Editors' Suggestion | Featured in Physics

Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution

Xiaoqing Zhong,[1,*] Jianyong Hu,[2,†] Marcos Curty,[3] Li Qian,[2] and Hoi-Kwong Lo[1,2]
[1]*Center for Quantum Information and Quantum Control, Department of Physics, University of Toronto, Toronto, Ontario, M5S 1A7, Canada*
[2]*Center for Quantum Information and Quantum Control, Department of Electrical and Computer Engineering, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*
[3]*EI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, E-36310 Vigo, Spain*

(Received 27 February 2019; revised manuscript received 8 May 2019; published 5 September 2019)

The twin-field (TF) quantum key distribution (QKD) protocol and its variants are highly attractive because they can beat the well-known fundamental limit of the secret key rate for point-to-point QKD without quantum repeaters (repeaterless bound). In this Letter, we perform a proof-of-principle experimental demonstration of TFQKD based on the protocol proposed by Curty, Azuma, and Lo, which removes the need for postselection on the matching of a global phase from the original TFQKD scheme and can deliver a high secret key rate. Furthermore, we employ a Sagnac loop structure to help overcome the major difficulty in the practical implementation of TFQKD, namely, the need to stabilize the phase of the quantum state over kilometers of fiber. As a proof-of-principle demonstration, the estimated secure key rate from our experimental TFQKD data at the high loss region surpasses the repeaterless bound of QKD with current technology.

DOI: 10.1103/PhysRevLett.123.100506

Introduction.—Quantum key distribution (QKD) [1–3] allows the distribution of secret keys between remote users with information-theoretic security [4–8]. Experimentally, QKD has been performed over 421 km of fiber [9], and over 1000 km of free space through satellite to ground links [10,11]. There is, however, a fundamental limit on the achievable secret key rate with QKD without intermediate nodes [12,13]. This limit, called the repeaterless bound in this Letter, states that the key rate scales basically linearly with the channel transmittance η.

To overcome this bound, besides using quantum repeaters [14–16], one could employ measurement-device-independent (MDI) QKD [17] together with quantum memories [18,19] or quantum nondemolition measurements [20]. While promising, these approaches are, however, far away from our current experimental capabilities. Remarkably, more recently, a new type of QKD, so-called twin-field (TF) QKD, has been proposed [21] which can beat the repeaterless bound with one untrusted intermediate node (Charlie) performing a simple interferometric measurement. This advantage suggests the feasibility of intercity QKD with today's technology. While the original TFQKD was proven to be secure against some restricted attacks by Eve, variations of TFQKD have been proven to be secure against general attacks [22–28]. In TFQKD, two users (Alice and Bob) send two optical fields to produce a single-photon interference at Charlie. The fact of using singles (i.e., single-photon detection events) results in a secret key rate that scales as $\sqrt{\eta}$ because, now, only one photon (either from Alice or from Bob) has to arrive at Charlie. Importantly, since TFQKD has a similar structure as MDIQKD, it is also immune to detector side-channel attacks and is particularly suited for star networks [17–20,29–33]. In summary, now that the security of TFQKD has been firmly established, it is essential to investigate its experimental feasibility, especially because TFQKD requires long-distance subwavelength path-length phase stability.

The first proof-of-principle experimental demonstration of TFQKD has been done very recently [34] and shows the feasibility of overcoming the repeaterless key rate bound. In this Letter, we perform another proof-of-principle experimental implementation of the TFQKD protocol introduced by Curty *et al.* [26]. In contrast to the work in Ref. [34], our scheme is a two-way QKD system consisting of a Sagnac interferometer, which could help overcome the main practical challenge in implementing TFQKD, namely, maintaining long-term phase stability between the coherent states sent from Alice and Bob. The Sagnac-like interferometer has been exploited in QKD systems in Refs. [35,36] and, also, has been theoretically applied in a TFQKD protocol [28]. It is similar to the plug-and-play system that is widely used in QKD [37,38] and is the workhorse of a widely deployed commercial QKD system (ID Quantique). Security proofs for such plug-and-play QKD systems have been developed in [39,40]. Here, we experimentally demonstrate that the Sagnac interferometer configuration can achieve phase stability in a

