Beating the Fundamental Rate-Distance Limit in a Proof-of-Principle Quantum Key Distribution System

Shuang Wang,[1,2,3] De-Yong He,[1,2,3] Zhen-Qiang Yin,[1,2,3,*] Feng-Yu Lu,[1,2,3] Chao-Han Cui,[1,2,3] Wei Chen,[1,2,3,†] Zheng Zhou,[1,2,3] Guang-Can Guo,[1,2,3] and Zheng-Fu Han[1,2,3]

[1]*CAS Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China*

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

[3]*State Key Laboratory of Cryptology, P. O. Box 5159, Beijing 100878, China*

(Received 14 November 2018; revised manuscript received 10 February 2019; published 4 June 2019)

With the help of quantum key distribution (QKD), two distant peers are able to share information-theoretical secure key bits. Increasing the key rate is ultimately significant for the applications of QKD in the lossy channel. However, it has been proven that there is a fundamental rate-distance limit, called the linear bound, which restricts the performance of all existing repeaterless protocols and realizations. Surprisingly, a recently proposed protocol, called twin-field (TF) QKD, can beat the linear bound with no need for quantum repeaters. Here, we present one of the first implementations of the TF-QKD protocol and demonstrate its advantage of beating the linear bound at a channel distance of 300 km. In our experiment, a modified TF-QKD protocol that does not assume phase postselection is considered, and thus a higher key rate than the original one is expected. After controlling the phase evolution of the twin fields traveling through hundreds of kilometers of optical fibers, the implemented system achieves high-visibility single-photon interference and allows stable and high-rate measurement-device-independent QKD. Our experimental demonstration and results confirm the feasibility of the TF-QKD protocol and its prominent superiority in long-distance key distribution services.

DOI: 10.1103/PhysRevX.9.021046 Subject Areas: Photonics, Quantum Information

I. INTRODUCTION

Since the invention of the first QKD protocol [1] in 1984, great efforts have been devoted to improving its key rate in a real lossy channel. To overcome the transmission loss of photons, which is the main obstacle to a high key rate, the most powerful way may be to introduce quantum repeaters [2–4]; however, these are still far from applicable today. In practice, many repeaterless QKD experiments [5–12] have been realized to increase the key rate and extend the channel distance. Nevertheless, theorists have proposed that there are some fundamental limits [13,14] on the key rates of all these repeaterless QKD protocols and experiments. Denoting the transmission efficiency of the lossy channel as η, the key rate R for any point-to-point repeaterless QKD protocol will satisfy $R \leq -\log_2(1-\eta)$, i.e., $R \sim O(\eta)$, which is called the linear bound [14]. Surprisingly, several months ago, a revolutionary work [15] pointed out that this bound may be overcome in a so-called twin-field (TF) QKD protocol. In the TF-QKD protocol, both peers Alice and Bob prepare and send phase-coding optical fields (weak coherent states) to an untrusted third party, Charlie, who is in the middle of the channel and interferes with the incoming fields. Then, Alice and Bob can generate sifted key bits, provided Charlie observes a single-photon click after interference. One can imagine that if Charlie is honest, his counting rate of single-photon clicks is only attenuated by the channel loss between Alice to Charlie or Bob to Charlie. Consequently, one may conjecture that R may be proportional to $\sqrt{\eta}$; thus, $R \sim \sqrt{\eta}$ is expected. However, the full security of TF-QKD is not proven in Ref. [15], which leads to the question of its security and the calculation of R [16]. Fortunately, subsequent theoretical works [17–22] remedied the security of TF-QKD with different methods and reconfirmed its advantage of beating the linear bound. Besides, these theoretical works also showed that the security of TF-QKD does not rely on Charlie's measurement; thus, it is measurement-device independent (MDI) [23].

*yinzq@ustc.edu.cn
†weich@ustc.edu.cn

Although the TF-QKD has been the subject of intensive theoretical studies, a successful demonstration of beating the linear bound is still missing, partially because TF-QKD needs steady interference between two weak coherent states from distant peers. In addition, the original theory of TF-QKD predicts that beating the linear bound only occurs when the channel distance is very long. Achieving steady interference between two sources so far away is very challenging since the phase drift is more severe at longer channel distances. Realizing and keeping two laser sources with high indistinguishability is also difficult.

Here, we demonstrate a TF-QKD system where beating the linear bound is achieved at a channel distance of over 300 km. Benefiting from TF-QKD without phase postselection [20,21], our experiment exhibits a key rate over the linear bound at a channel distance of 300 km, which is much shorter than the minimum value to overcome the linear bound predicted by the original protocol. In addition, with no need for phase postselection, our system enjoys a simple process of postprocessing.

II. PROTOCOL

A simplified version of TF-QKD is conducted in our experiment. Our protocol [20] consists of a code mode and a decoy mode. The former is used to generate sifted key bits, while the latter is used to collect some parameters to bound information leakage. The flow of our protocol can be summarized in four steps.

(1) The code mode or decoy mode is randomly selected by Alice (Bob) in each trial.

(2) In the code mode, Alice and Bob prepare phase-coding weak coherent states $|\pm\sqrt{\mu}\rangle_A$ and $|\pm\sqrt{\mu}\rangle_B$, respectively, and then send them to Charlie who interferes with the incoming weak coherent states and measures the phase shift between them. If Charlie successfully registers a photon click, Alice and Bob will retain this key bit. According to Charlie's measurement result, Bob may decide to flip his key bit or not.

(3) In the decoy mode, which is quite similar to the decoy-state method [24–26] used in the MDI-QKD protocol, Alice and Bob prepare and send phase-randomized weak coherent states with four different intensities (μ, ν_1, ν_2, ν_3). Charlie is not aware of the code or decoy modes. He still performs the measurement on the phase shift and announces his measurement result to Alice and Bob.

