SCIENTIFIC REPORTS

OPEN

Measurement-Device-Independent Twin-Field Quantum Key Distribution

Received: 2 August 2018
Accepted: 25 January 2019
Published online: 28 February 2019

Hua-Lei Yin[1,2] & Yao Fu[2]

The ultimate aim of quantum key distribution (QKD) is improving the transmission distance and key generation speed. Unfortunately, it is believed to be limited by the secret-key capacity of quantum channel without quantum repeater. Recently, a novel twin-field QKD (TF-QKD) is proposed to break through the limit, where the key rate is proportional to the square-root of channel transmittance. Here, by using the vacuum and one-photon state as a qubit, we show that the TF-QKD can be regarded as a measurement-device-independent QKD (MDI-QKD) with single-photon Bell state measurement. Therefore, the MDI property of TF-QKD can be understood clearly. Importantly, the universal security proof theories can be directly used for TF-QKD, such as BB84 encoding, six-state encoding and reference-frame-independent scheme. Furthermore, we propose a feasible experimental scheme for the proof-of-principle experimental demonstration.

Throughout history, the battle between encryption and decryption never ends. Currently, relying on computational complexity, the widely used public-key cryptosystem becomes vulnerable to quantum computing attacks. The one-time pad is the only provably secure cryptosystem according to information theory known today. Thereinto, an important issue exists that the common secret key is at least as long as the message itself and can be used only once. Quantum key distribution (QKD) constitutes the only way to solve the real time key distribution problem[1]. QKD allows two distant parties to establish a string of secret keys with information-theoretic security[2,3]. One can ensure legitimate parties to exchange messages with perfect confidentiality by combining QKD with one-time pad.

The longest transmission distance of QKD has been implemented over 421 km with ultralow-loss optical fiber[4] and 1200 km satellite-to-ground[5]. Improving the transmission distance and key rate are the most important tasks of QKD research. However, this task has been proven impossible beyond a certain limit without quantum repeaters[6,7]. The secret-key capacity of quantum channel can be used to bound the extractable maximum secret key[6,7]. Generally, the secret-key capacity can be regarded as a linear key rate Pirandola-Laurenza-Ottaviani-Banchi (PLOB) bound[7] $R_{\mathrm{PLOB}} = -\log_2(1-\eta)$, where η is the transmittance. To overcome the rate-distance limit of QKD, quantum repeaters are usually believed as a strong candidate[8,9]. However, the long-time quantum memory and high-fidelity entanglement distillation are far from feasible. Despite the recent advance[10] relaxing the requirement, the actual implementation is also difficult to realize, for example, quantum non-demolition (QND) measurement. Although the trusted relay-based QKD has been deployed over 2000 km[11], its security is compromised.

Recently, a novel protocol called twin-field QKD (TF-QKD)[12] has been proposed to overcome the rate-distance limit. The secret key rate of TF-QKD has been scaled with the square-root of the transmittance, $R \sim O(\sqrt{\eta})$. In the TF-QKD, a pair of optical fields are generated respectively at locations of two remote parties and then sent to the untrusted center to implement single-photon detection. Compared with measurement-device-independent QKD (MDI-QKD)[13], TF-QKD retains the properties of being immune to all detector attack, multiplexing of expensive single-photon detectors and natural star network architecture. In the original paper of TF-QKD[12], the communication parties, Alice and Bob, prepare the phase-randomized coherent state with phase encoding in X and Y basis. To acquire the correction of raw keys, they should announce the random phase of each pulse. The key rate of unconditional security proof is still missing in the original paper[12].

[1]National Laboratory of Solid State Microstructures and School of Physics, Nanjing University, Nanjing, 210093, China. [2]Department of Physics, Zhejiang Institute of Modern Physics and ZJU-Phoenix Synergetic Innovation Center in Quantum Technology, Zhejiang University, Hangzhou, 310027, China. Correspondence and requests for materials should be addressed to H.-L.Y. (email: hlyin@nju.edu.cn)

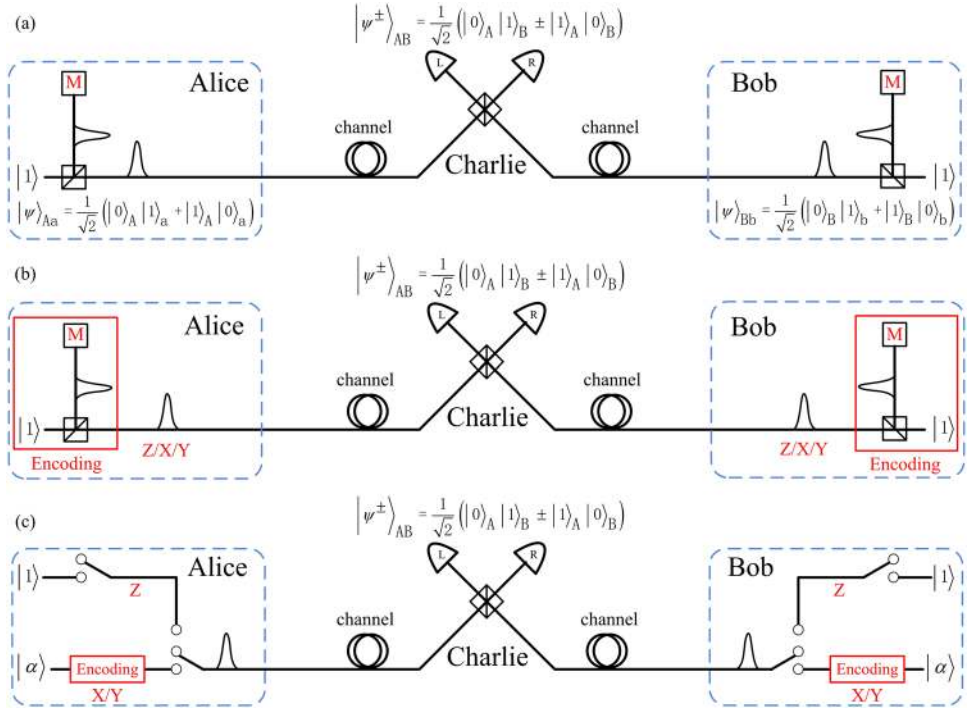

Figure 1. Scheme to overcome the PLOB bound of QKD. (**a**) Setup for entanglement-based MDI-QKD with single-photon BSM. Alice and Bob prepare single-photon Bell state, while Charlie implements entanglement swapping. *M* represents the measurement operation, such as *Z*, *X* and *Y* basis. Alice and Bob implement the *M* measurement operation after Charlie performs the single-photon BSM. (**b**) Prepare-and-measure MDI-QKD with single-photon BSM. Alice and Bob directly prepare the qubit with superpositions of the vacuum and one-photon states. Alice and Bob implement the *M* measurement operation before Charlie performs the single-photon BSM. (**c**) Effective TF-QKD with single-photon and laser sources. The photons from single-photon source and laser source are indistinguishable in every degree of freedom. The phase-reference of long-distance should be stabilized to implement laser interference. The single-photon source is used to implement *Z* basis encoding, while the laser source is used to implement the phase encoding, such as *X* and *Y* basis.