practical TFQKD system. The common-path nature of the Sagnac loop automatically compensates for phase fluctuations of the two fields from Alice and Bob, which enables us to perform TFQKD with >10 km of actual fibers between Alice and Bob, in contrast to the results reported in [34] where the fiber is only around 40 meters. The protocol we adopt [26] does not need a post-selection step based on the matching of a global phase and can deliver a high secret key rate. The key idea is using coherent states for key generation and photon number states as the complementary basis to prove security [8]. The latter type of states can be simulated by means of phase-randomized coherent states in combination with the decoy-state method [41–44].

Protocol and experiment.—The TFQKD protocol introduced in [26] is composed of the following five steps.

Step 1: Alice and Bob each prepare a weak coherent state, choosing the X basis with probability P_X and the Z basis with probability $P_Z = 1 - P_X$. If the X basis is chosen, Alice (Bob) randomly prepares a coherent state $|\alpha\rangle_A$ ($|\alpha\rangle_B$) for the bit value $b_A = 0$ ($b_B = 0$) or $|-\alpha\rangle_A$ ($|-\alpha\rangle_B$) for the bit value $b_A = 1$ ($b_B = 1$). If the Z basis is chosen, Alice (Bob) prepares a phase-randomized coherent state

$$\rho_A = \frac{1}{2\pi}\int_0^{2\pi} d\varphi_A |\beta_A e^{i\varphi_A}\rangle_A\langle\beta_A e^{i\varphi_A}| \tag{1}$$

(ρ_B has the same expression as (1) with all subscripts changed to B). The intensity $|\beta_A|^2$ ($|\beta_B|^2$) is chosen at random from a set $S = \{\mu, \nu, \omega\}$.

Step 2: Alice and Bob send their states to the middle node, Charlie, through optical channels with transmittance $\sqrt{\eta}$.

Step 3: On Charlie's station, the incoming states interfere with each other at a 50:50 beam splitter followed by two single-photon detectors, D_0 and D_1. Each detector click at the expected arrival time slot is recorded.

Step 4: At the end of the quantum communication phase, Charlie announces all the results obtained, and Alice and Bob declare the bases used.

Step 5: Based on the information announced, Alice and Bob estimate the bit and phase error rate and distill secret keys from those instances where they used X basis and Charlie declared one detection click. More precisely, whenever Charlie reports one click event in say D_0 (D_1) and both Alice and Bob choose the X basis, b_A and b_B ($b_B \oplus 1$) are regarded as their raw keys.

In our implementation (Fig. 1), Charlie produces weak coherent pulses (900 ps FWHM, 10 MHz) from a continuous-wave distributed feedback laser (1552.6 nm) using an intensity modulator (IM) followed by an attenuator (ATT), and distributes the pulses to Alice and Bob, providing a phase reference to all three parties. The pulses go through an optical circulator and enter the Sagnac loop through a 50:50 fiber-based beam splitter (BS). Clockwise