(4) After repeating steps 1–3 many times and after some public communication, Alice and Bob can accumulate sufficient sifted key bits from code modes and estimate the yields for decoy states Q_d^{xy} ($x, y = \mu, \nu_1, \nu_2, \nu_3$). For instance, $Q_d^{\mu\nu_1}$ is the probability that Charlie announces a successful measurement on the phase shift when Alice and Bob actually prepare weak coherent pulses with mean photon numbers of μ and ν_1, respectively, in the decoy mode. From Q_d^{xy}, information leakage can be bounded, and then secret key bits may be generated.

A notable advantage of our protocol is that phase randomization and postselection in the code mode are both removed. Thus, the experimental system is simplified, and a higher key rate is expected.

III. IMPLEMENTATION SYSTEM OF TF-QKD

The experimental setup performing the TF-QKD protocol is summarized in Fig. 1. As a MDI scenario, two senders, Alice and Bob, have symmetric positions in relation to the measurement node Charlie. Alice and Bob have the same experimental setup, which mainly consists of three modules denoted as source, chopper, and encoder, respectively. Both Alice's and Bob's sources are phase locked with the laser from Charlie to generate the twin fields with a central wavelength of 1550.12 nm.

The chopper is composed of two intensity modulators (IM): IM_1 first modulates the locked continuous-wave (CW) laser into a pulse train with a 130-ps temporal width at a repetition rate of 1 GHz; IM_2 then chops the pulse train into the time-multiplexed reference part and quantum part, in which the reference part is bright and unmodulated by the encoder in order to measure the phase shift of the channels, and the quantum part carries the information of the keys. The duration time of either part is 50 μs.

The encoder only applies to the quantum part, and it is composed of IM_3 and one phase modulator (PM); IM_3 is used to create four intensity levels required by the protocol, and PM is used to modulate a specific or random phase on each pulse of the quantum part. The encoder is randomly operated in the code mode or decoy mode. In the code mode, IM_3 creates the signal state with μ photons per pulse, and PM modulates the phase $\{0, \pi\}$ according to the random key bit $\{0, 1\}$. In the decoy mode, IM_3 randomly creates four decoy states with μ, ν_1, ν_2, and ν_3 photons per pulse, and PM randomizes the phase of each pulse belonging to the quantum part with amplitude resolution of 10 bits [27,28].

Charlie is in the middle to take a single-photon interference measurement. The two fields sent by Alice and Bob interfere on the 50/50 beam splitter (BS). In order to achieve a good interference visibility, a polarization controller (PC) and a feedback PM are added before each input of the BS. The PC is used to set correct polarization, and the feedback PM is used to compensate for the fast phase drift in fiber channels. The interference results are detected by two superconducting single-photon detectors (SSPDs). When both Alice's and Bob's encoders are in the code mode, the detector D0 would click if the phase difference modulated by Alice and Bob is 0, and the detector D1 would click if the phase difference modulated by them is π. These two SSPDs are made by Scontel Inc. and have almost

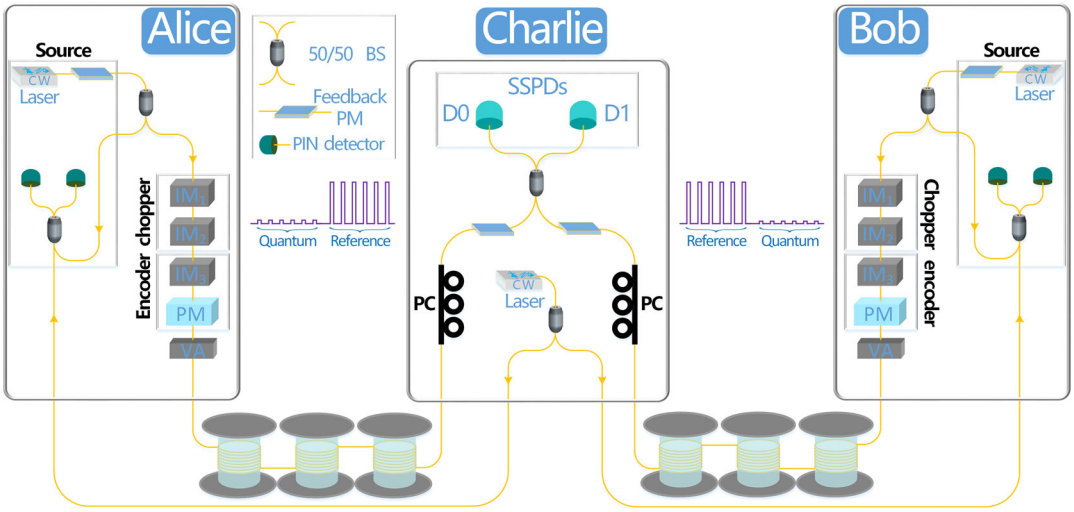

FIG. 1. *Experimental setup to implement the twin-field quantum key distribution*. CW laser, continuous-wave laser; IM, intensity modulator; PM, phase modulator; VA, variable attenuator; 50/50 BS, beam splitter with a 50/50 splitting ratio; PC, polarization controller; SSPDs, superconducting single-photon detectors. Alice and Bob have the same setup, which mainly consists of the source, chopper, and encoder modules. The source generates the laser with a locked frequency and phase with the laser from Charlie. The chopper is used to first modulate the CW laser into a pulse train (IM_1) and then chop it into time-multiplexed bright reference and weak quantum parts (IM_2). The encoder adds code or decoy information into the quantum part (IM_3 and PM).

identical characteristics, exhibiting a detection efficiency close to 60.8% and a dark count rate of 95 Hz.

IV. EXPERIMENTAL RESULTS

There are two main technical challenges when TF-QKD is implemented. One is making the fields generated by Alice and Bob "twin," which means the frequency difference between Alice's and Bob's lasers is nearly constant (as close to zero as possible is desirable), and the phase difference between these two lasers is stable. The other challenge is compensation of the fast phase drift over long fibers.