Various different important works have been shown to give the key rate formulas with information-theoretic security[14–19].

Here, we prove that TF-QKD can be seen as a special type of MDI-QKD. Thereinto, a qubit is physically implemented by a two-dimensional subspace with vacuum and one-photon state. One can consider that the untrusted center performs the single-photon Bell state measurement (BSM) while Alice and Bob prepare quantum state in the complementary bases. Since the vacuum state is immune to the loss, it can always have a detection (detector without click means a successful detection), thus the probability of coincident detection is exactly equal to that of single detection. Therefore, the TF-QKD inherits all positive features of MDI-QKD and increases the key rate a lot to break through the linear key rate bound. The unconditional security proof technologies with entanglement purification[20,21], information theory analysis[22], entropy uncertainty relation[23] can be directly applied in the TF-QKD. The bit of *Z* basis is independent of the phase misalignment. Naturally, there is no need to publish random phase of *Z* basis and the state can be seen as a mixture of photon number states. Therefore, the distilled secret key of *Z* basis in the TF-QKD can exploit the tagging-method of Gottesman-Lo-Lütkenhaus-Preskill (GLLP) analysis[24]. Combining the decoy-state method[25–27], we could acquire the tight key rate formula of TF-QKD with BB84 encoding[1], six-state encoding[28] and reference-frame-independent (RFI)[29] scheme.

Results

MDI-QKD with single-photon BSM. Here, let us first introduce an entanglement-based MDI-QKD with single-photon BSM protocol, as shown in Fig. 1(a). Let $\{|0\rangle, |1\rangle\}$ represent *Z* basis, where 0 and 1 are the vacuum and the one-photon state, respectively. Accordingly, the eigenvectors of *X* basis and *Y* basis are $|\pm\rangle = (|0\rangle \pm |1\rangle)/\sqrt{2}$ and $|\pm i\rangle = (|0\rangle \pm i|1\rangle)/\sqrt{2}$. Considering that one photon inputs a lossless symmetric beam splitter, the output state is a single-photon entangled state, $|\psi^+\rangle = (|0\rangle|1\rangle + |1\rangle|0\rangle)/\sqrt{2}$. Alice and Bob prepare a series of entangled states $|\psi^+\rangle_{Aa} = (|0\rangle_A|1\rangle_a + |1\rangle_A|0\rangle_a)/\sqrt{2}$ and $|\psi^+\rangle_{Bb} = (|0\rangle_B|1\rangle_b + |1\rangle_B|0\rangle_b)/\sqrt{2}$, respectively, where *A* (*B*) and *a* (*b*) are a pair of field modes. Afterwards, they hold the qubit of *a* and *b* modes and send the quantum states of *A* and *B* modes to the untrusted third party, Charlie, who performs the BSM to identify the two single-photon Bell states $|\psi^+\rangle_{AB} = (|0\rangle_A|1\rangle_B + |1\rangle_A|0\rangle_B)/\sqrt{2}$ and $|\psi^-\rangle_{AB} = (|0\rangle_A|1\rangle_B - |1\rangle_A|0\rangle_B)/\sqrt{2}$. Therefore, a coincidence detection with *L* click and *R* no click indicates a projection into the Bell state $|\psi^+\rangle_{AB}$. A coincidence detection with *R* click and *L* no click, implies a projection into the Bell state $|\psi^-\rangle_{AB}$. Note that the

identification of any one Bell state is enough to prove the security. When Charlie performs a successful BSM, the qubit that the legitimate users hold becomes a single-photon Bell state, the process of which can be regarded as an entanglement swapping, as experimentally demonstrated[30]. Alice and Bob can utilize quantum memory to store their qubit a and b modes. After Charlie announces the events through public channels whether he has obtained a Bell state and which Bell state he has identified, Alice and Bob will measure qubit a and b modes, respectively. They publish the basis information through an authenticated classical channel. Bob will apply a bit flip when they choose Z (X or Y) basis and Charlie receives a Bell state $|\psi^{\pm}\rangle_{AB}$ ($|\psi^{-}\rangle_{AB}$). They use the data of Z basis to form the raw key, while the data of other bases are all used to estimate the leaked information. Alice and Bob can acquire the secure key through the error correction and privacy amplification.

We can equivalently convert our entanglement-based protocol in Fig. 1(a) to the prepare-and-measure protocol as shown in Fig. 1(b) by the Shor-Preskill's arguments[21]. Let Alice and Bob measure the modes a and b before they send the qubit of A and B modes to Charlie, meaning Alice and Bob directly prepare the quantum state A mode and B mode. Other steps are all same to the entanglement-based protocol, including the BSM, basis comparison, bit flip, error correction and privacy amplification. Hereafter, we use the TF state to represent the joint quantum state of Alice's A mode and Bob's B mode. In the case of ideal detector (photon-number-resolving and without dark count) and lossless channel, the MDI-QKD with single-photon BSM protocol is similar with the two-photon BSM protocol. However, the single-photon BSM exploits the vacuum state identification, namely, detector without click, the case of TF state with $|1_A\rangle|1_B\rangle$ will create error Bell state detection under the case of lossy channel, which will cause the unbalanced bit value and high bit error rate.

To solve this issue, Alice and Bob need to decrease the probability of qubit $|1\rangle$ preparation and increase the probability of qubit $|0\rangle$ preparation. Therefore, Alice (Bob) should exploit the entangled state $|\psi\rangle_t = \sqrt{1-t}|0\rangle|1\rangle + \sqrt{t}|1\rangle|0\rangle$ to replace the maximally entangled state $|\psi^+\rangle = (|0\rangle|1\rangle + |1\rangle|0\rangle)/\sqrt{2}$ in the entanglement-based protocol with Fig. 1(a), where t is the transmittance of partial BS. Note that the non-maximally entangled state is also used to prove the security in the TF-QKD[18]. Taking into account the threshold detector and lossy channel, the joint quantum state of Alice's a mode and Bob's b mode after Charlie's BSM with $|\psi^{\pm}\rangle_{AB}$ under the case without eavesdropper's disturbance can be written as (see Methods for detail)

$$\rho_{ab}^{\pm} = \frac{q_0}{q}|11\rangle_{ab}\langle 11| + \frac{q_1}{q}|\psi^{\pm}\rangle_{ab}\langle\psi|^{\pm} + \frac{q_2}{q}|00\rangle_{ab}\langle 00|, \tag{1}$$

where $q = q_0 + q_1 + q_2$, q_0, q_1 and q_2 are the probabilities of Charlie's successful BSM given that the photon numbers of TF state are zero, one and two. Consider a virtual step, if Alice and Bob jointly perform QND measurement on TF state to implement photon-number-resolving before they send TF state to Charlie, the joint quantum state of Alice's a mode and Bob's b mode is $|\psi^{\pm}\rangle_{ab}$ given that the TF state with one-photon and Charlie's BSM with $|\psi^{\pm}\rangle_{AB}$, which reduces to the the case of ideal detector and lossless channel.