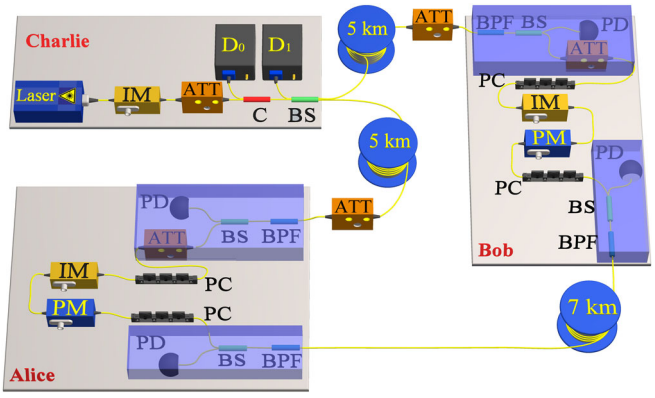

FIG. 1. Schematic experimental setup of twin-field quantum key distribution based on Sagnac interferometer. Charlie distributes unmodulated weak coherent pulses to Alice and Bob, ensuring a common phase reference without active stabilization. The clockwise (counterclockwise) traveling pulses are modulated by Alice's (Bob's) phase modulator (PM) and intensity modulator (IM), before looping back to Charlie, interfering at Charlie's beam splitter (BS), and detected by two single photon detectors D_0 and D_1. Note that the components in the translucent blue areas on both Alice's and Bob's stations are not experimentally implemented but should be added to enhance security. ATT: attenuator; C: circulator; BPF: bandpass filter; PD: photodiode; PC: polarization controller.

(counterclockwise) traveling pulses go through a 5-km fiber spool (only in one case), an ATT, and Bob's (Alice's) station, without being modulated. Therefore, no information is directly communicated between Alice and Bob. Then the pulses travel through a 7-km fiber spool (with 7 dB loss) separating Alice and Bob, and reach Alice's (Bob's) station. On Alice's (Bob's) station, the clockwise (counterclockwise) pulses are modulated by a phase modulator (PM) and an IM, which sets the intensity of the pulse to either $|\alpha|^2$ or one from the set $S = \{\mu, \nu, \omega\}$. A high-speed arbitrary waveform generator (AWG, Keysight M8195A) with multiple output channels provides the rf signals to all the modulators on Alice's, Bob's, and Charlie's stations. The AWG channels are synchronized by its internal clock and the delay time between any two channels can be adjusted. After the phase and intensity modulations, Alice (Bob) sends the pulses to Charlie through the ATT and the 5-km fiber spool (only in one case). The ATT is used here to simulate the loss due to the communication channel. The pulses from Alice and Bob interfere at Charlie's BS, with one output directed to a single-photon detector (SPD) D_0 via the circulator, and the other output followed directly by another SPD, D_1. The SPDs are commercial free-run avalanche photodiodes (ID220) with an efficiency of 11.7% and a dark count rate of about 7×10^{-7} (per 900 ps gate window). Charlie records each click event within the gate window and publicly announces the result. Afterward, Alice and Bob declare their bases choices and select the single-detection

events where they both use the X basis to distill a secure secret key.

As a proof-of-principle demonstration, we primarily focus on the feasibility of TFQKD implementation, rather than aiming for a complete system with all necessary hardware. For example, as indicated in the translucent blue areas on both Alice's and Bob's stations (Fig. 1), the attenuators are used for attenuating the pulses traveling from Alice (Bob) back to Charlie to single photon level. The taps, photodiodes (PD), and bandpass filters (BPFs) are necessary for Alice and Bob to detect and limit strong optical injections from the outside, so as to prevent eavesdroppers from probing the sources. These monitors and filters are not implemented due to resource limitations, but they can be added to our current system without invalidating any of the experimental results we have obtained.

It is crucial to ensure that Alice (Bob) only modulates the clockwise (counterclockwise) traveling pulses. This is achieved by using appropriate fiber lengths between the three parties, so that the two counterpropagating pulses never overlap with each other at any modulator. Note that this is not a practical limitation, since Alice and Bob can always add or remove small lengths of fiber within their own setup to avoid "pulse collision." As in any practical system, there are reflections and backscattering from the channel, causing unintended "clicks" in the detectors. Fortunately, Alice and Bob can adjust fiber lengths and move the unintended clicks outside the signal detection window.