A. Results of the source part

The optical phase-locked loop (OPLL) architecture [29,30] is employed in the source part to generate the twin fields between Alice and Bob. The CW laser transmitted from Charlie takes the role of a master laser, while the local laser belonging to Alice (Bob) takes the role of a slave laser. The master laser and part of the output of the slave laser are combined in a 50/50 BS to produce a phase error signal, which is then detected by two PIN detectors connected to the feedback loop. The error signal from PIN detectors passes through a loop filter and generates a bias current to tune the frequency of the slave laser. Once the OPLL is locked, the phase difference between the master and slave lasers is stable, and these two lasers have the same frequency.

The master laser (X15 model) is an ultralow-noise fiber laser made by NKT Photonics Inc. During all measurements in the experiment, the master laser is free running, in which its linewidth is less than 0.1 kHz and the wavelength stability over the case temperature is approximately 0.1 pm/°C. The slave laser is an external cavity diode laser with a standard 14-pin butterfly package, whose driving circuit is homemade. The external cavity diode laser (PLANEX^{TM}, RIO Inc.) has a linewidth of less than 2 kHz, and a wavelength sensitivity to temperature and bias current of approximately 12.5 pm/°C and 0.2 pm/mA, respectively. The resolution of the laser temperature controller is 0.001 °C. In the experiment, the central wavelength of the master laser is set at 1550.12 nm, and the wavelength of the slave laser is slowly tuned by changing its temperature. Once the beat note frequency of these two lasers is close to 10 MHz (0.08 pm), the homodyne OPLL will be locked, and we will finally achieve a zero-offset frequency between the master and slave lasers.

The lock performance is tested by observing the beat note signal and the interference visibility, respectively. The beat note signal is measured with a PIN detector and recorded with an oscilloscope. The result of the quadrature interference is displayed in Fig. 2(a), and it exhibits a stable interference result. The interference visibility is measured with two SSPDs—one connects the constructive interference output, and the other connects the destructive interference output. The counts of these two SSPDs are shown in Fig. 2(c); each point is the total count in 50 μs, and the curve is smoothened by averaging every 20 adjacent points. The distributions of the constructive count and destructive count are shown in the insets of Fig. 2(c). The mean value of the constructive count is 251.97, and that of the destructive count is 2.26; thus, the interference visibility is approximately 98.22%.

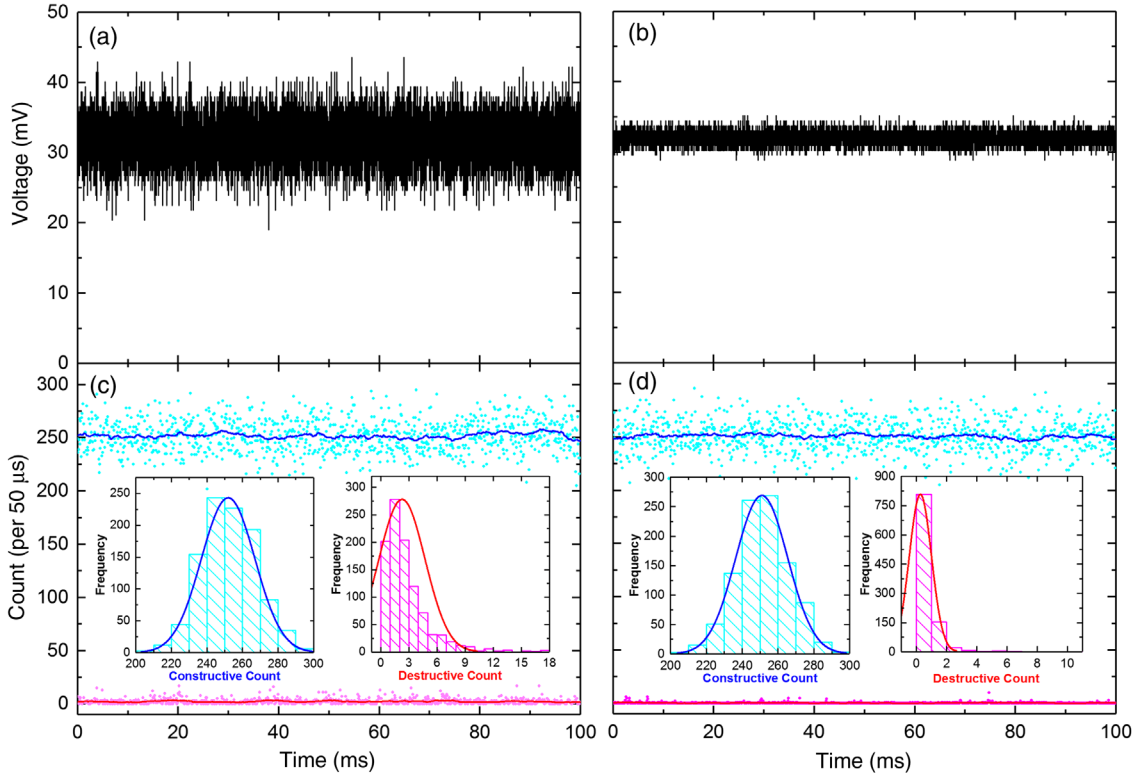

FIG. 2. *Characteristics of the source part.* (a) The quadrature interference results recorded by an oscilloscope. (b) The quadrature interference results with a feedback PM. (c) The in-phase interference results detected by two SSPDs. (d) The in-phase interference results with a feedback PM. The cyan points correspond to the counts of the constructive interference output; the magenta points refer to the counts of the destructive interference output. The curves are smoothened by averaging every 20 adjacent points. The insets are the distributions of the constructive counts and destructive counts.

Furthermore, a feedback PM is added in the source part to reduce residual phase noise. The error signal from PIN detectors is amplified and connected to the PM as negative feedback. The corresponding result of the quadrature interference is displayed in Fig. 2(b); the improvement is significant compared with Fig. 2(a). With almost the same mean value of 32 mV, the standard deviation is changed from 3.18 mV to 0.92 mV. The corresponding counts of two SSPDs are shown in Fig. 2(d). Compared with Fig. 2(c), the improvement mainly comes from the destructive count, whose mean value is changed from 2.26 to 0.27; the corresponding interference visibility becomes approximately 99.78%.