Similarly, we can have a equivalent prepare-and-measure protocol corresponding to the entanglement-based protocol with entangled state $|\psi\rangle_t = \sqrt{1-t}|0\rangle|1\rangle + \sqrt{t}|1\rangle|0\rangle$. Alice (Bob) prepares the qubit $|+z\rangle = |0\rangle$ and $|-z\rangle = |1\rangle$ with probability $1-t$ and t as Z basis logic bit 0 and 1, respectively. Alice (Bob) prepares the qubit $|+x\rangle = \sqrt{1-t}|0\rangle + \sqrt{t}|1\rangle$ and $|-x\rangle = \sqrt{1-t}|0\rangle - \sqrt{t}|1\rangle$ with equal probability as X basis logic bit 0 and 1, respectively. Alice (Bob) prepares the qubit $|+y\rangle = \sqrt{1-t}|0\rangle + i\sqrt{t}|1\rangle$ and $|-y\rangle = \sqrt{1-t}|0\rangle - i\sqrt{t}|1\rangle$ with equal probability as Y basis logic bit 0 and 1, respectively. Obviously, the quantum state can be seen as a mixture of photon number states for TF state in the Z basis. For the TF state with one-photon in the Z basis, one of Alice and Bob needs to prepare $|0\rangle$ as logic bit 0 and the other prepare $|1\rangle$ as logic bit 1. However, the quantum state is coherent superposition of photon number states for TF state in the X (Y) basis. Here, if we assume Alice and Bob knowing the quantum bit error rate (QBER) of TF state with one-photon in the X basis, for example, Alice and Bob can perform joint QND measurement on TF state to implement photon-number-resolving in the X basis, one can use the case of TF state with one-photon to extract secure key in the BB84 encoding, which can be given by (see Methods for detail)

$$R_{\mathrm{BB84}} = q_1[1 - H(e_{XX}^{b1})] - qH(E_{ZZ}), \tag{2}$$

where $E_{ZZ} = (q_0 + q_2)/q$ is the QBER of Z basis, $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy and e_{XX}^{b1} is the QBER in X basis for TF state with one-photon. We can have optimal secure key rate in Eq. (2) with the transmittance of partial BS $t \approx 8\%$ given that QBER $e_{XX}^{b1} = 3\%$, dark count rate of threshold detector $p_d = 10^{-6}$, efficiency of threshold detector $\eta_d = 40\%$ and the fiber distance between Alice and Bob $L \geq 100$ km. Note that the entanglement-based protocol in Fig. 1(a) and prepare-and-measure protocol in Fig. 1(b) are the virtual protocols, which are not used to perform experiment but prove the security in theory.

TF-QKD with phase-encoding coherent state. Manipulating the quantum state with superpositions of the vacuum and one-photon states and, in particular, requiring control about the relative phase between the vacuum and one-photon state is quite problematic[31]. However, we consider the coherent state $|\alpha\rangle = e^{-\mu/2}\sum_{n=0}^{\infty}\frac{(e^{i\theta}\sqrt{\mu})^n}{\sqrt{n!}}|n\rangle$, where the relative phase θ between the different Fock states in the superposition is reflected physically in the phase of the classical electric field. Hereafter, the phase-encoding basis means to implement phase modulation of coherent state, such as X and Y basis. In order to achieve Alice and Bob knowing the QBER of TF state with one-photon in the phase-encoding basis without the requirement of QND measurement, one can use the post-selected phase-matching method for phase-randomized coherent state[12,15]. By using the post-selected phase-matching method, the phases of

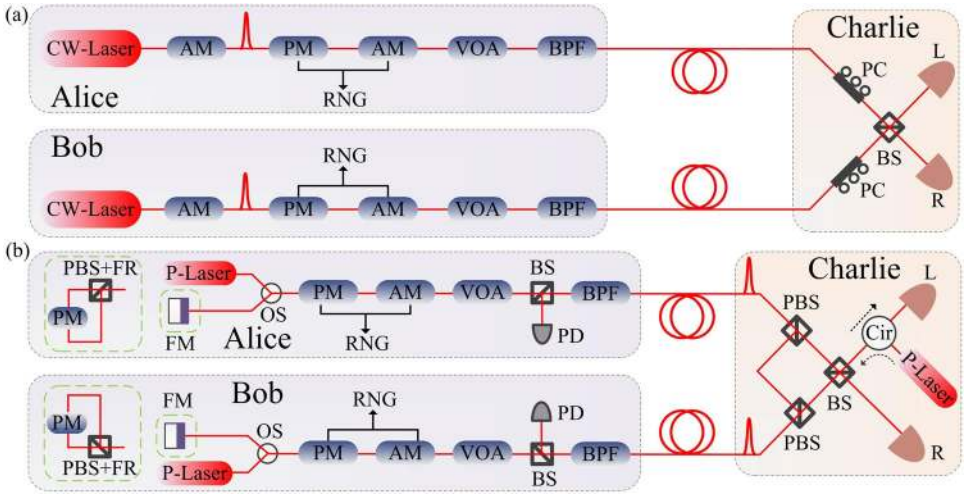

Figure 2. The practical TF-QKD setup. (**a**) practical TF-QKD with independent lasers. The phase modulator (PM) can realize phase encoding and random phase modulation at one time. CW-Laser: continuous-wave laser, AM: amplitude modulator, VOA, variable optical attenuator, BPF: band pass filter, PC: polarization controller, BS: beam splitter, RNG: random number generator. (**b**) Phase self-aligned TF-QKD with single laser. The Faraday mirror (FM) or the polarization beam splitter (PBS) and the $\pi/2$ Faraday rotator (FR) are exploited to realize the transformation between horizontal and vertical polarizations. Alice and Bob could choose to prepare the qubit in Z basis by using Charlie's laser or their own pulse lasers. The security will be enhanced if they use their own laser. Some polarization-maintaining fiber are required to keep the polarization in the systems of Alice, Bob and Charlie. P-Laser: pulse laser, OS: optical switch, PD, photoelectric detector, Cir: circulator.