A number of fiber-based polarization controllers are installed inside the Sagnac loop (see Fig. 1) to ensure that the interfering pulses are aligned in polarization. To maintain polarization stability, all fiber spools are stored in sealed boxes. Polarization alignment is done before each 40-minute QKD session, and no active polarization stabilization is applied during the QKD session. Owing to both phase and polarization stability, the interference visibility of our system is kept above 99% (for the X basis) for the 40-minute QKD session, as shown in Fig. 2(a). When the 5-km fiber spools are taken out, the system is more stable and the average interference visibility is about 99.8%. With fiber spools in the system, the interference visibility is slightly lower. We attribute this degradation of the visibility to polarization fluctuations and depolarization effects, as well as low levels of Rayleigh backscattering in long fiber spools. Nonetheless, the interference visibility with fiber spools is still stable at about 99.7%. When a random phase is applied (to a decoy state signal), equal probability of detection at D_0 and D_1 is expected, as, indeed, observed [Fig. 2(b)]. Both cases (with and without the 5-km fiber spools) maintain a stable ratio close to 1, which indicates that phase randomization has been effectively implemented.

Results.—We implement the experiment for four different values of the overall system loss between Alice and Bob,

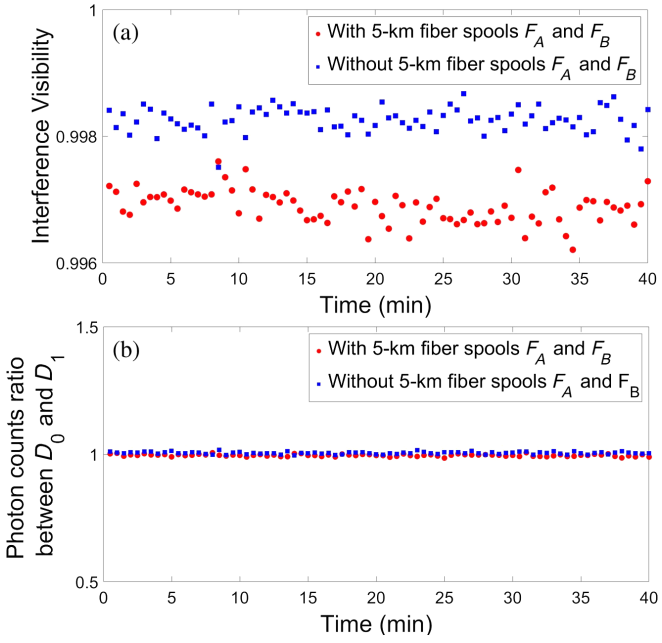

FIG. 2. System performance when Alice (Bob) and Charlie are connected through attenuators only (blue squares), and when 5-km fiber spools are added between Alice, Bob, and Charlie (red circles). (a) Interference visibility of the system over 40 minutes. Each data point is obtained using 30 seconds of detector integration time. (b) Ratio of the total number of photon counts between detector D_0 and detector D_1 over 40 minutes when phase randomization is applied. The total photon counts at detector D_0 is calibrated to compensate for the loss in the circulator.

38.0, 46.7, 49.4, and 55.1 dB, respectively. For the 49.4 dB loss, a 5-km fiber spool (about 1.2 dB of loss) is inserted between Alice (Bob) and Charlie in addition to the ATT to demonstrate the practicality of our scheme. The detector efficiency (11.7%) is equivalently attributed as part of the total loss in the Alice-Charlie-Bob link, as our low-efficiency detector can be modeled as a loss element followed by a high-efficiency detector and the interference signals go through this loss element before being detected. In practice, this implies that the use of higher efficiency detectors would result in an enhancement of the maximum transmission distance. For different values of the system loss, we choose different optimal intensity sets $\{|\alpha|^2, \mu, \nu, \omega\}$, as shown in Table I. For each value of the system loss and each intensity pair, Alice and Bob each send 3×10^9 coherent pulses. The quantum bit error rates (QBERs) observed in both detectors D_0 and D_1 are also listed in Table I. Given the high stability of the system and the high interference visibility, the QBERs observed in the experiment are correspondingly low. Even the maximum QBER observed at the highest system loss is lower than 1.2%. More experimental data, such as the experimentally observed gains, can be found in the Supplemental Material [45].