B. Results of compensation of the fast phase drift

After making the fields generated by Alice and Bob twins, the phase drift is mainly due to the fluctuations in the fiber channels. Depending on the surrounding environment (the temperature and vibration), the phase drift accumulates with the length of fiber channels. To compensate this fast phase drift over much longer fibers, a feedback PM is inserted in each arm of the BS at Charlie's site. Two feedback PMs are employed here to get a larger range of phase compensation, though only one feedback PM is sufficient to compensate the differential phase of two channels. The active feedback loop that acts on the feedback PMs is based on the interference outputs of Alice's and Bob's bright pulses belonging to the corresponding reference parts, which are unmodulated and time multiplexed with quantum parts. The interference outputs are detected by two SSPDs (D0 and D1). The goal of the active feedback loop is to maximize (minimize) the counts of detector D0 (D1) through a fast change of the voltage of the feedback PMs. Based on the counts of D0 and D1 belonging to the reference part, the active feedback loop estimates the corresponding compensation voltage and immediately loads it on the feedback PMs.

The active feedback is realized with a field programmable gate array (FPGA), operating at a 40-MHz clock rate that is synchronized with the QKD control system. The feedback PM with an insertion loss of 2.2 dB has a high-impedance input for a bandwidth of approximately 200 MHz. This bandwidth is enough to compensate for the phase drift over long fiber channels, and the high-impedance input is relatively easier to drive at a 40-MHz clock rate. Considering the actuating time from FPGA to PM (~0.2 μs) and the transition time from the reference part to the quantum part, a time window of 48 μs is set to select the counts during each 50 μs.

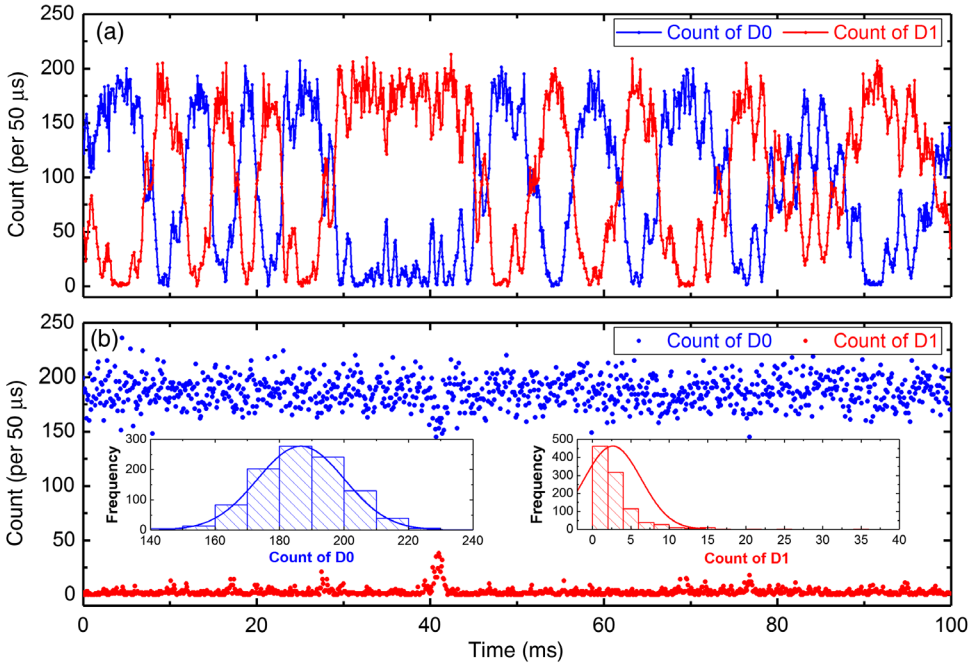

FIG. 3. *Characteristics of the compensation of the fast phase drift at a total distance of 300 km optical fiber.*(a) The phase drift by recording the counts of D0 and D1 when the driving voltage over the feedback PMs is disconnected. (b) The results of actively compensating the phase drift by recording the counts of D0 and D1 after connecting the PM driving voltage. The insets are the distributions of the counts of two SSPDs. Here, only the counts belonging to the reference parts are recorded.

The performance of the compensation of the fast phase drift is tested without and with the active feedback loop. During the test, both Alice's and Bob's sources have been locked with the laser from Charlie, the chopper works, and only the counts belonging to the reference part are recorded. At a total distance of 300-km optical fiber, the pulses in the reference part are attenuated to approximately 2.9 photons per pulse. The phase drift is measured when the driving voltage over the feedback PMs is disconnected, and the counts of the detectors D0 and D1 are displayed in Fig. 3(a). The phase drift mainly depends on the ambient vibration; the drift rate in Fig. 3(a) is less than π rad/ms. The results of actively compensating the phase drift are shown in Fig. 3(b). After connecting the PMs' driving voltage, the counts of D0 and D1 stay relatively stable: D0 corresponds to the constructive interference, and D1 corresponds to the destructive interference. The mean value of the count of D0 is 186.66, and that of the count of D1 is 2.64. Thus, the interference visibility is approximately 97.21%.