Alice's and Bob's coherent state can be seen as equal and randomized, which means that they can use decoy-state method to estimate the yield and QBER of TF state with one-photon in the phase-encoding basis (see Methods).

Efficient TF-QKD. Here, we propose an efficient TF-QKD that the single-photon source used for Z basis and laser source used for phase-encoding basis in Fig. 1(c). The qubit prepared in Z basis can be implemented by turning on and off (such as optical switch) the single-photon source, while the qubit of phase encoding basis should exploit the phase-randomized coherent state combined with phase modulation. However, the perfect single-photon source is still a challenge under the current technology. Therefore, we propose a practical TF-QKD by exploiting phase-randomized coherent state to replace single-photon source used for Z basis encoding.

Practical TF-QKD. In the following, let us explain our practical TF-QKD in detail as shown in Fig. 2(a). (i) Alice and Bob use the stabilized narrow line-width continuous-wave laser and amplitude modulator to prepare the global phase stabilized optical pulses. Alice's and Bob's random phases $\theta_A \in [0, 2\pi)$ and $\theta_B \in [0, 2\pi)$ are realized by using phase modulators. For Z basis encoding, the phase-randomized coherent state with intensities 0 and μ as logic bits 0 and 1 with probabilities $1-t$ and t by using amplitude modulator. For X (Y) basis encoding, they use the phase and amplitude modulator to randomly implement 0 ($\pi/2$) and π ($-\pi/2$) phase modulation as logic bits 0 and 1 with intensities $\{\nu/2, \omega/2, 0\}$. (ii) Then they send quantum states to Charlie for single-photon BSM through the insecure quantum channel. Charlie publishes the successful events of single-photon BSM. (iii) Alice and Bob will announce the basis information through the authenticated classical channel. The intensity and random phase information $k_{A,B}$ of phase-encoding basis should be disclosed, while those of Z basis are confidential to Charlie, where they have $\theta_{A,B} \in \Delta_{k_{A,B}}, \Delta_{k_{A,B}} = \left[\frac{2\pi k_{A,B}}{M}, \frac{2\pi(k_{A,B}+1)}{M}\right)$ and $k_{A,B} \in \{0, 1, \ldots, M-1\}$. (iv) Alice and Bob use the data of Z basis as the raw key, while the data of phase-encoding basis are announced to estimate the amount of leaked information. (v) They exploit the classical error correction and privacy amplification to extract the secure key rate.

After Charlie announces the measurement results, he cannot change the yield and QBER due to information causality[32]. The decoy-state method of estimating the yield and QBER of TF state with n-photon in phase-encoding basis is also true even for the post-selected phase-matching method, which has also been used in phase-matching QKD[15]. The GLLP analysis[24] can be used for the data of Z basis, since the random phases information of Alice's and Bob's coherent states are all confidential to Charlie. Bob will always flit his bit in Z basis. Due to the density matrix of TF state with one-photon $\rho_{\mathrm{TF}}^{1ZZ} = \rho_{\mathrm{TF}}^{1XX} = \frac{1}{2}(|01\rangle_{AB}\langle 01| + |10\rangle_{AB}\langle 10|)$, we can use the yield of TF state with one-photon $Y_{\mathrm{TF}}^{1ZZ} = Y_{\mathrm{TF}}^{1XX}$ in the asymptotic limit. Note that, we can also directly estimate the yield Y_{TF}^{1ZZ} by using the data of phase-encoding basis given that one of Alice and Bob sends intensity 0.

For the BB84 encoding[1], Alice and Bob only keep the data of $|k_B - k_A| = 0$ and $M/2$ when they both choose X basis by the post-selected phase-matching method. If $|k_B - k_A| = 0$ ($|k_B - k_A| = M/2$), Bob will flit his bit when Charlie receives a Bell state $|\psi^-\rangle_{AB}$ ($|\psi^+\rangle_{AB}$). The secure key rate of practical TF-QKD can be given by

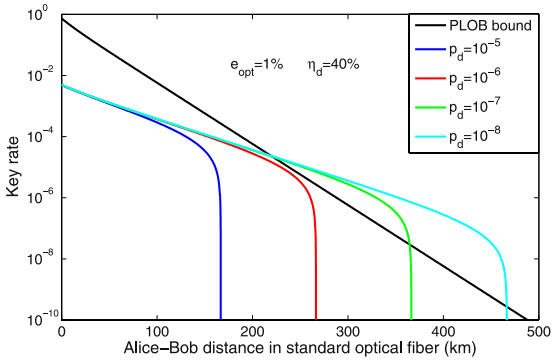

Figure 3. The key rate of practical TF-QKD with BB84 encoding in the asymptotic limit. For each transmission loss, we optimize the parameters μ and t with $e_{\text{opt}}=1\%$, $\nu=0.1$, $\omega=0.02$ and $M=16$. For the PLOB bound, we use $R_{\text{PLOB}}=-\log_2(1-\eta_{\text{PLOB}})$, $\eta_{\text{PLOB}}=\eta_d\times 10^{-0.02L}$. The secure key rate of TF-QKD with BB84 encoding can surpass the PLOB bound under the case of detector with $\eta_d=40\%$, $p_d=10^{-7}$, the performance of detector has been realized much more[34].

$$R_{\text{TF-BB84}}=2t(1-t)\mu e^{-\mu}Y_{\text{TF}}^{1ZZ}[1-H(e_{XX}^{b1})]-Q_{ZZ}fH(E_{ZZ}), \tag{3}$$

where Q_{ZZ} is the gain in Z basis acquired directly from the experiment, $f=1.15$ is the error correction coefficient.

