}) is the left (right) detector of the second measurement branch. $D_{L_{N-1}}$ ($D_{R_{N-1}}$) is the left (right) detector of the $(N-1)$th measurement branch. BS, beam splitter. C_π, controlled phase gate.

pulses can be regarded as a mixture of different photon-number states in which their phases are meaningless to the untrusted party, Eve, while after the announcement, their pulses can no longer be regarded as a mixture of photon number states. Here we show that the PM-QCC protocol is secure against phase announcements.

Firstly, the random phases are announced after Eve's announcements. Thus, Eve's announcement strategies cannot depend on the phase information os parties P_1, $P_2, \ldots, P_N$.

Secondly, the security analysis is based on entanglement distillation. After the phase announcement, one can still distill perfect GHZ states that are decoupled from Eve according to the monogamy of entanglement. Specifically, let us consider the beam-splitting attack as an example in which Eve manages to get the key information using the announced phases.

In the beam-splitting attack, Eve can modulate the transmission rates of the channels. For example, she using a beam splitter with transmission rate η to simulate a lossy channel. The reflection signal beams are intercepted by Eve's registers, and then the transmission beams are sent to an interferometer through perfect channels. After the phase announcements, Eve will extract some information from the intercepted beams according to the phase announcements. From Eq. (B3), we know that the state arriving at the detectors can be sorted to $n_1+n_2+\cdots+n_{N-1}\in$ even or odd. Without loss of generality, we consider only the components that would result in the detection events $D_{L_1}D_{L_2}\cdots D_{L_{N-1}}$ in Eq. (B3). The correlated components are

$$\frac{1}{\sqrt{2}}(|00\cdots0\rangle+|11\cdots1\rangle)\sqrt{p_{\text{even}}}|\text{even}\rangle_\mu + \frac{1}{\sqrt{2}}(|00\cdots0\rangle-|11\cdots1\rangle)\sqrt{p_{\text{odd}}}|\text{odd}\rangle_\mu, \tag{B10}$$

where

$$|\text{even}\rangle_\mu(|\text{odd}\rangle_\mu)=\frac{1}{\sqrt{p_{\text{even(odd)}}}}\sum_{n_1+n_2+\cdots+n_{N-1}\in\text{even(odd)}}\frac{e^{-(N-1)\mu/2}(\mu)^{\frac{n_1+n_2+\cdots+n_{N-1}}{2}}}{n_1!n_2!\cdots n_{N-1}!}\left\{\left[\frac{p_1^\dagger+(-1)^{i_1}p_{2L}^\dagger}{\sqrt{2}}\right]^{n_1}\otimes\left[\frac{(-1)^{i_1}p_{2R}^\dagger+(-1)^{i_2}p_{3L}^\dagger}{\sqrt{2}}\right]^{n_2}\otimes\cdots\otimes\left[\frac{(-1)^{i_{N-2}}p_{(N-1)R}^\dagger+(-1)^{i_{N-1}}p_N^\dagger}{\sqrt{2}}\right]^{n_{N-1}}\right\}|\text{vac}\rangle, \tag{B11}$$

$$p_{\text{even}}=\sum_{n_1+n_2+\cdots+n_{N-1}\in\text{even}}\frac{e^{-(N-1)\mu}(\mu)^{n_1+n_2+\cdots+n_{N-1}}}{n_1!n_2!\cdots n_{N-1}!}=e^{-(N-1)\mu}\cosh[(N-1)\mu], \tag{B12}$$

$$p_{\text{odd}}=1-p_{\text{even}}=e^{-(N-1)\mu}\sinh[(N-1)\mu], \tag{B13}$$

with $i_1 = i_2 = \cdots = i_{N-1} = 0$ for Eq. (B10). Here we omit the phase because Eve's announcement strategy cannot be dependent on ϕ.

When the phases are not announced, $|\text{even}\rangle_\mu(|\text{odd}\rangle_\mu)$ is a mixture of photon-number states from Eve's perspective after the phase randomization, while if the phases are announced, $|\text{even}\rangle_\mu(|\text{odd}\rangle_\mu)$ can no longer be regarded as a mixture of photon-number states. For the beam-splitting attack using beam splitters with transmission rate η, Eq. (B10) can be rewritten as

$$\begin{aligned}
&\frac{1}{\sqrt{2}}\Bigg[|00\cdots0\rangle|\sqrt{\frac{(1-\eta)\mu}{2}}\rangle|\sqrt{\frac{(1-\eta)\mu}{2}}\rangle\cdots|\sqrt{\frac{(1-\eta)\mu}{2}}\rangle\\
&\quad+|11\cdots1\rangle|-\sqrt{\frac{(1-\eta)\mu}{2}}\rangle|-\sqrt{\frac{(1-\eta)\mu}{2}}\rangle\cdots|-\sqrt{\frac{(1-\eta)\mu}{2}}\rangle\Bigg]\sqrt{p^{\eta\mu}_{\text{even}}}|\text{even}\rangle_{\eta\mu}\\
&\quad+\frac{1}{\sqrt{2}}\Bigg[|00\cdots0\rangle|\sqrt{\frac{(1-\eta)\mu}{2}}\rangle|\sqrt{\frac{(1-\eta)\mu}{2}}\rangle\cdots|\sqrt{\frac{(1-\eta)\mu}{2}}\rangle\\
&\quad-|11\cdots1\rangle|-\sqrt{(1-\eta)\frac{\mu}{2}}\rangle|-\sqrt{(1-\eta)\frac{\mu}{2}}\rangle\cdots|-\sqrt{(1-\eta)\frac{\mu}{2}}\rangle\Bigg]\sqrt{p^{\eta\mu}_{\text{odd}}}|\text{odd}\rangle_{\eta\mu}\\
&\quad=\frac{1}{\sqrt{2}}(|00\cdots0\rangle+|11\cdots1\rangle)\left[\sqrt{p^{(1-\eta)\mu}_{\text{even}}}|\text{even}\rangle_{(1-\eta)\mu}\sqrt{p^{\eta\mu}_{\text{even}}}|\text{even}\rangle_{\eta\mu}+\sqrt{p^{(1-\eta)\mu}_{\text{odd}}}|\text{odd}\rangle_{(1-\eta)\mu}\sqrt{p^{\eta\mu}_{\text{odd}}}|\text{odd}\rangle_{\eta\mu}\right]\\
&\quad+\frac{1}{\sqrt{2}}(|00\cdots0\rangle-|11\cdots1\rangle)\left[\sqrt{p^{(1-\eta)\mu}_{\text{odd}}}|\text{odd}\rangle_{(1-\eta)\mu}\sqrt{p^{\eta\mu}_{\text{even}}}|\text{even}\rangle_{\eta\mu}+\sqrt{p^{(1-\eta)\mu}_{\text{even}}}|\text{even}\rangle_{(1-\eta)\mu}\sqrt{p^{\eta\mu}_{\text{odd}}}|\text{odd}\rangle_{\eta\mu}\right],
\end{aligned} \tag{B14}$$