V. PERFORMANCE OF THE TF-QKD SYSTEM

After the main technical challenges are tackled, the TF-QKD experiment is performed over three total distances of 100 km, 200 km, and 300 km optical fibers. The optical fibers used in the experiment are standard single-mode fibers (ITU-G. 652D) with a loss coefficient of approximately 0.18 dB/km. The overall loss of Charlie's devices is approximately 5.16 dB. From the yields $Q_{\mu\mu}$, $Q_d^{\mu\mu}$, $Q_d^{v_1v_1}$, $Q_d^{v_2v_2}$, $Q_d^{v_3v_3}$, $Q_d^{\mu v_3}$, $Q_d^{v_1v_3}$, $Q_d^{v_2v_3}$, $Q_d^{v_3\mu}$, $Q_d^{v_3v_1}$, $Q_d^{v_3v_2}$, and the error rate e_b, the upper bound of information leakage I_{AE}^u could be estimated numerically (see the Appendix). Then, the secret key rate is obtained by $R = Q_{\mu\mu}(1 - fh_2(e_\mu) - I_{\mathrm{AE}}^u)$, where the efficiency of the error correction $f = 1.15$ and h_2 is the binary Von Neumann entropy. The results are listed in Table I. For comparison, the linear bound of the secret key rate R_{LB} is also presented. We can clearly see that our secret key rate overwhelms the linear bound at a channel distance of 300 km. Thus, the secret key rate (~2.01 kbps) can significantly surpass the

TABLE I Experimental results.

Distance (km)	Total loss (dB)	Visibility	$Q_{\mu\mu}$	e_μ	R	R_{LB}
100	23.06	98.64%	2.02×10^{-3}	1.86%	8.87×10^{-4}	7.15×10^{-3}
200	40.66	98.05%	1.94×10^{-4}	2.42%	8.01×10^{-5}	1.24×10^{-4}
300	58.46	96.79%	2.11×10^{-5}	3.59%	6.46×10^{-6}	2.06×10^{-6}

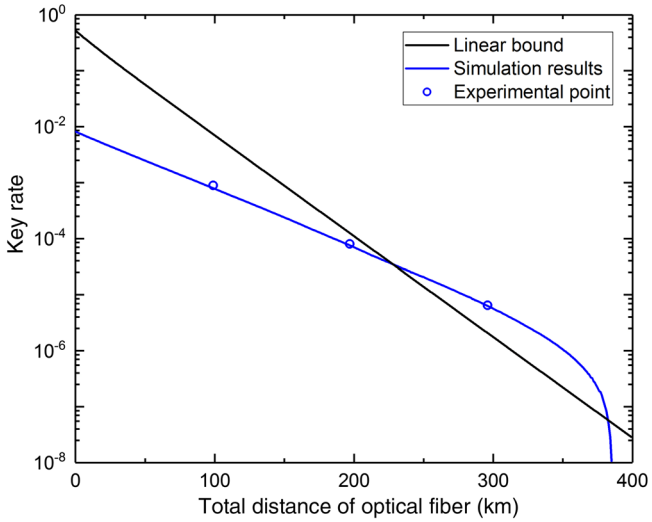

FIG. 4. *Key rate of the TF-QKD system.* The rates are plotted against the total distance of optical fiber (from Alice to Bob) with a loss efficiency of 0.18 dB/km. The open dots refer to experimental points at distances of 100 km, 200 km, and 300 km, respectively.

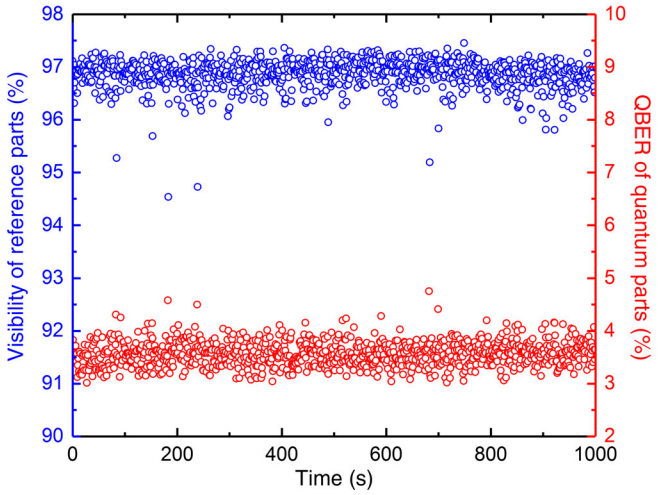

FIG. 5. *Stability of the TF-QKD system over a total distance of 300 km.* The blue open dots represent the interference visibility of Alice's and Bob's reference parts, and the red open dots are QBER of the corresponding quantum parts. Each dot corresponds to the data acquired in one second.

state-of-the-art QKD experiment with the same channel loss (53.3 dB), which is 5 orders of magnitude larger than the previous QKD experiment in the MDI scenario [11], and 4 times more than the rate in the BB84 experiment with a 2.5-GHz repetition rate [12].

The key rates of our implementation, the simulation results and the linear bound, are summarized in Fig. 4. The key rates of the simulation and linear bound are plotted against the total distance of fiber channels (from Alice to Bob) with a loss efficiency of 0.18 dB/km. (The linear bound here includes the detector's nonunity efficiency and the receiver loss. Details of the simulation can be found in the Appendix). Experimental results (open dots) at distances of 100 km, 200 km, and 300 km are moved to the positions with equivalent attenuations. For instance, the measured loss of 300 km fiber in the experiment is approximately 53.3 dB, and the corresponding experimental dot is moved to the distance of 296 km in Fig. 4. In general, the experimental points fit the simulation results quite well. In the same environment, the phase drift of the channels mainly depends on the length of optical fibers. Employing the same active feedback module, the phase drift could be compensated very well at relatively short distances. The visibility of the reference parts is 98.64% at a distance of 100 km, and 98.05% at a distance of 200 km. Because of the relatively high visibility of reference parts and low QBER of quantum parts, the key rates at distances of 100 km and 200 km are a little higher than the simulation results.