For the RFI scheme[29,33], one can allow Alice and Bob to have different phase references which can be changed slowly (details can be found in Methods). Therefore, they can collect the data of $|k_B-k_A|=k$, $k\in\{0,1,\ldots,M-1\}$ to form a set D_k, where the probability of $|k_B-k_A|=k$ is $\frac{1}{M}$. For each set D_k, they calculate the value $C_k^1=(1-2e_{XXk}^{b1})^2+(1-2e_{XYk}^{b1})^2+(1-2e_{YXk}^{b1})^2+(1-2e_{YYk}^{b1})^2$, where $e_{XXk(XYk,YXk,YYk)}^{b1}$ is the QBER of TF state with one-photon in set D_k given that Alice and Bob choose $X-X(X-Y,Y-X,Y-Y)$ basis. The secure key rate of practical TF-QKD with RFI scheme can be given by

$$R_{\text{TF-RIF}}=2t(1-t)\mu e^{-\mu}Y_{\text{TF}}^{1ZZ}[1-I_E(C^1)]-Q_{ZZ}fH(E_{ZZ}), \tag{4}$$

where $I_E(C^1)=(1-e_{ZZ}^{b1})H\left(\frac{1+\mu}{2}\right)+e_{ZZ}^{b1}H\left(\frac{1+\nu}{2}\right)$ describes eavesdropper Eve's information, thereinto, $\nu=\sqrt{C^1/2-(1-e_{ZZ}^{b1})^2u^2}/e_{ZZ}^{b1}$, $u=\min[\sqrt{C^1/2}/(1-e_{ZZ}^{b1}),1]$ and $C^1=\frac{1}{M}\sum_{k=0}^{M-1}C_k^1$. Compared with the BB84 encoding, all data of RFI scheme can be exploited to estimate parameter C^1, which can be used to slow down the finite size effect. Alice and Bob can change M to acquire the maximum key rate without impacts on efficiency. The QBER of Z basis for TF state with one-photon $e_{ZZ}^{b1}\equiv 0$ leads to $I_E(C^1)=H((1+\sqrt{C^1/2})/2)$.

The secure key rate of practical TF-QKD using BB84 encoding changes with the dark count rate as shown in Fig. 3. We use the practical parameters to simulate the secure key rate in Fig. 3, where the efficiency of detector is $\eta_d=40\%$, the loss coefficient of the channel is 0.2 dB/km and the optical error rate of system is $e_{\text{opt}}=1\%$. The optical error rate is usually large due to the long-distance single-photon-type interference. We compare the secure key rates of practical TF-QKD using BB84 encoding and RFI scheme with the different optical error rate as shown in Fig. 4. To show the advantage of TF-QKD, the efficiency and dark count rate of detector are assumed to be $\eta_d=90\%$ and $p_d=10^{-9}$ in Fig. 4, respectively. In the simulation, both schemes can surpass the PLOB bound and tolerate the big optical error rate e_{opt}. The key rate of TF-QKD with BB84 encoding will significantly decline with e_{opt} rising, while the RFI scheme is robust. However, the long-distance phase-stabilization (it could not be a perfect match but is required to vary slowly) also exists since the relative phase changes too fast in the long-distance fiber or free-space channel.

The experimental demonstration of TF-QKD with independent lasers in Fig. 2(a) is a big challenge, although the MDI-QKD with two-photon BSM has been implemented over 404 km optical fiber[34] by using asymmetric four-intensity decoy-state method[35]. Compared with the two-photon BSM, greater technological challenges exist in the TF-QKD with single-photon BSM. The frequency difference of two independent lasers is required more rigorously[12]. The phase-locking technique may be used to compensate the frequency difference. Importantly, the long-distance phase-stabilization technique is required to implement single-photon interference with phase matching. The RFI scheme can allow the phase mismatching. However, the relative phase change is still required to vary slowly. To rapidly implement the proof-of-principle TF-QKD experiment, we present a phase self-aligned TF-QKD with single laser interference as shown in Fig. 2(b). The horizontal polarization optical pulse generated by Charlie is divided into two pulses by the polarization-maintaining beam splitter. By exploiting the $\pi/2$ rotation effect of Faraday mirror, the two pulses interfere after they go through the same path. Though the phase self-aligned scheme would be affected by the loss and noise, the frequency difference and long-distance phase-stabilization problems are both solved[36]. An extra security analysis with untrusted source[37] should be used to defeat the attack from systems of Alice and Bob.

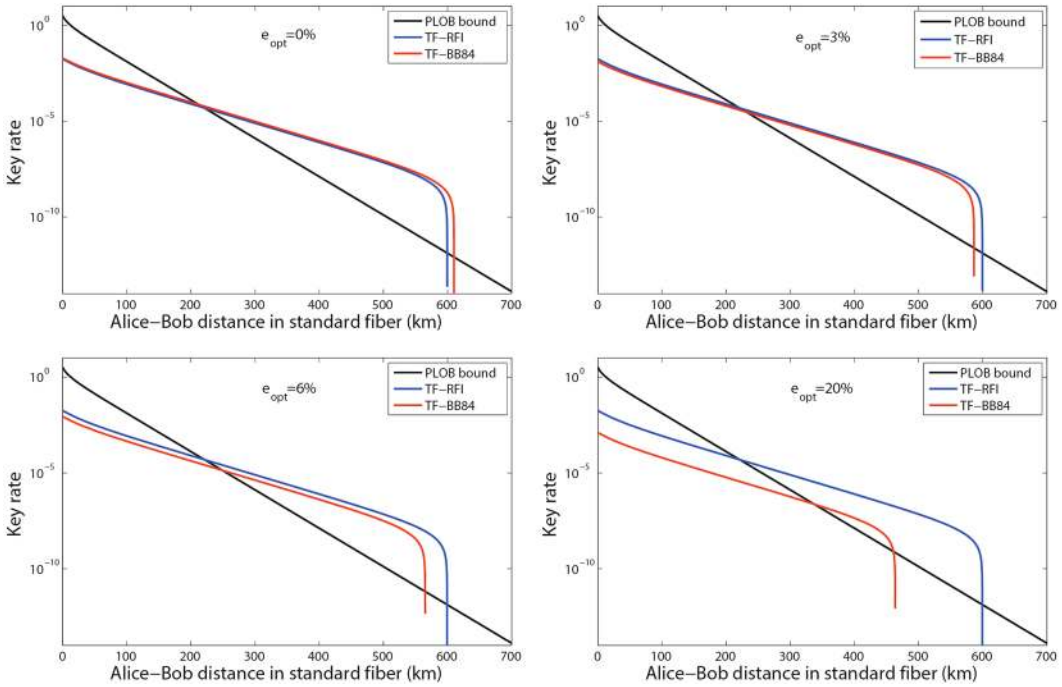

Figure 4. The key rates of practical TF-QKD with BB84 encoding and RFI scheme in the asymptotic limit. For each transmission loss, we optimize the parameters μ and t with $\eta_d = 90\%$, $p_d = 10^{-9}$, $\nu = 0.1$, $\omega = 0.02$ and $M = 16$. The secure key rate of practical TF-QKD with RFI scheme do not change obviously with optical error rate e_{opt}. The secure key rate of practical TF-QKD with BB84 encoding can also beat the PLOB bound even the optical error rate up to $e_{\text{opt}} = 20\%$.