To estimate the secret key rate, we use the security analysis and secret key rate formula reported in [26,46] (see Supplemental Material [45]) and the results for different

TABLE I. List of intensity sets and experimental results for four different values of the overall system loss. $|\alpha|^2$ is the average photon number of the coherent pulse in X basis. μ, ν, and ω are the average photon number (per pulse) of the decoy states in Z basis. The uncertainty of each intensity refers to the measurement of its statistical fluctuation. QBER is the experimental quantum bit error rate. The experimental secret key rate includes three cases, i.e., the case where intensity fluctuations are disregarded (R_{mean}) and the worst (R_{min}) and best (R_{max}) case scenarios where intensity fluctuations are taken into account. For comparison purposes, the repeaterless bound introduced in Ref. [13] is also listed. *: 5-km fiber spools are inserted.

Loss	Fiber inserted*	Intensities				QBER		Experimental secret key rates			Repeaterless bound
		$\|\alpha\|^2$	μ	ν	ω	D_0	D_1	R_{mean}	R_{min}	R_{max}	
38.0 dB	No	0.0256±0.0001	0.087±0.001	0.0088±0.0002	$(1.0\pm0.2)\times10^{-4}$	0.0032	0.0036	2.6484×10^{-4}	1.9917×10^{-4}	3.4765×10^{-4}	2.2867×10^{-4}
46.7 dB	No	0.02495±0.00005	0.0978±0.0008	0.0099±0.0001	$(7.5\pm0.2)\times10^{-5}$	0.0058	0.0032	7.8389×10^{-5}	6.9058×10^{-5}	8.8458×10^{-5}	3.0845×10^{-5}
49.4 dB	Yes	0.0183±0.0001	0.02005±0.00002	0.00828±0.00007	$(9.2\pm1.0)\times10^{-6}$	0.0059	0.0056	3.6306×10^{-5}	2.4061×10^{-5}	5.4130×10^{-5}	1.6564×10^{-5}
55.1 dB	No	0.0175±0.0002	0.0382±0.0004	0.00790±0.00007	$(6.5\pm1.0)\times10^{-5}$	0.0116	0.0108	1.7542×10^{-5}	1.0516×10^{-5}	2.5652×10^{-5}	4.4584×10^{-6}

system losses are given in Table I. For each value of the system loss, Table I includes three cases, i.e., the case where intensity fluctuations are disregarded and the worst- and best-case scenarios where intensity fluctuations are taken into account, which are indicated with the notation R_{mean}, R_{min}, and R_{max}, respectively. For the worst- and best-case scenarios, we numerically minimize and maximize the secret key rate formula among all possible values for the different intensities (within the reported experimental intensity fluctuations). Figure 3 shows the secure key rate (bits per pulse) in logarithmic scale as a function of the overall system loss between Alice and Bob. The dashed red line illustrates the repeaterless bound introduced in [13] and the solid green line corresponds to the theoretical simulation result [45].

As depicted in Fig. 3, the experimental secret key rates are reasonably close to the theoretical simulation results, except that the key rate at the system loss of 49.4 dB is slightly lower compared with the simulation result. This is because of the two 5-km fiber spools that are added in this case, which reduces interference visibility. Nonetheless, the experimental results, as expected, follow the rate-loss dependence of TFQKD, scaling with the square root of the channel transmittance. More importantly, the observed experimental key rate evidently surpasses the repeaterless bound as the overall system loss is larger than 40 dB, even when the minimum key rate in the worst-case scenario is considered. This achievement experimentally proves that TFQKD, with >10 km of actual fibers in the links, can beat the repeaterless bound at the high loss region.