where $|\text{even}\rangle_{\eta\mu}$ ($|\text{odd}\rangle_{\eta\mu}$) interferes before phase announcements, and cannot be used for eavesdropping. $\sqrt{p^{\eta\mu}_{\text{odd}}}$ is the normalization coefficient for pure state $|\text{odd}\rangle_{\eta\mu}$, and similarly for other coefficients, while $|\text{even}\rangle_{(1-\eta)\mu}$ and $|\text{odd}\rangle_{(1-\eta)\mu}$ are intercepted by Eve, and cannot be decoupled from private qubits after phase announcements. Furthermore, one can derive

$$\begin{aligned}
&\sqrt{p^{(1-\eta)\mu}_{\text{even}}}|\text{even}\rangle_{(1-\eta)\mu}\sqrt{p^{\eta\mu}_{\text{even}}}|\text{even}\rangle_{\eta\mu}\\
&\qquad+\sqrt{p^{(1-\eta)\mu}_{\text{odd}}}|\text{odd}\rangle_{(1-\eta)\mu}\sqrt{p^{\eta\mu}_{\text{odd}}}|\text{odd}\rangle_{\eta\mu}\\
&\quad=\sqrt{p^{\mu}_{\text{even}}}|\text{even}\rangle_{\mu},\\
&\sqrt{p^{(1-\eta)\mu}_{\text{odd}}}|\text{odd}\rangle_{(1-\eta)\mu}\sqrt{p^{\eta\mu}_{\text{even}}}|\text{even}\rangle_{\eta\mu}\\
&\qquad+\sqrt{p^{(1-\eta)\mu}_{\text{even}}}|\text{even}\rangle_{(1-\eta)\mu}\sqrt{p^{\eta\mu}_{\text{odd}}}|\text{odd}\rangle_{\eta\mu}\\
&\quad=\sqrt{p^{\mu}_{\text{odd}}}|\text{odd}\rangle_{\mu}.
\end{aligned} \tag{B15}$$

From Eq. (B8), the phase error is estimated for coherent states with intensity μ. Meanwhile, as shown in Eq. (B14), the phase error after the phase announcement can also be estimated by Eq. (B8). This means that the phase error induced by the phase announcement is estimated in Eq. (B8), and can be corrected during the entanglement-distillation protocol according to Eq. (B9). Thus, the PM-QCC protocol is secure against the phase announcements.

Furthermore, if we can estimate the phase error accurately in Eq. (B8), the PM-QCC protocol is still secure even when the phase choices for the signal pulses are announced before Eve's measurement according to Eq. (B14). Thus, the phase-compensation method provides a practical and secure way to align phases for signal pulses, and the PM-QCC protocol can be improved to a version without phase postselection in signal pulses (see Appendix E for details).

APPENDIX C: PARAMETER ESTIMATION FOR PM QCC

Experimentally, the overall gain Q_μ and QBERs $E^Z_{\mu,P_1P_2}, E^Z_{\mu,P_1P_3}, \ldots, E^Z_{\mu,P_1P_N}$ can be directly estimated from the announced results. However, the phase error E^X_μ cannot be measured directly in experiments. We can use the decoy-state method to estimate the phase error rate E^X_μ.

As shown in Fig. 5(b), if the phase-matching condition $|j_m + j^a_m - j_{m+1}| \mod M = 0$ or $M/2$ is satisfied, the click events in each branch are independent. In branch 1, the gain $Q_{\mu,1}$ and the QBER $E_{\mu}^{Z,1}$ can be estimated as

$$\begin{aligned} Q_{\mu,1} &= P(D_{L_1}) + P(D_{R_1}), \\ E_{\mu}^{Z,1} &= \frac{P(D_{L_1})}{P(D_{L_1}) + P(D_{R_1})}, \end{aligned} \tag{C1}$$

where $P(D_{L_1})$ is the probability that only detector D_{L_1} clicks in branch 1 and $P(D_{R_1})$ is the probability that only the detector D_{R_1} clicks in branch 1. Because of the independence between the detection events in each branch when the phases are matched, the gain and QBERs for other branches can be estimated as $Q_{\mu,t} = Q_{\mu,1}$ and $E_{\mu}^{Z,t} = E_{\mu}^{Z,1}$ $(2 \leq t \leq N-1)$. Thus, the overall gain Q_{μ} and the marginal QBER $E_{\mu,P_1P_m}^{Z}$ between parties P_1 and P_m are

$$Q_{\mu} = (Q_{\mu,1})^{N-1} = p_{\text{odd}} Y_{\mu}^{\text{odd}} + p_{\text{even}} Y_{\mu}^{\text{even}}, \tag{C2a}$$

$$E_{\mu,P_1P_m}^{Z} = \sum_{k=0}^{\lfloor (m-2)/2 \rfloor} C_{m-1}^{2k+1} (E_{\mu}^{Z,1})^{2k+1} (1 - E_{\mu}^{Z,1})^{m-2k-2}, \tag{C2b}$$

where C_{m-1}^{2k+1} is the binomial coefficient, $\lfloor x \rfloor$ is the floor function, and Y_{μ}^{odd} (Y_{μ}^{even}) is the overall yield for an odd-photon-number (even-photon-number) component. With use of the decoy-state method, we can estimate $p_{\text{odd}} Y_{\mu}^{\text{odd}}$ from Eq. (C2a) (see Appendix D for details). Then, the phase error rate E_{μ}^{X} can be estimated by Eqs. (B7) and (B8).

Without loss of generality, one can derive the gain $Q_{\mu,1}$ and the QBER $E_{\mu}^{Z,1}$ for branch 1 [35] when the phase-matching condition $|j_1 + j_1^a - j_2| \mod M = 0$ or $M/2$ and $k_1 = k_2 = 0$. If the phase reference deviation ϕ_0 is constrained to be $\phi_0 \in [-\pi/M, \pi/M)$ with the help of the phase-compensation method, the phases of parties P_1 and P_2 are uniformly distributed on $\phi_1 \in [(2\pi/M)j_1, (2\pi/M)(j_1+1))$ and $\phi_2 \in [(2\pi/M)j_1 + \phi_0, (2\pi/M)(j_1+1) + \phi_0)$. To be simple and consistent with Ref. [35], we take $j_1 = 0$. Thus,

$$\begin{aligned} \phi_1 &\in \left[0, \frac{2\pi}{M}\right), \\ \phi_2 &\in \left[\phi_0, \frac{2\pi}{M} + \phi_0\right). \end{aligned} \tag{C3}$$