VI. DISCUSSION

At a total distance of 300 km optical fiber, the stability of the TF-QKD system is shown with the interference visibility (blue open dots) and QBER (red open dots) in Fig. 5. Over 1000 seconds, the mean value of the interference visibility of Alice's and Bob's reference parts is 96.86%, and the mean value of the QBER of the corresponding quantum parts is 3.56%. Since the phase drift mainly depends on the ambient vibration, there are some abrupt vibrations that cannot be compensated very well, and they cause some relatively low visibility and high QBER, such as the dots at 182 seconds; the interference visibility and QBER are 94.54% and 4.58%, respectively. Still, the performance of the system is relatively stable, the standard deviation of the interference visibility and QBER are 0.28% and 0.23%, respectively. The stability of the system is important to set a suitable data size during the quantum transmission. Considering that the effective absolute rate of the quantum part is 480 MHz, the total number of transmitted pulses is approximately 4.8×10^{11} (1000-second transmission time) at distances of 100 km and 200 km, and 2.4×10^{12} (5000-second transmission time) at a distance of 300 km. As a proof-of-principle experiment, we do not take the finite-size effects into account in this work. The main reason is that the aim of a proof-of-principle demonstration is to verify the feasibility of TF-QKD and its advantage of beating the linear bound. For this purpose, we accumulate sufficient clicks to characterize parameters with negligible statistical fluctuations; we then calculate the asymptotic key rate. Although finite-size effects inevitably lower the key rate, one can always alleviate this influence by sending more signals.

Compared with the interference visibilities at distances of 100 km and 200 km (above 98%), the relatively low visibility at a distance of 300 km shows the limitation of the compensation of the phase drift. If we want to reduce the

channel optical error, the interference visibility of the reference parts should be improved. The duration time of both reference and quantum parts needs to be shortened, and the intensity of the reference part needs to be increased. This is a key step towards longer distances, in addition to choosing a large-misalignment-error-tolerant protocol [18] and SSPDs with an ultralow dark count rate.

As a proof-of-principle experiment, the reference lasers from Charlie are distributed to Alice and Bob with short fibers, and the phase error signal is detected by PIN detectors. Once Alice's and Bob's lasers are in a remote location, the intensity would be attenuated intensively, and the phase drift of the channel would also be introduced in the optical field. Considering that the bandwidth of the loop filter belonging to the OPLL is approximately 100 kHz, the phase drift over long fiber channels could be well compensated in the loop. In order to get a strong phase error signal, one could amplify the attenuated laser from Charlie but introduce as little phase noise as possible. Although the quantum channels used in the experiment are fiber spools in the laboratory, we guess that the phase drift rate in a real-life setting would be no faster than the value measured in the laboratory. These fiber spools, which are arranged in a centralized way, could be considered as a transducer with high sensitivity, and a very small vibration from the external environment that acts on these fiber spools (with 300-km length) could be converted into (or amplified by) a large phase drift. For the field-installed fibers, they would suffer inevitable and unpredictable variations, but the length of the affected fibers is limited. Thus, these local variations lead to random local phase drifts; on average, the overall phase drift rate in the field-installed fiber is the sum of the local phase drift rates and will likely be less than the one measured in the laboratory. Intensity fluctuation is another issue may degrade the performance of TF-QKD. Fortunately, according to the Refs. [31,32], the level of intensity variations ($<2\%$) in our experiment has negligible impact on the key rate.

To summarize, we have successfully demonstrated an implementation of the TF-QKD protocol without phase postselection. The implemented system can control well the phase evolution of the twin fields traveling over hundreds of kilometers of optical fiber channels to achieve a single-photon interference with high visibility. Moreover, at a total distance of 300-km standard single-mode fiber, our system overcomes the fundamental rate-distance limit of QKD. The system runs a modified version of the original TF-QKD. Its code mode no longer requires phase randomization and postselection; thus, the secret key rate is further improved compared with the original TF-QKD. Our achievement demonstrates that the TF-QKD protocol is feasible in practice, and it will be a very promising solution for high-rate QKD over long distances in the future. We believe that there will be a notable improvement on the performance of QKD products with the help of the TF-QKD protocol. However, there are still a few points that must be addressed in future studies. First, the finite-key analysis is needed for the real applications of TF-QKD. Second, the phase drift of the field fiber setup may be different from our experiment in the laboratory; thus, a field experiment would be needed. Finally, Charlie distributes the master laser to Alice and Bob as the phase-locking references; that architecture could be easily expanded to a star-type network.

ACKNOWLEDGMENTS

This work has been supported by the National Key Research and Development Program of China (Grant No. 2016YFA0302600), the National Natural Science Foundation of China (NSFC) (Grants No. 61622506, No. 61575183, No. 61822115, No. 61775207, and No. 61627820), and the Anhui Initiative in Quantum Information Technologies.

S. W. and D.-Y. H. contributed equally to this work.

Notes added.—Recently, several other TF-QKD implementations were reported in Refs. [33–35]. It is worth noting that the quantum channel in Refs. [33,34] is (mainly) simulated by a variable optical attenuator but not real fiber. In Ref. [35], the advantage of beating the linear bound is not realized.

APPENDIX: SOME DETAILS OF CALCULATION AND EXPERIMENT

The calculation of key rate.—The key rate is obtained by $R = Q_{\mu\mu}(1 - fh_2(e_b) - I^u_{\mathrm{AE}})$. The essential goal is to estimate the upper bound of Eve's information on key bits I^u_{AE}. According to Eq. (2) of Ref. [20], I^u_{AE} can be calculated by an optimization problem, which is

$$I^u_{\mathrm{AE}} = \max_x h\left(\frac{x_{00}}{Q_{\mu\mu}}, \frac{x_{10}}{Q_{\mu\mu}}\right) + h\left(\frac{x_{11}}{Q_{\mu\mu}}, \frac{x_{01}}{Q_{\mu\mu}}\right).$$