Discussion.—As a proof-of-principle demonstration, we only implement one case with 5 km of actual fibers connecting Alice (Bob) and Charlie. As shown in Figs. 2 and 3, adding 5 km of fibers reduces the system performance. Hence, at this stage, we implement other loss points only with the attenuators to show that the secret key rate vs loss trend is consistent with the simulation. Note that the "automatic" phase stability of the Sagnac loop is only guaranteed when the phase of the loop ($(2\pi/\lambda)L$, L being the loop length) remains stable over the light transit time through half the loop. A simple estimation [47] suggests that this condition could be satisfied for 300 km of loop length. For much longer loops, active phase stabilization might be required.

Sagnac configuration does have unique challenges arising from the fact that Charlie needs to send strong optical pulses to Alice and Bob, particularly when the channel loss (between Charlie and Alice or Bob) is high. The strong optical pulses can result in high backscattering. Quantitative study on the effect of backscattering is beyond the scope of this work, and will be performed in the future. On the other hand, the loss in the channel directly linking Alice and Bob can be compensated through optical amplification, since this channel is "classical," and there is no information transmitted through it.

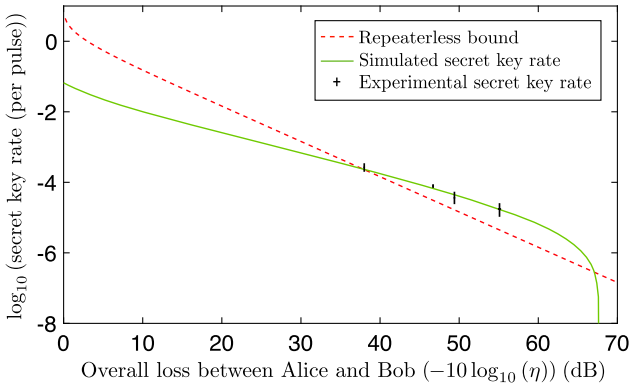

FIG. 3. Secret key rate (per pulse) versus the overall loss between Alice and Bob. Note that the single photon detector efficiency is included in the overall system loss. The experimental key rates shown in Table I are illustrated as black crosses. The vertical line of each cross shows the difference between the worst and best case scenarios when intensity fluctuations are considered. The horizontal line of each cross shows the uncertainty of the overall loss. The dashed red line illustrates the repeaterless bound introduced in [13]. The solid green line corresponds to a theoretical simulation result realized with the channel model introduced in [26]. The experimental results clearly demonstrate that the experiments performed beat the repeaterless bound at the high loss region.

In summary, we have experimentally implemented a proof-of-principle demonstration of a twin-field quantum key distribution scheme. Some related experiments of twin-field type QKD protocols have also been reported recently [50,51]. However, their experimental setups appear to be different from ours and require phase locking and active phase stabilization. Our scheme removes these requirements and employs a Sagnac loop as a passive way to achieve phase stabilization, which enables us to demonstrate TFQKD with actual fibers. The intensity fluctuations are also taken into consideration in our secret key analysis. The experimental secure key rate of the system scales as the square root of the overall channel transmittance. In particular, we have observed that the resulting secret key rate clearly beats the repeaterless bound when the overall system loss is larger than 40 dB. The use of actual fibers in our scheme, even if the fiber length is not significantly long, suggests the feasibility of overcoming the private capacity of a point-to-point QKD link with current experimental capabilities. Various issues including practical security, phase stability, and optical loss in long-distance implementations, as we have discussed above, deserve further investigations in the future.

We thank Olinka Bedroya and Shihan Sajeed for their assistance and enlightening discussions. We also acknowledge financial support from NSERC, CFI, ORF, U.S. Office of Naval Research, MITACS, Royal Bank of Canada, and Huawei Technologies Canada, Ltd. M. C. acknowledges support from the Spanish Ministry of Economy and Competitiveness (MINECO), the Fondo Europeo de Desarrollo Regional (FEDER) through Grants No. TEC2014-54898-R and No. TEC2017-88243-R, and the European Unions Horizon 2020 Research and Innovation Programme under the Marie Sklodowska-Curie Grant Agreement No. 675662 (Project QCALL).