As shown in Fig. 5, the evolution of the encoded state of parties P_1 and P_2 in branch 1 is

$$\begin{aligned} &|e^{i\phi_1}\sqrt{\eta\mu/2}\rangle_{P_1} \otimes |e^{i\phi_2}\sqrt{\eta\mu/2}\rangle_{P_{2L}} \\ &\xrightarrow{\text{BS}} |\sqrt{\eta\mu/2}(e^{i\phi_1} + e^{i\phi_2})\rangle_{L_1} \otimes |\sqrt{\eta\mu/2}(e^{i\phi_1} - e^{i\phi_2})\rangle_{R_1}, \end{aligned} \tag{C4}$$

where the transmission efficiency η consists of channel losses and detection efficiencies. From Eq. (C4), the pulses hitting detectors D_{L_1} and D_{R_1} are independent. The probabilities of click and nonclick events for D_{L_1} and D_{R_1} can be directly calculated:

$$\begin{aligned} P(\bar{L}_1) &= (1 - p_d)\exp\left(-\eta\mu\cos^2\frac{\phi_\delta}{2}\right), \\ P(L_1) &= 1 - P(\bar{L}_1), \\ P(\bar{R}_1) &= (1 - p_d)\exp\left(-\eta\mu\sin^2\frac{\phi_\delta}{2}\right), \\ P(R_1) &= 1 - P(\bar{R}_1), \end{aligned} \tag{C5}$$

where $P(L_1)$ $[P(\bar{L}_1)]$ is the click (nonclick) probability of detector D_{L_1}, $P(R_1)$ $[P(\bar{R}_1)]$ is the click (nonclick) probability of detector D_{R_1}, and $\phi_\delta = \phi_2 - \phi_1$. The successful-detection probabilities for branch 1 are

$$\begin{aligned} P(D_{L_1}) &= P(L_1)P(\bar{R}_1), \\ P(D_{R_1}) &= P(\bar{L}_1)P(R_1), \end{aligned} \tag{C6}$$

respectively. Then, the gain $Q_{\mu,1}$ of branch 1 is [35]

$$\begin{aligned} Q_{\mu,1} &= P(D_{L_1}) + P(D_{R_1}) \\ &\approx 1 - e^{-\eta\mu} + 2p_d e^{-\eta\mu}, \end{aligned} \tag{C7}$$

where the approximation is obtained by our ignoring $\sin^2(\phi_\delta/2)$ with a small ϕ_δ and ignoring the higher-order term $p_d(1 - e^{-\eta\mu} + 2p_d e^{-\eta\mu})$. For given ϕ_δ, the QBER is [35]

$$\begin{aligned} E_{\mu}^{Z,1}(\phi_\delta) &= \frac{P(D_{R_1})}{P(D_{L_1}) + P(D_{R_1})} \\ &\approx \frac{e^{-\eta\mu}}{Q_{\mu,1}}\left(p_d + \eta\mu\sin^2\frac{\phi_\delta}{2}\right), \end{aligned} \tag{C8}$$

where the approximation is obtained by our taking $e^{\eta\mu\sin^2(\phi_\delta/2)} \approx 1 + \eta\mu\sin^2(\phi_\delta/2)$ with a small ϕ_δ and ignoring the higher-order term $p_d[p_d + \eta\mu\sin^2(\phi_\delta/2)]$. From Eq. (C3) and $\phi_0 \in [-\pi/M, \pi/M)$, the QBER $E_{\mu}^{Z,1}$ is of the form

$$\begin{aligned} E_{\mu}^{Z,1} &= \frac{M}{2\pi}\int_{-\pi/M}^{\pi/M} d\phi_0 \int_{-3\pi/M}^{3\pi/M} d\phi_\delta f^{\phi_0}(\phi_\delta) E_{\mu}^{Z,1}(\phi_\delta) \\ &= \frac{(p_d + \eta\mu e_\delta)e^{-\eta\mu}}{Q_{\mu,1}}, \end{aligned} \tag{C9}$$

where $e_\delta = \pi/M - (M^2/\pi^2)\sin^3(\pi/M)$. Here $f^{\phi_0}(\phi_\delta)$ is the probability distribution of ϕ_δ for given ϕ_0:

$$f^{\phi_0}(\phi_\delta) = \begin{cases} \left(\frac{M}{2\pi}\right)^2 \left[\phi_\delta + \left(\frac{2\pi}{M} - \phi_0\right)\right], \phi_\delta \in \left[\phi_0 - \frac{2\pi}{M}, \phi_0\right), \\ \left(\frac{M}{2\pi}\right)^2 \left[-\phi_\delta + \left(\frac{2\pi}{M} + \phi_0\right)\right], \phi_\delta \in \left[\phi_0, \phi_0 + \frac{2\pi}{M}\right). \end{cases}$$

APPENDIX D: DECOY-STATE ANALYSIS FOR PM QCC

As stated in the main text, the signal pulses with intensity μ are used only to estimate the gain Q_μ and marginal QBERs E^Z_{μ,P_1P_2}, $E^Z_{\mu,P_1P_3},\ldots,E^Z_{\mu,P_1P_N}$. The phase errors E^X_μ are estimated from decoy pulses in the intensity set $\{\nu,\omega,\tau,\ldots,0\}$. The phase choices and intensities of the users are announced after Eve's announcement. Eve's attacks are independent of signal pulses and decoy pulses. Thus, the decoy states can be used to estimate the phase error E^X_μ for the signal pulses.

Considering the decoy pulses, the virtual sources in each branch of the protocol in Fig. 5(b) are simultaneously randomized if the phase-matching conditions are satisfied: $|\phi_1-\phi_2|=0$ or π, $|\phi_2-\phi_3|=0$ or $\pi,\ldots,|\phi_{N-1}-\phi_N|=0$ or π. For simplicity, we take $N=3$ and $\phi_1=\phi_2=\cdots=\phi_N=\phi$, and the virtual source under the phase-matching condition is [57]

$$\frac{1}{2\pi}\int_0^{2\pi} d\phi|e^{i\phi}\sqrt{\mu}\rangle_{C_1}|e^{i\phi}\sqrt{\mu}\rangle_{C_2}\langle e^{i\phi}\sqrt{\mu}|_{C_1}\langle e^{i\phi}\sqrt{\mu}|_{C_2} = \sum_k^\infty P_{2\mu}(k)|k\rangle\langle k|, \tag{D1}$$

where $P_{2\mu}(k)=e^{-2\mu}[(2\mu)^k/k!]$ is the probability of generating k photons in the virtual source, $|k\rangle=[(1/\sqrt{2})(C_1^\dagger+C_2^\dagger)]^k/\sqrt{k!}|\text{vac}\rangle$, and $k=n_1+n_2$ is the total photon number of branches 1 and 2. Then the overall Q_μ [Eq. (C2a)] and phase error rate E^X_μ [Eq. (B8)] are