Discussion

In summary, we have proved that the TF-QKD can be regarded as a MDI-QKD with single-photon BSM. By introducing the Z basis encoding, the secret key extraction can exploit the tagging method of GLLP analysis and the decoy-state method. Compared with BB84 encoding, the RFI scheme has the advantages of increasing the data of parameter estimation and reducing the effect of phase drift. We should point out that the extra Y basis preparation in RFI scheme does not add additional operation due to the active phase randomization requirement, which is different from the traditional QKD. We propose a feasible experimental scheme to implement the proof-of-principle experimental demonstration. Note that, the security of this proof-of-principle experiment in Fig. 2b is not guaranteed with our current analysis, which requires a further security evaluation due to introducing untrusted source. Through simulation, we show that the secure key rate of practical TF-QKD can surpass the PLOB bound. The universally composable security with finite-key analysis needs to be considered in the future. Our proposal suggests an important avenue for practical high-speed and long-distance QKD without detector vulnerabilities. During the preparation of this paper and posting it on the arXiv, we became aware of some important works[14–19] of TF-QKD.

Methods

MDI-QKD with single-photon BSM. For the case of entanglement-based protocol with the entangled state $|\psi_t\rangle = \sqrt{1-t}\,|0\rangle|1\rangle + \sqrt{t}\,|1\rangle|0\rangle$, the joint quantum state of Alice and Bob can be given by

$$\begin{aligned}\varphi_{ABab} &= |\psi^+\rangle_{Aa} \otimes |\psi^+\rangle_{Bb} \\ &= (1-t)|0011\rangle_{ABab} + \sqrt{t(1-t)}\,(|0110\rangle_{ABab} + |1001\rangle_{ABab}) + t|1100\rangle_{ABab}.\end{aligned} \tag{5}$$

For the threshold detector and lossy channel, the TF state $|00\rangle_{AB}$, $|01\rangle_{AB}$, $|10\rangle_{AB}$ and $|11\rangle_{AB}$ will all have single-photon Bell state clicks. Due to the single-photon BSM of Charlie, the photon number of TF state will collapse to three events, namely vacuum, one-photon and two-photon. The corresponding probability can be expressed as

$$\begin{aligned}q_0 &= 2(1-t)^2 p_d(1-p_d), \\ q_1 &= 2t(1-t)\{p_d(1-p_d)(1-\sqrt{\eta}) + (1-p_d)[1-(1-p_d)(1-\sqrt{\eta})]\}, \\ q_2 &= t^2\{p_d(1-p_d)(1-\sqrt{\eta})^2 + (1-p_d)[1-(1-p_d)(1-\sqrt{\eta})^2]\},\end{aligned} \tag{6}$$

where the expression of q_2 is acquired by the Hong-Ou-Mandel interference of two-photon. The parameter $\sqrt{\eta} = \eta_d \times 10^{-0.02L/2}$ is the transmittance between Alice (Bob) and Charlie.

For the case of prepare-and-measure protocol corresponding to entanglement-based protocol with the entangled state $|\psi_t\rangle = \sqrt{1-t}|0\rangle|1\rangle + \sqrt{t}|1\rangle|0\rangle$, the density matrix of TF state in the Z basis is

$$\rho_{TF}^{ZZ} = t(1-t)\,(|01\rangle_{AB}\langle 01| + |10\rangle_{AB}\langle 10|) + (1-t)^2|00\rangle_{AB}\langle 00| + t^2|11\rangle_{AB}\langle 11|, \tag{7}$$

which means a mixture of photon number states for TF state in the Z basis. The TF state of Z basis is the product state of Alice's and Bob's quantum state. The density matrix of TF state with one-photon in the Z basis is

$$\rho_{\mathrm{TF}}^{1ZZ} = \frac{1}{2}(|01\rangle_{AB}\langle 01| + |10\rangle_{AB}\langle 10|), \tag{8}$$

which needs one of Alice and Bob prepares $|0\rangle$ as logic bit 0 and the other prepares $|1\rangle$ as logic bit 1.

The density matrix of TF state in the X basis can be written as

$$\begin{aligned}\rho_{\mathrm{TF}}^{XX} &= \frac{1}{4}[|+x,\ +x\rangle_{AB}\langle +x,\ +x| + |+x,\ -x\rangle_{AB}\langle +x,\ -x| \\ &\quad + |-x,\ +x\rangle_{AB}\langle -x,\ +x| + |-x,\ -x\rangle_{AB}\langle -x,\ -x|].\end{aligned} \tag{9}$$

Thereinto, we have

$$\begin{aligned}|\pm x,\ +x\rangle_{AB} &= (1-t)|00\rangle_{AB} + \sqrt{t(1-t)}(|01\rangle_{AB} \pm |10\rangle_{AB}) \pm t|11\rangle_{AB}, \\ |\pm x,\ -x\rangle_{AB} &= (1-t)|00\rangle_{AB} - \sqrt{t(1-t)}(|01\rangle_{AB} \mp |10\rangle_{AB}) \mp t|11\rangle_{AB},\end{aligned} \tag{10}$$

which means a coherent superposition of photon number state for TF state in the X basis. If Alice and Bob jointly perform QND measurement on TF state to implement photon-number-resolving, we have

$$\begin{aligned}|\pm x,\ +x\rangle_{AB} &\xrightarrow[\text{one-photon}]{\text{QND measurement}} \frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB}), \\ |\pm x,\ -x\rangle_{AB} &\xrightarrow[\text{one-photon}]{\text{QND measurement}} \frac{1}{\sqrt{2}}(|01\rangle_{AB} \mp |10\rangle_{AB}), \\ \rho_{\mathrm{TF}}^{1XX} &= \frac{1}{2}(|01\rangle_{AB}\langle 01| + |10\rangle_{AB}\langle 10|) = \rho_{\mathrm{TF}}^{1Z},\end{aligned} \tag{11}$$

where ρ_{TF}^{1ZZ} (ρ_{TF}^{1XX}) is the density matrix of TF state with one-photon in the Z (X) basis. We have $Y_{\mathrm{TF}}^{1ZZ} = Y_{\mathrm{TF}}^{1XX}$ in the asymptotic limit due to $\rho_{\mathrm{TF}}^{1ZZ} = \rho_{\mathrm{TF}}^{1XX}$, where Y_{TF}^{1ZZ} (Y_{TF}^{1XX}) is the yield given that Alice and Bob choose Z (X) basis and TF state contains one-photon. Alice and Bob can know the locations of the TF state with one-photon by using the QND measurement, they could discard all other states and apply error correction and privacy amplification only to the TF state with one-photon. In this case with BB84 encoding, they can achieve a key rate of[20,21]

$$R_{\mathrm{BB84}} = q_1[1 - H(e_{ZZ}^{b1}) - H(e_{XX}^{b1})]). \tag{12}$$

For the TF state with one-photon in the Z basis, we have $e_{ZZ}^{b1} \equiv 0$ since we only have the case of Alice's logic bit 0 (1) and Bob's logic bit 1 (0) corresponding to quantum state $|01\rangle$ ($|10\rangle$).