*xzhong@physics.utoronto.ca
†Present address: Institute of Laser Spectroscopy, Shanxi University, Taiyuan, Shanxi 030006, China.
jyhusxu@gmail.com

[1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing, in *Proceedings of International Conference on Computers, Systems & Signal Processing, Bangalore, India* (1984), pp. 175–179.
[2] A. K. Ekert, Quantum Cryptography Based on Bells Theorem, Phys. Rev. Lett. **67**, 661 (1991).
[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Quantum cryptography, Rev. Mod. Phys. **74**, 145 (2002).
[4] D. Mayers, Unconditional security in quantum cryptography, J. Assoc. Comput. Mach. **48**, 351 (2001).
[5] H.-K. Lo and H. F. Chau, Unconditional security of quantum key distribution over arbitrarily long distances, Science **283**, 2050 (1999).
[6] P. W. Shor and J. Preskill, Simple Proof of Security of the BB84 Quantum Key Distribution Protocol, Phys. Rev. Lett. **85**, 441 (2000).
[7] E. Biham, M. Boyer, P. O. Boykin, T. Mor, and V. Roychowdhury, A proof of the security of quantum key distribution, J. Cryptol. **19**, 381 (2006).
[8] M. Koashi, Simple security proof of quantum key distribution based on complementarity, New J. Phys. **11**, 045018 (2009).
[9] A. Boaron *et al.*, Secure Quantum Key Distribution Over 421 km of Optical Fiber, Phys. Rev. Lett. **121**, 190502 (2018).
[10] S. K. Liao *et al.*, Satellite-to-ground quantum key distribution, Nature (London) **549**, 43 (2017).
[11] S. K. Liao *et al.*, Satellite-Relayed Intercontinental Quantum Network, Phys. Rev. Lett. **120**, 030501 (2018).
[12] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, Nat. Commun. **5**, 5235 (2014).
[13] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, Nat. Commun. **8**, 15043 (2017).
[14] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication, Phys. Rev. Lett. **81**, 5932 (1998).
[15] L. M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, Long-distance quantum communication with atomic ensembles and linear optics, Nature (London) **414**, 413 (2001).
[16] N. Sangouard, C. Simon, H. De Riedmatten, and N. Gisin, Quantum repeaters based on atomic ensembles and linear optics, Rev. Mod. Phys. **83**, 33 (2011).
[17] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **108**, 130503 (2012).
[18] S. Abruzzo, H. Kampermann, and D. Bruß, Measurement-device-independent quantum key distribution with quantum memories, Phys. Rev. A **89**, 012301 (2014).
[19] C. Panayi, M. Razavi, X. Ma, and N. Lütkenhaus, Memory-assisted measurement-device-independent quantum key distribution, New J. Phys. **16**, 043005 (2014).
[20] K. Azuma, K. Tamaki, and W. J. Munro, All-photonic intercity quantum key distribution, Nat. Commun. **6**, 10171 (2015).
[21] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the ratedistance limit of quantum key distribution without quantum repeaters, Nature (London) **557**, 400 (2018).
[22] 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.
[23] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum Key Distribution, Phys. Rev. X **8**, 031043 (2018).
[24] 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).
[25] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, Phys. Rev. A **98**, 042332 (2018).