$$Q_\mu = \sum_k^\infty P_{2\mu}(k)Y_k, \tag{D2a}$$

$$\begin{aligned}
E^X_\mu &= \sum_{k\in\text{odd}} P_{2\mu}(k)\frac{Y_k}{Q_\mu}\\
&= 1-\sum_{k\in\text{even}} P_{2\mu}(k)\frac{Y_k}{Q_\mu}\\
&= 1-e^{-2\mu}\frac{Y_0}{Q_\mu}-e^{-2\mu}\frac{(2\mu)^2}{2}\frac{Y_2}{Q_\mu}-\cdots \qquad \text{(D2b)}\\
&\le 1-e^{-2\mu}\frac{Y_0}{Q_\mu}-e^{-2\mu}\frac{(2\mu)^2}{2}\frac{Y_2}{Q_\mu}\\
&\le E^{X,U}_\mu = 1-e^{-2\mu}\frac{Y_0}{Q_\mu}-e^{-2\mu}\frac{(2\mu)^2}{2}\frac{Y^L_2}{Q_\mu},
\end{aligned}$$

where $Y_k\in[0,1]$ is the yield when k photons are generated in the virtual source, Y^L_2 is the lower bound of the yield when two photons are generated in the virtual source, and $E^{X,U}_\mu$ is the upper bound of the phase error rate. The first inequality is obtained by our setting high-order terms including $Y_4, Y_6,\ldots$ to 0. The second inequality is obtained by our replacing Y_2 with its lower bound Y^L_2. From Eq. (D2a), one can obtain a set of overall gains with different decoy states that can be used to estimate the yield Y_k. For the three-party PM-QCC protocol, four decoy states with intensities $\{\nu>\omega>\tau>0\}$ are used to estimate Y^L_2 using the Gaussian-elimination method [43,58]:

$$\begin{aligned}
e^{2\nu}Q_\nu &= Y_0+2\nu Y_1+\frac{(2\nu)^2}{2}Y_2+\frac{(2\nu)^3}{6}Y_3\\
&\quad+\frac{(2\nu)^4}{4!}Y_4+\cdots,\\
e^{2\omega}Q_\omega &= Y_0+2\omega Y_1+\frac{(2\omega)^2}{2}Y_2+\frac{(2\omega)^3}{6}Y_3\\
&\quad+\frac{(2\omega)^4}{4!}Y_4+\cdots,\\
e^{2\tau}Q_\tau &= Y_0+2\tau Y_1+\frac{(2\tau)^2}{2}Y_2+\frac{(2\tau)^3}{6}Y_3\\
&\quad+\frac{(2\tau)^4}{4!}Y_4+\cdots,\\
Q_0 &= Y_0,
\end{aligned} \tag{D3}$$

where Q_ν, Q_ω, Q_τ, and Q_0 are overall gains for different decoy states. From Eq. (D3), one can cancel out the terms Y_0, Y_1, and Y_3 with the Gaussian-elimination method and generate an equation given by

$$G=G_2Y_2+G_4Y_4+G_5Y_5+\cdots, \tag{D4}$$

where

$$\begin{aligned}
G &= [2\omega(2\nu)^3-2\nu(2\omega)^3][2\tau(e^{2\omega}Q_\omega-Q_0)-2\omega(e^{2\tau}Q_\tau-Q_0)]\\
&\quad-[2\tau(2\omega)^3-2\omega(2\tau)^3][2\omega(e^{2\nu}Q_\nu-Q_0)-2\nu(e^{2\omega}Q_\omega-Q_0)],
\end{aligned} \tag{D5a}$$

$$G_2=\frac{[2\omega(2\nu)^3-2\nu(2\omega)^3][2\tau(2\omega)^2-2\omega(2\tau)^2]-[2\tau(2\omega)^3-2\omega(2\tau)^3][2\omega(2\nu)^2-2\nu(2\omega)^2]}{2}, \tag{D5b}$$

$$G_4=\frac{[2\omega(2\nu)^3-2\nu(2\omega)^3][2\tau(2\omega)^4-2\omega(2\tau)^4]-[2\tau(2\omega)^3-2\omega(2\tau)^3][2\omega(2\nu)^4-2\nu(2\omega)^4]}{4!}, \tag{D5c}$$

$$\vdots$$

Since $\nu > \omega > \tau > 0$, one can see that G, $G_2 > 0$ and G_4, $G_5 \cdots < 0$ by simple calculation. Thus, the lower bound Y_2^L is obtained by our setting $Y_4 = Y_5 = \cdots = 0$ from Eq. (D4) since $Y_k \in [0,1]$ (see Ref. [59]):

$$Y_2^L = \frac{2\{[2\omega(2\nu)^3 - 2\nu(2\omega)^3][2\tau(e^{2\omega}Q_\omega - Q_0) - 2\omega(e^{2\tau}Q_\tau - Q_0)] - [2\tau(2\omega)^3 - 2\omega(2\tau)^3][2\omega(e^{2\nu}Q_\nu - Q_0) - 2\nu(e^{2\omega}Q_\omega - Q_0)]\}}{[2\omega(2\nu)^3 - 2\nu(2\omega)^3][2\tau(2\omega)^2 - 2\omega(2\tau)^2] - [2\tau(2\omega)^3 - 2\omega(2\tau)^3][2\omega(2\nu)^2 - 2\nu(2\omega)^2]}. \tag{D6}$$

The upper bound of the phase error rate is

$$E_\mu^{X,U} = 1 - e^{-2\mu}\frac{Y_0}{Q_\mu} - e^{-2\mu}\frac{(2\mu)^2}{2}\frac{Y_2^L}{Q_\mu}. \tag{D7}$$

Thus, the lower bound of the key-generation rate for three-party PM QCC is

$$\begin{aligned} R_{\text{three-party}} &\geq R^L_{\text{three-party}} \\ &= \left(\frac{2}{M}\right)^2 Q_\mu\{1 - f \times \max[H(E^Z_{\mu,P_1P_2}), \\ &\quad H(E^Z_{\mu,P_1P_3})] - H(E_\mu^{X,U})\}. \end{aligned} \tag{D8}$$

The above decoy-state method can be directly generalized to PM-QCC protocols with $N \geq 4$ parties. For $N \geq 4$ parties, more linear constraints are needed to tightly estimate the phase error rate E_μ^X shown in Eq. (D10b). Specifically, on the basis of the structure of the N-party GHZ state, there are more than two interference branches in the virtual protocol in Fig. 5(b). If some of the branches have no photons, the corresponding yield Y_k will be rather small. Thus, to obtain a tight upper bound of E_μ^X with Eq. (D2b), one needs more decoy states to estimate the high-order terms of the yield Y_k with the Gaussian-elimination method shown by Eqs. (D3)–(D6). The main steps to conduct the decoy-state method presented are as follows:

Step 1. For the N-party PM-QCC protocol, the randomized virtual source under phase-matching condition $\phi_1 = \phi_2 = \cdots = \phi_N = \phi$ is

$$\begin{aligned} \frac{1}{2\pi}\int_0^{2\pi} d\phi |e^{i\phi}\sqrt{\mu}\rangle_{C_1}\cdots|e^{i\phi}\sqrt{\mu}\rangle_{C_{N-1}}\langle e^{i\phi}\sqrt{\mu}|_{C_1}\cdots \\ \langle e^{i\phi}\sqrt{\mu}|_{C_{N-1}} = \sum_k^\infty P_{(N-1)\mu}(k)|k\rangle\langle k|, \end{aligned} \tag{D9}$$

where $P_{(N-1)\mu}(k) = e^{-(N-1)\mu}\{[(N-1)\mu]^k/k!\}$ is the probability of generating k photons in the virtual source, $|k\rangle = [(1/\sqrt{N-1})(C_1^\dagger + C_2^\dagger + \cdots + C_{N-1}^\dagger)]^k/\sqrt{k!}|\text{vac}\rangle$, and $k = n_1 + n_2 + \cdots + n_{N-1}$ is the total photon number of all the branches.