The constraints for the non-negative real variables x_{00}, x_{10}, x_{11}, and x_{01} are functions of $Y_{n,m}$, which is defined as the yield when Alice and Bob prepare the n photon and m photon, respectively, in the decoy mode. In the case of finite decoy states, the upper bound and lower bound of $Y_{n,m}$, i.e., $Y^u_{n,m}$ and $Y^l_{n,m}$, can be used to bound x_{00}, x_{10}, x_{11}, and x_{01}. Then, I^u_{AE} is obtained. Concretely, linear programming is used to search $Y^{u(l)}_{0,0}$, $Y^{u(l)}_{0,1}$, $Y^{u(l)}_{1,0}$, $Y^{u(l)}_{1,1}$, $Y^{u(l)}_{0,2}$, and $Y^{u(l)}_{2,0}$ satisfying the experimental observed yields $Q^{\mu\mu}_d$, $Q^{v_1v_1}_d$, $Q^{v_2v_2}_d$, $Q^{v_3v_3}_d$, $Q^{\mu v_3}_d$, $Q^{v_1v_3}_d$, $Q^{v_2v_3}_d$, $Q^{v_3\mu}_d$, $Q^{v_3v_1}_d$, and $Q^{v_3v_2}_d$, since $Q^{xy}_d = \sum_{n,m=0}^{+\infty} P^x_n P^y_m Y_{n,m}$, where $P^x_n = e^{-x}x^n/n!$. Similarly, the lower bound of $P^\mu_0 P^\mu_0 Y_{0,0} + P^\mu_0 P^\mu_1 Y_{0,1} + P^\mu_1 P^\mu_0 Y_{1,0} + P^\mu_2 P^\mu_0 Y_{2,0} + P^\mu_0 P^\mu_2 Y_{2,0} + P^\mu_1 P^\mu_1 Y_{1,1}$ is obtained by linear programming. With these bounds, the constraints of x_{00}, x_{10}, x_{11}, and x_{01} are established by Eqs. (A.22)–(A.25) of Ref. [20]. Finally, I^u_{AE} and the key rate R are found. We list the detailed experimental data in Tables II and III.

TABLE II. Here, LL is the distance between Alice and Bob, the attenuation column is for the channel between Alice and Bob; μ is the intensity of the signal state; $\nu_1(\nu_2, \nu_3)$ are the intensities of decoy states; Q is the yield of the code mode; and e is the error rate of the raw key bit.

L (km)	Attenuation (dB)	μ	ν_1	ν_2	ν_3	Q	e (%)
100	17.9	0.026	0.005	0.002	8×10^{-5}	2.02×10^{-3}	1.86
200	35.5	0.019	0.005	0.002	6×10^{-5}	1.94×10^{-4}	2.42
300	53.3	0.016	0.005	0.002	5×10^{-5}	2.11×10^{-5}	3.59

TABLE III. The yields of the decoy mode.

L (km)	$Q_d^{\mu\mu}$	$Q_d^{\upsilon_1\upsilon_1}$	$Q_d^{\upsilon_2\upsilon_2}$	$Q_d^{\upsilon_3\upsilon_3}$	$Q_d^{\mu\upsilon_3}$ ($Q_d^{\upsilon_3\mu}$)	$Q_d^{\upsilon_1\upsilon_3}$ ($Q_d^{\upsilon_3\upsilon_1}$)	$Q_d^{\upsilon_2\upsilon_3}$ ($Q_d^{\upsilon_3\upsilon_2}$)
100	2.02×10^{-3}	3.88×10^{-4}	1.56×10^{-4}	6.40×10^{-6}	1.01×10^{-3}	1.97×10^{-4}	8.10×10^{-5}
200	1.94×10^{-4}	5.12×10^{-5}	2.06×10^{-5}	8.02×10^{-7}	9.73×10^{-5}	2.60×10^{-5}	1.07×10^{-5}
300	2.11×10^{-5}	6.74×10^{-6}	2.81×10^{-6}	2.55×10^{-7}	1.07×10^{-5}	3.50×10^{-6}	1.53×10^{-6}

The simulation of key rate.—In the simulation, we assume the transmittance of the channel is $\eta = 10^{-0.018l}\eta_D$, in which l is the channel distance (km) and $\eta_D = 0.305$ is the overall efficiency of the measurement device. The linear bound is calculated by $R = -\log_2(1-\eta)$, where $\eta = 10^{-0.018l}\eta_D$ represents the overall efficiency. The dark count rate of each channel of SPD is $d = 10^{-7}$ per pulse. The optical misalignment is set to 0.03. In the decoy mode, $\upsilon_1 = 0.005$, $\upsilon_2 = 0.002$, and $\upsilon_3 = 10^{-2.5}\mu$, while μ is optimized to maximize the key rate at each distance. All experimentally observed yields and error rates can be simulated with the formulas given in Appendix B of Ref. [20].

The phase randomization.—The phase randomization in the decoy mode is performed by the PM belonging to the encoder in Fig. 1. The amplitude resolution of the phase randomization is 10 bits. The phase modulation range is from 0 to 2π. At a 1-GHz rate, the half-wave voltage of the PM is approximately 3.5 V. Thus, the amplitude resolution of the driving voltage is about 7 mV. Considering the noise of the RF amplifier, the phase randomization is quasicontinuous, though the discrete phase randomization method is employed. To verify the phase randomization, we have performed a separate experiment before the TF-QKD experiment, using a variable delay asymmetric interferometer, a high-speed PIN detector, and an oscilloscope. In the TF-QKD experiment, the phase randomization could also be verified by the QBER, which would increase up to around 50% in the decoy mode, similar to the useful method proposed by Zhao *et al.* in Ref. [27].

Temperature control of the laser source.—The temperature control of the laser source is important to keep the stability of the central wavelength. In the OPLL, the central wavelength of the slave laser is first tuned to be close to the wavelength of the master laser by changing its temperature. Once the wavelength difference is less than 0.08 pm, the OPLL would be locked. The wavelength sensitivity of the slave laser is about 12.5 pm/°C; thus, 0.005 °C is enough for the OPLL. However, in order to keep the long-term stability, we improve the control precision up to 0.001 °C. To achieve this temperature control precision, the choices of the signal amplifier and analog-to-digital converter (ADC) are important. Here, a precision instrument amplifier is employed; it has a high input impedance, a high CMRR, and a low offset, and is very suitable for small signal amplification. Also, the high-resolution (24 bits) ADC is used. Moreover, the thermal insulation of the diode laser is also important. If every aspect is considered, a control precision up to 10^{-6} °C will be possible in some research papers.