However, if we assume that Alice and Bob can know the QBER of TF state with one-photon in the X basis, one can acquire the secure key in the Z basis without Alice and Bob knowing the locations (QND measurement) of the TF state with one-photon by using the GLLP analysis[24]. The secure key rate can be given by

$$R_{\mathrm{BB84}} = q_1[1 - H(e_{XX}^{b1})] - qH(E_{ZZ}), \tag{13}$$

where the parameter q_1 should be calculated by using the decoy-state method, for example, we choose three value of t in the Z basis.

TF-QKD with phase-encoding coherent state. In order to make Alice and Bob know the QBER of TF state with one-photon in the X basis without the requirement of QND measurement, we need to consider the case of phase-randomized coherent state

$$\begin{aligned}\rho &= \frac{1}{2\pi}\int_0^{2\pi} |\alpha\rangle_A\langle\alpha| \otimes |e^{i\delta}\alpha\rangle_B\langle e^{i\delta}\alpha| d\theta \\ &= e^{-2\mu}\sum_{n=0}^{\infty}\sum_{m=0}^{\infty}\sum_{k=0}^{n+m}\frac{e^{i\delta(k-n)}\mu^{n+m}}{\sqrt{n!m!k!(n+m-k)!}}|n\rangle_A\langle k| \otimes |m\rangle_B\langle n+m-k|,\end{aligned} \tag{14}$$

where the global phases of Alice's coherent state $|\alpha\rangle_A = |e^{i\theta}\sqrt{\mu}\rangle_A$ and Bob's $|e^{i\delta}\alpha\rangle_B = |e^{i(\theta+\delta)}\sqrt{\mu}\rangle_B$ should be randomized and have a fixed phase difference δ. Therefore, we have

$$|\alpha\rangle_A|e^{i\delta}\alpha\rangle_B \xrightarrow[\text{one-photon}]{\text{phase-randomized}} \frac{1}{\sqrt{2}}(|01\rangle_{AB} + e^{-i\delta}|10\rangle_{AB}). \tag{15}$$

For the X basis encoding, we have

$$
\begin{aligned}
|\pm\alpha\rangle_A|+\alpha\rangle_B &\xrightarrow[\text{one-photon}]{\text{phase-randomized}} \frac{1}{\sqrt{2}}(|01\rangle_{AB} \pm |10\rangle_{AB}),\\
|\pm\alpha\rangle_A|-\alpha\rangle_B &\xrightarrow[\text{one-photon}]{\text{phase-randomized}} \frac{1}{\sqrt{2}}(|01\rangle_{AB} \mp |10\rangle_{AB}),\\
\rho_{\mathrm{TF}}^{1XX} &= \frac{1}{2}(|01\rangle_{AB}\langle 01| + |10\rangle_{AB}\langle 10|),
\end{aligned}
\tag{16}
$$

where the global phases of Alice's and Bob's coherent state should be equal and randomized. It can be realized by using post-selected phase-matching method for phase-randomized coherent state introduced in the original TF-QKD[12] and phase-matching QKD[15]. If we consider the photon number space of TF state given that the global phases of Alice's coherent state and Bob's are randomized and have a fixed phase difference, the density matrix can be given by

$$
\rho = e^{-2\mu}\sum_{n=0}^{\infty}\frac{(2\mu)^n}{n!}|n\rangle_{TF}\langle n|,
\tag{17}
$$

which is similar with the phase encoding phase-randomized coherent state in the traditional decoy-state QKD[26,27]. Therefore, the decoy state method can be used for estimating the yield and QBER of TF state with one-photon.

For phase-randomized coherent state used for Z basis encoding, we have

$$
\begin{aligned}
\rho_{\mathrm{TF}}^{ZZ} &= (1-t)^2|00\rangle_{AB}\langle 00| + t^2\left(\sum_{n=0}^{\infty}e^{-\mu}\frac{\mu^n}{n!}|n\rangle_A\langle n|\right)\left(\sum_{m=0}^{\infty}e^{-\mu}\frac{\mu^m}{m!}|m\rangle_B\langle m|\right)\\
&\quad + t(1-t)\left[|0\rangle_A\langle 0|\left(\sum_{n=0}^{\infty}e^{-\mu}\frac{\mu^n}{n!}|n\rangle_B\langle n|\right) + \left(\sum_{n=0}^{\infty}e^{-\mu}\frac{\mu^n}{n!}|n\rangle_A\langle n|\right)|0\rangle_B\langle 0|\right].
\end{aligned}
\tag{18}
$$

We need $|0\rangle$ as logic bit 0 and $|1\rangle$ as logic bit 1, therefore the efficient TF state with one-photon in Z basis only results from the case of logic bit 0_A1_B and 1_A0_B with the probability $2t(1-t)\mu e^{-\mu}$. For simulation, we consider the case without Charlie's disturbance. In the Z basis of practical TF-QKD, by going through the quantum channel and beam splitter, we have $(1-t)^2$ probability of quantum state

$$
|0\rangle_A\langle 0|_B \xrightarrow{\mathrm{BS}} |0\rangle_L|0\rangle_R,
\tag{19}
$$

$t(1-t)$ probability of quantum state

$$
|0\rangle_A|e^{i\theta_B}\sqrt{\mu}\rangle_B \xrightarrow{\mathrm{BS}} \left|e^{i\theta_B}\sqrt{\frac{\mu\sqrt{\eta}}{2}}\right\rangle_L\left|-e^{i\theta_B}\sqrt{\frac{\mu\sqrt{\eta}}{2}}\right\rangle_R,
\tag{20}
$$

$t(1-t)$ probability of quantum state

$$
|e^{i\theta_A}\sqrt{\mu}\rangle_A|0\rangle_B \xrightarrow{\mathrm{BS}} \left|e^{i\theta_A}\sqrt{\frac{\mu\sqrt{\eta}}{2}}\right\rangle_L\left|e^{i\theta_A}\sqrt{\frac{\mu\sqrt{\eta}}{2}}\right\rangle_R,
\tag{21}
$$

and t^2 probability of quantum state

$$
|e^{i\theta_A}\sqrt{\mu}\rangle_A|e^{i\theta_B}\sqrt{\mu}\rangle_B \xrightarrow{\mathrm{BS}} \left|e^{i\theta_A}\sqrt{\frac{\mu\sqrt{\eta}}{2}} + e^{i\theta_B}\sqrt{\frac{\mu\sqrt{\eta}}{2}}\right\rangle_L\left|e^{i\theta_A}\sqrt{\frac{\mu\sqrt{\eta}}{2}} - e^{i\theta_B}\sqrt{\frac{\mu\sqrt{\eta}}{2}}\right\rangle_R.
\tag{22}
$$