Step 2. The overall Q_μ [Eq. (C2a)] and phase error rate E_μ^X [Eq. (B8)] are

$$Q_\mu = \sum_k^\infty P_{(N-1)\mu}(k)Y_k, \tag{D10a}$$

$$\begin{aligned} E_\mu^X &= \sum_{k\in\text{odd}} P_{(N-1)\mu}(k)\frac{Y_k}{Q_\mu} \\ &= 1 - \sum_{k\in\text{even}} P_{(N-1)\mu}(k)\frac{Y_k}{Q_\mu} \\ &= 1 - e^{-(N-1)\mu}\frac{Y_0}{Q_\mu} - e^{-(N-1)\mu}\frac{[(N-1)\mu]^2}{2}\frac{Y_2}{Q_\mu} \\ &\quad - \cdots \\ &\leq 1 - e^{-(N-1)\mu}\frac{Y_0}{Q_\mu} - e^{-(N-1)\mu}\frac{[(N-1)\mu]^2}{2}\frac{Y_2}{Q_\mu} \\ &\quad - \cdots \\ &\quad - e^{-(N-1)\mu}\frac{[(N-1)\mu]^{N_{\text{cut}}}}{N_{\text{cut}}!}\frac{Y_{N_{\text{cut}}}}{Q_\mu} \\ &\leq E_\mu^{X,U} = 1 - e^{-(N-1)\mu}\frac{Y_0}{Q_\mu} \\ &\quad - e^{-(N-1)\mu}\frac{[(N-1)\mu]^2}{2}\frac{Y_2^L}{Q_\mu} - \cdots \\ &\quad - e^{-(N-1)\mu}\frac{[(N-1)\mu]^{N_{\text{cut}}}}{N_{\text{cut}}!}\frac{Y^L_{N_{\text{cut}}}}{Q_\mu}, \end{aligned} \tag{D10b}$$

where N_{cut} is the cut number to bound the phase error rate, and $N_{\text{cut}} = N - 1$ (N) if N is odd (even)

Step 3. The Gaussian-elimination method shown in Eqs. (D3)–(D6) is used to estimate the lower bounds $Y_2^L, \ldots, Y^L_{N_{\text{cut}}}$. To estimate the high-order terms Y_k^L, one needs to add extra linear constraints to Eq. (D3) by adding extra decoy states, say, $\{\nu, \omega, \tau, \ldots, 0\}$, to construct Eq. (D4). Then, one can directly obtain the high-order terms Y_k^L from Eq. (D4).

Step 4. With the lower bounds $Y_2^L, \ldots, Y_{N_{\text{cut}}}^L$, one can obtain the upper bound of the phase error rate $E_\mu^{X,U}$ according to Eq. (D10b).

From the view of linear programming, to well bound the yield $Y_{N_{\text{cut}}}$, $N_{\text{cut}} + 1$ linear constraints are needed for the Gaussian-elimination method. Thus, the number of decoy sates increases linearly with the number of communication parties N in the decoy-state method presented. On the other hand, if one uses the decoy-state estimation using the data when different parties send out different intensities, one can generate more decoy-state constraints for Eq. (D3). In this case, when the number of parties N gets larger, the number of constraints also increases. This has already been studied in quantum key distribution; see for example, Refs. [41,43]. From this point of view, when N gets larger, one may not need more decoy states for each party. Similar problems have been solved in a different scenario in Ref. [60], where a few decoy-state settings are enough to generate a good estimation of the yield when each of the N parties sends out one photon. Thus, with a more-advanced decoy-state method, it is possible to reduce the required decoy-state number for each party.

APPENDIX E: PM QCC* WITHOUT PHASE POSTSELECTION FOR THE SIGNAL PULSES

As stated in Appendix B, if we can estimate the phase error accurately, the PM-QCC protocol is still secure even when the phase choices for the signal pulses are announced before Eve's measurement. Without loss of generality, the phase choices for signal pulses of party P_i can be set to $\phi_i = 0$. The PM-QCC* protocol without phase postselection for the signal pulses is as follows:

Step 1. Preparation. The pulses are divided into a signal mode with intensity μ and a decoy mode with intensities $\{\nu, \omega, \tau, \ldots, 0\}$. In the signal mode, party P_1 randomly generates one bit $k_1 \in \{0, 1\}$ and a coherent pulse $|\sqrt{\mu_1}\rangle$. Then, he encodes the random bit in the coherent pulse and gets an encoded coherent pulse $|e^{i\pi k_1}\sqrt{\mu_1}\rangle$. Similarly, parties $P_2, \ldots, P_N$ get encoded coherent pulses $|e^{i\pi k_2}\sqrt{\mu_2}\rangle, \ldots, |e^{i\pi k_N}\sqrt{\mu_N}\rangle$, respectively. In the decoy mode, party P_1 randomly generates one bit $k_1 \in \{0, 1\}$ and a coherent pulse with random phase $\phi_1 \in [0, 2\pi)$. Then, he encodes the random bit in the coherent pulse and gets a phase-randomized coherent pulse $|e^{i(\phi_1+\pi k_1)}\sqrt{\mu_1}\rangle$. Similarly, parties $P_2, \ldots, P_N$ prepare their phase -randomized coherent pulses $|e^{i(\phi_2+\pi k_2)}\sqrt{\mu_2}\rangle, \ldots, |e^{i(\phi_N+\pi k_N)}\sqrt{\mu_N}\rangle$, respectively.

As shown in Fig. 1, the experimental setup is asymmetric for parties P_1, P_N, and $P_2, \ldots, P_{N-1}$. Thus, the intensities of the weak coherent pulses for parties P_1 and P_N are set to be μ_1 and $\mu_N \in \{\mu/2 > \nu/2 > \frac{\omega}{2} > \tau/2 > \cdots > 0\}$, while the intensities for parties $P_2, \ldots, P_{N-1}$ are set to be $\mu_t \in \{\mu > \nu > \omega > \tau > \cdots > 0\}$ $(2 \le t \le N-1)$ for signal and decoy pulses. The corresponding pulses with intensity μ are signal pulses and the corresponding pulses with intensities $\{\nu, \omega, \tau, \ldots, 0\}$ are used as decoy pulses.