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing* (IEEE, New York, 1984) 175–179.

[2] 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).

[3] 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).

[4] 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).

[5] H. Takesue, S. W. Nam, Q. Zhang, R. H. Hadfield, T. Honjo, K. Tamaki, and Y. Yamamoto *Quantum Key Distribution over a 40-dB Channel Loss Using Superconducting Single-Photon Detectors*, Nat. Photonics **1**, 343 (2007).

[6] A. Dixon, Z. Yuan, J. Dynes, A. Sharpe, and A. Shields, *Gigahertz Decoy Quantum Key Distribution with 1 Mbit/s Secure Key Rate*, Opt. Express **16**, 18790 (2008).

[7] S. Wang, W. Chen, J.-F. Guo, Z.-Q. Yin, H.-W. Li, Z. Zhou, G.-C. Guo, and Z.-F. Han *2 GHz Clock Quantum Key Distribution over 260 km of Standard Telecom Fiber*, Opt. Lett. **37**, 1008 (2012).

[8] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, *Experimental Demonstration of Long-Distance Continuous-Variable Quantum Key Distribution*, Nat. Photonics **7**, 378 (2013).
[9] B. Korzh, C. C. W. Lim, R. Houlmann, N. Gisin, M. J. Li, D. Nolan, B. Sanguinetti, R. Thew, and H. Zbinden *Provably Secure and Practical Quantum Key Distribution over 307 km of Optical Fibre*, Nat. Photonics **9**, 163 (2015).
[10] A. Dixon *et al. High Speed Prototype Quantum Key Distribution System and Long Term Field Trial*, Opt. Express **23**, 7583 (2015).
[11] H.-L. Yin *et al. Measurement-Device-Independent Quantum Key Distribution over a 404 km Optical Fiber*, Phys. Rev. Lett. **117**, 190501 (2016).
[12] A. Boaron *et al. Secure Quantum Key Distribution over 421 km of Optical Fiber*, Phys. Rev. Lett. **121**, 190502 (2018).
[13] M. Takeoka, S. Guha, and M. M. Wilde, *Fundamental Rate-Loss Tradeoff for Optical Quantum Key Distribution*, Nat. Commun. **5**, 5235 (2014).
[14] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, *Fundamental Limits of Repeaterless Quantum Communications*, Nat. Commun. **8**, 15043 (2017).
[15] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, *Overcoming the Rate–Distance Limit of Quantum Key Distribution without Quantum Repeaters*, Nature (London) **557**, 400 (2018).
[16] X.-B. Wang, X.-L. Hu, and Z.-W. Yu, *Effective Eavesdropping to Twin Field Quantum Key Distribution*, arXiv:1805.02272.
[17] 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.
[18] 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).
[19] X.-F. Ma, P. Zeng, and H.-Y. Zhou, *Phase-Matching Quantum Key Distribution*, Phys. Rev. X **8**, 031043 (2018).
[20] C.-H. 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).
[21] M. Curty, K. Azuma, and H.-K. Lo, *Simple Security Proof of Twin-Field Type Quantum Key Distribution Protocol*, arXiv:1807.07667.
[22] J. Lin and N. Lütkenhaus, *A Simple Security Analysis of Phase-Matching Measurement-Device Independent Quantum Key Distribution*, Phys. Rev. A **98**, 042332 (2018).
[23] H.-K. Lo, M. Curty, and B. Qi, *Measurement-Device-Independent Quantum Key Distribution*, Phys. Rev. Lett. **108**, 130503 (2012).
[24] W.-Y. Hwang, *Quantum Key Distribution with High Loss: Toward Global Secure Communication*, Phys. Rev. Lett. **91**, 057901 (2003).
[25] X.-B. Wang, *Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography.* Phys. Rev. Lett. **94**, 230503 (2005).
[26] H.-K. Lo, X. Ma, and K. Chen, *Decoy State Quantum Key Distribution*, Phys. Rev. Lett. **94**, 230504 (2005).
[27] Y. Zhao, B. Qi, and H.-K. Lo, *Experimental Quantum Key Distribution with Active Phase Randomization*, Appl. Phys. Lett. **90**, 044106 (2007).
[28] Z. Cao, Z. Zhang, H.-K. Lo, and X. Ma *Discrete-Phase-Randomized Coherent State Source and Its Application in Quantum Key Distribution*, New J. Phys. **17**, 053014 (2015).
[29] L. Kazovsky, *Balanced Phase-Locked Loops for Optical Homodyne Receivers: Performance Analysis, Design Considerations, and Laser Linewidth Requirements*, J. Lightwave Technol. **4**, 182 (1986).
[30] S. Ristic, A. Bhardwaj, M. J. Rodwell, L. A. Coldren, and L. A. Johansson *An Optical Phase-Locked Loop Photonic Integrated Circuit*, J. Lightwave Technol. **28**, 526 (2010).
[31] F.-Y. Lu *et al. Practical Issues of Twin-Field Quantum Key Distribution*, arXiv:1901.04264.
[32] F. Grasselli *et al. Practical Decoy-State Method for Twin-Field Quantum Key Distribution*, arXiv:1902.10034.
[33] M. Minder *et al. Experimental Quantum Key Distribution Beyond the Repeaterless Secret Key Capacity*, Nat. Photonics **13**, 334 (2019).
[34] X. Zhong *et al. Proof-of-Principle Experimental Demonstration of Twin-Field Type Quantum Key Distribution*, arXiv:1902.10209.
[35] Y. Liu *et al. Experimental Twin-Field Quantum Key Distribution through Sending-or-Not-Sending*, arXiv:1902.06268.