[26] 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).
[27] 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. Applied **11**, 034053 (2019).
[28] H. L. Yin and Y. Fu, Measurement-device-independent twin-field quantum key distribution, Sci. Rep. **9**, 3045 (2019).
[29] K. Tamaki, H.-K. Lo, C. H. F. Fung, and B. Qi, Phase encoding schemes for measurement-device-independent quantum key distribution with basis-dependent flaw, Phys. Rev. A **85**, 042307 (2012).
[30] T. F. Da Silva, D. Vitoreti, G. B. Xavier, G. C. Do Amaral, G. P. Temporao, and J. P. Von Der Weid, Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits, Phys. Rev. A **88**, 052303 (2013).
[31] A. Rubenok, J. A. Slater, P. Chan, I. Lucio-Martinez, and W. Tittel, Real-World Two-Photon Interference and Proof-of-Principle Quantum Key Distribution Immune to Detector Attacks, Phys. Rev. Lett. **111**, 130501 (2013).
[32] Y. Liu *et al.*, Experimental Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **111**, 130502 (2013).
[33] Z. Tang, Z. Liao, F. Xu, B. Qi, L. Qian, and H.-K. Lo, Experimental Demonstration of Polarization Encoding Measurement-Device-Independent Quantum Key Distribution, Phys. Rev. Lett. **112**, 190503 (2014).
[34] 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. Photonics **13**, 334 (2019).
[35] B. Qi, L. L. Huang, H.-K. Lo, and L. Qian, Polarization insensitive phase modulator for quantum cryptosystems, Opt. Express **14**, 4264 (2006).
[36] F. A. Bovino and A. Messina, Increasing operational command and control security by the implementation of device independent quantum key distribution, Quantum Inf. Sci. Technol. II **9996**, 999606 (2016).
[37] A. Muller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, Plug and play systems for quantum cryptography, Appl. Phys. Lett. **70**, 793 (1997).
[38] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, Quantum key distribution over 67 km with a plug & play system, New J. Phys. **4**, 41 (2002).
[39] Y. Zhao, B. Qi, and H.-K. Lo, Quantum key distribution with an unknown and untrusted source, Phys. Rev. A **77**, 052327 (2008).
[40] Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, Security analysis of an untrusted source for quantum key distribution: Passive approach, New J. Phys. **12**, 023024 (2010).
[41] W. Y. Hwang, Quantum Key Distribution with High Loss: Toward Global Secure Communication, Phys. Rev. Lett. **91**, 057901 (2003).
[42] H.-K. Lo, X. Ma, and K. Chen, Decoy State Quantum Key Distribution, Phys. Rev. Lett. **94**, 230504 (2005).
[43] X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, Practical decoy state for quantum key distribution, Phys. Rev. A **72**, 012326 (2005).
[44] X. B. Wang, Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography, Phys. Rev. Lett. **94**, 230503 (2005).
[45] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevLett.123.100506 for the theory model and experimental data.
[46] F. Grasselli and M. Curty, Practical decoy-state method for twin-field quantum key distribution, New J. Phys. **21**, 073001 (2019).
[47] A simple estimation is made here. First, we assume that the phase change increases with the square root of the fiber length [48,49]. In addition, according to Ref. [49], the overall phase fluctuation might be much smaller in installed telecom fibers than in laboratory fibers. As reported in Refs. [21,49], the phase drift rate of 36.5 km installed telecom fibers is around 0.3–1 rad/ms. If we take the optimistic value 0.3 rad/ms as a reference, we find that the phase drift rate of 150 km installed telecom fibers would be about 0.6 rad/ms. Then, taking into account that the transit time is 0.75 ms, we have that the phase drift would be about 0.45 rad and the corresponding QBER is below 5%. This implies that, with a loop length of as long as 300 km, the Sagnac configuration without active phase stabilization is still applicable for TFQKD.
[48] L. Jiang, J. M. Taylor, and M. D. Lukin, Fast and robust approach to long-distance quantum communication with atomic ensembles, Phys. Rev. A **76**, 012301 (2007).
[49] J. Minář, H. de Riedmatten, C. Simon, H. Zbinden, and N. Gisin, Phase-noise measurements in long-fiber interferometers for quantum-repeater applications, Phys. Rev. A **77**, 052325 (2008).
[50] Y. Liu *et al.*, preceding Letter, Experimental Twin-Field Quantum Key Distribution Through Sending-or-not-Sending, Phys. Rev. Lett. **123**, 100505 (2019).
[51] 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).