Step 2. Measurement. Same as for PM QCC.

Step 3. Announcement. Same as for PM QCC.

Step 4. Sifting. Same as for PM QCC.

Step 5. Parameter estimation and key distillation. The above steps are repeated enough times to distill the raw-key bits. From the data set generated by the signal pulses, the users can directly estimate the gain Q_μ^* and marginal QBERs $E_{\mu,P_1P_2}^{Z*}$, $E_{\mu,P_1P_3}^{Z*}, \ldots, E_{\mu,P_1P_N}^{Z*}$ from the measurement results. From the data set generated by the decoy pulses, the users can estimate the phase error E_μ^{X*} according to decoy-state methods. Finally, they distill private-key bits by performing error correction and privacy amplification on the raw key.

According to Appendix D, the decoy states are simultaneously randomized under the phase-matching condition, and the above-mentioned decoy-state method can be directly used to estimate the phase error E_μ^X in the signal mode for the PM-QCC protocol. However, in the PM-QCC* protocol the signal pulses from the parties can no longer be regarded as photon-number states since the phase randomization for signal pulses has been canceled out. Thus, the preceding discussion of decoy states becomes unsuitable for the PM-QCC* protocol, and a more-delicate decoy-state method is required to evaluate the phase error rate for the signals [39,41,42]. For example, as in Ref. [41], the estimation of the phase error rate is converted to the estimation of the yields for the photon-number state, which can be estimated using phase-randomized decoy states. Thus, the phase-randomized decoy states with different intensities can, in principle, be used to constrain the phase error rate E_μ^X tightly, and we leave this for further studies. The gain $Q_{\mu,1}^*$ of branch 1 is

$$Q_{\mu,1}^* = Q_{\mu,1}, \tag{E1}$$

and the QBER is

$$\begin{aligned} E_\mu^{Z*,1} &= \frac{P(D_{R_1})}{P(D_{L_1}) + P(D_{R_1})} \\ &= \frac{(1-p_d)(e^{-\eta\mu(1-e_\delta)})[1-(1-pd)(e^{-\eta\mu e_\delta})]}{Q_{\mu,1}^*}, \end{aligned} \tag{E2}$$

where e_δ is the phase misaligned error for the signal mode during the phase reference. From Eqs. (C2a), (C2b), and

(B8), the overall gain, marginal QBERs, and phase error are

$$Q_\mu^* = Q_\mu, \tag{E3a}$$

$$E_{\mu,P_1P_m}^{Z*} = \sum_{k=0}^{\lfloor (m-2)/2 \rfloor} C_{m-1}^{2k+1} (E_\mu^{Z*,1})^{2k+1} (1 - E_\mu^{Z*,1})^{m-2k-2}, \tag{E3b}$$

$$E_\mu^{X*} = E_\mu^X. \tag{E3c}$$

According to a former discussion on PM QKD [39], one can simply suppose that a sufficient parameter estimation can be made by a complete characterization of Eve's measurement operators. As a result, the estimated phase error rate E_μ^{X*} is equal to the detected fraction of the odd-photon-number component in the infinite-key regime. Then, the key-generation rate for the PM-QCC protocol without the phase-matching condition for signal modes is

$$R_{N\text{-party}}^* = Q_\mu^* \{1 - f \times \max[H(E_{\mu,P_1P_2}^{Z*}), H(E_{\mu,P_1P_3}^{Z*}), \ldots, H(E_{\mu,P_1P_N}^{Z*})] - H(E_\mu^{X*})\}. \tag{E4}$$

APPENDIX F: COMPARISON WITH MDI QCC

We compare the performance of PM QCC with that of MDI QCC in Ref. [17] when $N = 3$. The key rate of MDI QCC in the simulation is

$$R_{\text{MDI QCC}} = Q_{111}^Z [1 - H(e_{111}^{BX})] - H(E_{\mu\nu\omega}^{Z*}) f Q_{\mu\nu\omega}^Z, \tag{F1}$$

where $E_{\mu\nu\omega}^{Z*} = \max[H(E_{\mu\nu\omega}^{ZAB}), H(E_{\mu\nu\omega}^{ZAC})]$, $Q_{\mu\nu\omega}^Z (E_{\mu\nu\omega}^{Z*})$ is the gain (QBER) of the Z basis, Q_{111}^Z is the gain of the single-photon component, e_{111}^{BX} is the single-photon QBER of the X basis, f is the error-correction efficiency, and $H(x) = -x \log_2 x - (1-x)\log_2(1-x)$ is the binary entropy function.

From Eq. (C2a), one can obtain $Q_\mu \propto \eta^{N-1}$, where $\eta = e^{-\alpha L/10}$ is the transmission rate of the optical channel, where α is the corresponding loss rate and L is the distance from each party to the measurement station. Thus, the key-generation rate $R_{\text{PM QCC}} \propto \eta^{N-1}$. Nevertheless, in MDI QCC [17], one can calculate that $Q_{111}^Z \propto \eta^3$ when the dark-count rate $p_d = 0$. Intuitively, N photons are coincidentally detected by N different detectors for N-party MDI-QCC networks based on the GHZ-state analyzer [29] with coincidence probability $P_{\text{co}} \propto \eta^N$. Then, we obtain $R_{\text{MDI QCC}} \propto \eta^N$ according to Eq. (F1). Therefore, the PM-QCC presented can improve the key-generation rate from $O(\eta^N)$ to $O(\eta^{N-1})$.

APPENDIX G: REDUCTION TO SMALL-SCALE PM-QCC NETWORKS

Practically, the N-party PM-QCC network might not work perfectly (i.e., there might not be perfect N-party interferences of the weak coherent states). We consider the case where N'-party inferences (N' parties are near-neighbor connected, and $2 \le N' \le N$) are realized in some rounds of the N-party PM-QCC network. For example, as shown in Fig. 6(a), only the interferences of sets $\{P_1, P_2, P_3\}$ and $\{P_4, P_5\}$ are realized, while the interference of $\{P_3, P_4\}$ failed in the five-party PM-QCC network. According to step 1 of the PM-QCC network, the coherent pulses sent by parties at the broken point are $|\sqrt{\mu}\rangle$ instead of $|\sqrt{\mu/2}\rangle$ (here we omit the phase information). Considering asymmetric mean photon numbers for two arms of an interference branch, we show that reduced small-scale PM-QCC networks and the PM-QKD protocol can also be realized securely.

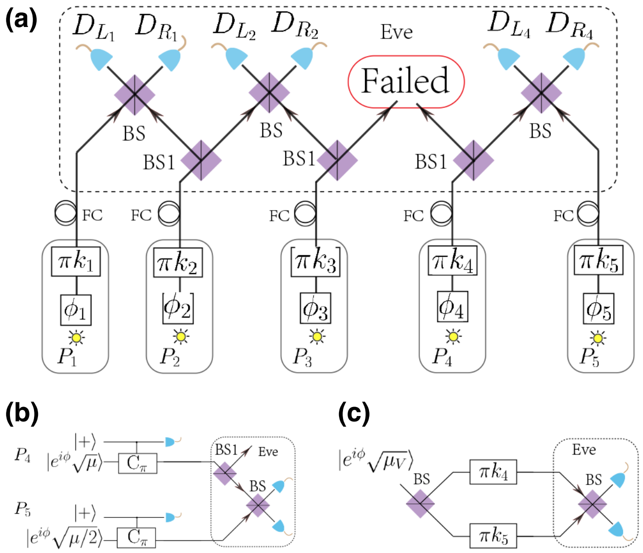

FIG. 6. (a) The three-party PM-QCC network and the two-party PM-QKD protocol reduced from the five-party PM-QCC network. In some rounds of the five-party PM-QCC network only sets $\{P_1, P_2, P_5\}$ and $\{P_4, P_5\}$ have successfully interference, while the interference of $\{P_3, P_4\}$ failed. (b) The entanglement-based PM-QKD protocol for parties P_4 and P_5. (c) The equivalent entanglement-based PM-QKD protocol for P_4 and P_5 with a virtual source. BS, beam splitter; FC, fiber channel; C_π, controlled phase gate.

Without loss of generality, we consider the interference of parties P_4 and P_5 as shown in Fig. 6(b). The virtual entanglement-based PM-QKD protocol with a virtual weak-coherent-state source $|e^{i\phi}\sqrt{\mu_V}\rangle$ ($\mu_V = \mu_a + \mu_b$) is shown in Fig. 6(c). For the small-scale PM-QCC network and PM-QKD protocol described above, the average numbers of photons for parties at the boundary are not equal. The weak coherent pulses after encoding of parties P_4 and P_5 are $|e^{i\phi_a}\sqrt{\mu_a}\rangle$ and $|e^{i\phi_b}\sqrt{\mu_b}\rangle$, respectively, with $\mu_a = \mu$ and $\mu_b = \mu/2$. As shown in Fig. 6(b), the weak coherent states arriving for interference are equal; that is, $|e^{i\phi_a}\sqrt{\eta_a\mu_a}\rangle$ and $|e^{i\phi_b}\sqrt{\eta_b\mu_b}\rangle$, with $\eta_a\mu_a = \eta_b\mu_b = \eta\mu/2$. According to Eqs. (C4)–(C9), the gain and QBER of this

TABLE II. Performance of the reduced three-party PM-QCC network shown in Fig. 6(a). The key-generation rate R, mean photon number μ, and phase-slice number M are optimized with $p_d = 7.2 \times 10^{-8}$, $\eta_d = 65\%$, $f = 1.16$, and $\alpha = 0.2$ dB/km at different transmission distances L.

$R_{\text{reduced three-party}}$ (bits per pulse)	L (km)	μ	M
1.7060×10^{-7}	50	0.1059	13
1.6152×10^{-9}	100	0.1032	13

branch with a asymmetric average number of photons are equal to those of the original branch:

$$\begin{aligned} Q^{'}_{\mu_{\text{V}},1} &= Q_{\mu,1}, \\ E^{'Z,1}_{\mu_{\text{V}},1} &= E^{Z,1}_{\mu}. \end{aligned} \tag{G1}$$

Meanwhile, higher numbers of weak coherent pulses are lost during the transmission. This will result in a lower key-generation rate for a small-scale PM-QCC network or the PM-QKD protocol, which is embodied in the estimation of E^X_μ from Eq. (B8). Specifically, we present the performance of the three-party PM-QCC network reduced from the five-party PM-QCC network shown in Fig. 6(a) in Table II. In practice, the coherent pulses and phase slices M might be preoptimized for a bigger PM-QCC network, and the key-generation rate for the reduced three-party PM-QCC network might decrease to a lower level compared with the results in Table II. However, according to Eq. (G1), the gain of this asymmetric branch still scales with $Q^{'}_{\mu_{\text{V}},1} \propto \eta$. Thus, a key-generation rate that scales with $R_{\text{reduced PM QCC}} \propto \eta^{N'-1}$ can also be obtained according to Eq. (B9) for the N'-party PM-QCC network.

Therefore, the N-party PM-QCC network can be reduced to small-scale PM-QCC networks and PM-QKD protocols when only some of the N parties interfere.

[1] C. Elliott, Building the quantum network, New J. Phys. **4,** 46 (2002).

[2] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, in *Quantum Inf. Comput. III*, edited by E. J. Donkor, A. R. Pirich, and H. E. Brandt, International Society for Optics and Photonics (SPIE, Orlando, Florida, United States, 2005), Vol. 5815, p. 138.

[3] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes *et al.*, The SECOQC quantum key distribution network in vienna, New J. Phys. **11,** 075001 (2009).

[4] F. Xu, W. Chen, S. Wang, Z. Yin, Y. Zhang, Y. Liu, Z. Zhou, Y. Zhao, H. Li, D. Liu, *et al.*, Field experiment on a robust hierarchical metropolitan quantum cryptography network, Chin. Sci. Bul. **54,** 2991 (2009).

[5] D. Stucki, M. Legré, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, *et al.*, Long-term performance of the SwissQuantum quantum key distribution network in a field environment, New J. Phys. **13,** 123001 (2011).

[6] H. J. Kimble, The quantum internet, Nature **453,** 1023 (2008).

[7] S.-K. Liao, W.-Q. Cai, J. Handsteiner, B. Liu, J. Yin, L. Zhang, D. Rauch, M. Fink, J.-G. Ren, W.-Y. Liu, *et al.*, Satellite-Relayed Intercontinental Quantum Network, Phys. Rev. Lett. **120,** 030501 (2018).

[8] S. Wehner, D. Elkouss, and R. Hanson, Quantum internet: A vision for the road ahead, Science **362,** 6412 (2018).

[9] M. Caleffi, A. S. Cacciapuoti, and G. Bianchi, in *Proceedings of the 5th ACM International Conference on Nanoscale Computing and Communication*, NANOCOM '18 (Association for Computing Machinery, New York, NY, USA, 2018).

[10] D. Castelvecchi, The quantum internet has arrived (and it hasn't), Nature **554,** 289 (2018).

[11] A. Steane, Quantum computing, Rep. Pro. Phys. **61,** 117 (1998).

[12] N. Gisin and R. Thew, Quantum communication, Nat. Photon. **1,** 165 (2007).

[13] V. Giovannetti, S. Lloyd, and L. Maccone, Quantum Metrology, Phys. Rev. Lett. **96,** 010401 (2006).

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

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

[16] K. Chen and H.-K. Lo, in *Proceedings of the 2005 IEEE International Symposium on Information Theory* (IEEE, Adelaide, Australia, 2005), p. 1607.

[17] 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).

[18] F. Grasselli, H. Kampermann, and D. Bru, Conference key agreement with single-photon interference, New J. Phys. **21,** 123002 (2019).

[19] G. Murta, F. Grasselli, H. Kampermann, and D. Bru, Quantum conference key agreement: A review, arXiv:2003.10186 (2020).

[20] D. M. Greenberger, M. A. Horne, and A. Zeilinger, in *Bell's Theorem, Quantum Theory and Conceptions of the Universe*, edited by M. Kafatos (Kluwer Academic, Dordrecht, 1989), pp. 69.

[21] J. S. Bell, On the einstein podolsky rosen paradox, Physics **1,** 195 (1964).

[22] N. Brunner, D. Cavalcanti, S. Pironio, V. Scarani, and S. Wehner, Bell nonlocality, Rev. Mod. Phys. **86,** 419 (2014).

[23] M. Bourennane, M. Eibl, S. Gaertner, N. Kiesel, C. Kurtsiefer, M. Żukowski, and H. Weinfurter, Multiphoton entanglement and interferometry, Fortschritte der Physik: Progress Phys. **51,** 273 (2003).

[24] J.-W. Pan, Z.-B. Chen, C.-Y. Lu, H. Weinfurter, A. Zeilinger, and M. Żukowski, Multiphoton entanglement and interferometry, Rev. Mod. Phys. **84,** 777 (2012).

[25] T. Monz, P. Schindler, J. T. Barreiro, M. Chwalla, D. Nigg, W. A. Coish, M. Harlander, W. Hänsel, M. Hennrich, and

R. Blatt, 14-Qubit Entanglement: Creation and Coherence, Phys. Rev. Lett. **106**, 130506 (2011).

[26] X.-L. Wang, L.-K. Chen, W. Li, H.-L. Huang, C. Liu, C. Chen, Y.-H. Luo, Z.-E. Su, D. Wu, Z.-D. Li, *et al.*, Experimental Ten-Photon Entanglement, Phys. Rev. Lett. **117**, 210502 (2016).

[27] C. Song, K. Xu, W. Liu, C.-P. Yang, S.-B. Zheng, H. Deng, Q. Xie, K. Huang, Q. Guo, L. Zhang, P. Zhang, D. Xu, D. Zheng, X. Zhu, H. Wang, Y.-A. Chen, C.-Y. Lu, S. Han, and J.-W. Pan, 10-Qubit Entanglement and Parallel Logic Operations with a Superconducting Circuit, Phys. Rev. Lett. **119**, 180511 (2017).

[28] X.-L. Wang, Y.-H. Luo, H.-L. Huang, M.-C. Chen, Z.-E. Su, C. Liu, C. Chen, W. Li, Y.-Q. Fang, X. Jiang, et al., 18-Qubit Entanglement with six Photons' Three Degrees of Freedom, Phys. Rev. Lett. **120**, 260502 (2018a).

[29] J. Qian, X.-L. Feng, and S.-Q. Gong, Universal greenberger-horne-zeilinger-state analyzer based on two-photon polarization parity detection, Phys. Rev. A **72**, 052308 (2005).

[30] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).

[31] S. L. Braunstein and S. Pirandola, Side-Channel-Free Quantum key Distribution, Phys. Rev. Lett. **108**, 130502 (2012).

[32] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).

[33] W. Dür, G. Vidal, and J. I. Cirac, Three qubits can be entangled in two inequivalent ways, Phys. Rev. A **62**, 062314 (2000).

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

[35] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum key Distribution, Phys. Rev. X **8**, 031043 (2018).

[36] K. Tamaki, H.-K. Lo, W. Wang, and M. Lucamarini, Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound, arXiv:1805.05511 (2018).

[37] X.-B. Wang, Z.-W. Yu, and X.-L. Hu, Twin-field quantum key distribution with large misalignment error, Phys. Rev. A **98**, 062323 (2018).

[38] C. Cui, Z.-Q. Yin, R. Wang, W. Chen, S. Wang, G.-C. Guo, and Z.-F. Han, Twin-Field Quantum key Distribution Without Phase Postselection, Phys. Rev. Appl. **11**, 034053 (2019).

[39] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, Phys. Rev. A **98**, 042332 (2018).

[40] Z.-W. Yu, X.-L. Hu, C. Jiang, H. Xu, and X.-B. Wang, Sending-or-not-sending twin-field quantum key distribution in practice, Sci. Rep. **9**, 3080 (2019).

[41] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, Npj Quantum Inf. **5**, 64 (2019).

[42] K. Maeda, T. Sasaki, and M. Koashi, Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit, Nat. Commun. **10**, 1 (2019).

[43] F. Grasselli and M. Curty, Practical decoy-state method for twin-field quantum key distribution, New J. Phys. **21**, 073001 (2019).

[44] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).

[45] 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).

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

[47] Y. Liu, Z.-W. Yu, W. Zhang, J.-Y. Guan, J.-P. Chen, C. Zhang, X.-L. Hu, H. Li, C. Jiang, and J. Lin, *et al.*, Experimental Twin-Field Quantum key Distribution through Sending or not Sending, Phys. Rev. Lett. **123**, 100505 (2019).

[48] 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).

[49] X.-T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, Y.-L. Tang, Y.-J. Sheng, Y. Xiang, W. Zhang, H. Li, *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, Nat. Photonics **14**, 422 (2020).

[50] E. N. Maneva and J. A. Smolin, Improved two-party and multi-party purification protocols, Contemp. Math. 305, 203 (2002).

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

[52] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).

[53] P. W. Shor and J. Preskill, Simple Proof of Security of the bb84 Quantum key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).

[54] B. M. Terhal, Is entanglement monogamous? IBM J. Res. Dev. **48**, 71 (2004).

[55] M. Koashi and A. Winter, Monogamy of quantum entanglement and other correlations, Phys. Rev. A **69**, 022309 (2004).

[56] H.-L. Yin, T.-Y. Chen, Z.-W. Yu, H. Liu, L.-X. You, Y.-H. Zhou, S.-J. Chen, Y. Mao, M.-Q. Huang, W.-J. Zhang, *et al.*, Measurement-Device-Independent Quantum key Distribution Over a 404 km Optical Fiber, Phys. Rev. Lett. **117**, 190501 (2016).

[57] P. Zeng, W. Wu, and X. Ma, Symmetry-Protected Privacy: Beating the Rate-Distance Linear Bound Over a Noisy Channel, Phys. Rev. Appl. **13**, 064013 (2020).

[58] F. Xu, M. Curty, B. Qi, and H. K. Lo, Practical aspects of measurement-device-independent quantum key distribution, New J. Phys. **15**, 113007 (2013).

[59] X. Ma, Quantum cryptography: Theory and practice, arXiv:0808.1385v1 (2008).

[60] X. Yuan, Z. Zhang, N. Lütkenhaus, and X. Ma, Simulating single photons with realistic photon sources, Phys. Rev. A **94**, 062305 (2016).