Here, we have $\theta_A \in [0, 2\pi)$ and $\theta_B \in [0, 2\pi)$, L and R represent the left detector and right detector of Charlie, respectively. The gain Q_{ZZ} and QBER E_{ZZ} of practical TF-QKD can be given by

$$
\begin{aligned}
Q_{ZZ} &= 2p_d(1-p_d)(1-t)^2 + 4(1-p_d)e^{-\frac{\mu}{2}\sqrt{\eta}}\left[1-(1-p_d)e^{-\frac{\mu}{2}\sqrt{\eta}}\right]t(1-t)\\
&\quad + 2(1-p_d)e^{-\mu\sqrt{\eta}}[I_0(\mu\sqrt{\eta}) - (1-p_d)e^{-\mu\sqrt{\eta}}]t^2,
\end{aligned}
\tag{23}
$$

and

$$
E_{ZZ}Q_{ZZ} = 2p_d(1-p_d)(1-t)^2 + 2(1-p_d)e^{-\mu\sqrt{\eta}}[I_0(\mu\sqrt{\eta}) - (1-p_d)e^{-\mu\sqrt{\eta}}]t^2.
\tag{24}
$$

For phase-encoding basis of practical TF-QKD, by going through the quantum channel and beam splitter, we have 1/4 probability of quantum state

$$
\begin{aligned}
& \left|e^{i(\theta_A+\pi g_A+\frac{\pi}{2}h_A)}\sqrt{\lambda}\right\rangle_A\left|e^{i(\theta_B+\pi g_B+\frac{\pi}{2}h_B)}\sqrt{\chi}\right\rangle_B \\
\xrightarrow{\text{BS}} & \left|e^{i(\theta_A+\pi g_A+\frac{\pi}{2}h_A)}\sqrt{\frac{\lambda\sqrt{\eta}}{2}}+e^{i(\theta_B+\pi g_B+\frac{\pi}{2}h_B)}\sqrt{\frac{\chi\sqrt{\eta}}{2}}\right\rangle_L \\
\otimes & \left|e^{i(\theta_A+\pi g_A+\frac{\pi}{2}h_A)}\sqrt{\frac{\lambda\sqrt{\eta}}{2}}-e^{i(\theta_B+\pi g_B+\frac{\pi}{2}h_B)}\sqrt{\frac{\chi\sqrt{\eta}}{2}}\right\rangle_R,
\end{aligned}
\tag{25}
$$

where $h_A, h_B \in \{0, 1\}$ represent basis X and Y, $g_A, g_B \in \{0, 1\}$ represent logic bit 0 and 1 given that the intensities of Alice's and Bob's are λ and χ, respectively, $\lambda, \chi \in \{\nu/2, \omega/2, 0\}$. Here, we define $Q_{h_A,h_B}^{\theta_A,\theta_B,\lambda,\chi}$ and $E_{h_A,h_B}^{\theta_A,\theta_B,\lambda,\chi}$ are the gain and QBER that Alice and Bob choose basis h_A and h_B when they send the global phase θ_A and θ_B optical pulses with intensities λ and χ, respectively. Here,

$$
Q_{h_A,h_B}^{\theta_A,\theta_B,\lambda,\chi} = (1-p_d)e^{-\frac{\lambda+\chi}{2}\sqrt{\eta}}[e^{-\sqrt{\lambda\chi\eta}\cos x}+e^{\sqrt{\lambda\chi\eta}\cos x}]-2(1-p_d)^2e^{-(\lambda+\chi)\sqrt{\eta}},
\tag{26}
$$

and

$$
E_{h_A,h_B}^{\theta_A,\theta_B,\lambda,\chi}Q_{h_A,h_B}^{\theta_A,\theta_B,\lambda,\chi} = (1-p_d)e^{-\left(\frac{\lambda+\chi}{2}+\sqrt{\lambda\chi}\cos x\right)\sqrt{\eta}}-(1-p_d)^2e^{-(\lambda+\chi)\sqrt{\eta}},
\tag{27}
$$

where $x = \theta_B - \theta_A + \frac{\pi}{2}(h_B - h_A)$, $E_{h_A,h_B}^{\theta_A,\theta_B,\lambda,\lambda} \simeq \frac{1-\cos x}{2}$ when we assume $\sqrt{\eta} \to 0$ and $p_d \to 0$.

Obviously, we can directly estimate the yield Y_{TF}^{1ZZ} by using the data of phase-encoding basis given that one of Alice and Bob sends intensity 0. We define $\lambda \uplus \chi$ as the intensity set when Alice and Bob send intensity λ and χ phase-randomized coherent state. Therefore, $Q^{\frac{\nu}{2}}$, $Q^{\frac{\nu}{2}}$ and Q^0 are the gain when Alice and Bob send intensities set $\left\{0\uplus\frac{\nu}{2},\ \frac{\nu}{2}\uplus 0\right\}, \left\{0\uplus\frac{\omega}{2},\ \frac{\omega}{2}\uplus 0\right\}$ and $\{0\uplus 0\}$, which can be written as

$$
\begin{aligned}
Q^{\frac{\nu}{2}} &= \frac{1}{2}\left(\frac{1}{4\pi^2}\int_0^{2\pi}\int_0^{2\pi}Q_{h_A,h_B}^{\theta_A,\theta_B,0,\frac{\nu}{2}}d\theta_A d\theta_B+\frac{1}{4\pi^2}\int_0^{2\pi}\int_0^{2\pi}Q_{h_A,h_B}^{\theta_A,\theta_B,\frac{\nu}{2},0}d\theta_A d\theta_B\right) \\
&= 2(1-p_d)e^{-\frac{\nu}{4}\sqrt{\eta}}[1-(1-p_d)e^{-\frac{\nu}{4}\sqrt{\eta}}], \\
Q^{\frac{\omega}{2}} &= 2(1-p_d)e^{-\frac{\omega}{4}\sqrt{\eta}}[1-(1-p_d)e^{-\frac{\omega}{4}\sqrt{\eta}}], \\
Q^0 &= 2p_d(1-p_d).
\end{aligned}
\tag{28}
$$

The Y_{TF}^{0ZZ} and Y_{TF}^{1ZZ} are the yields of TF state with vacuum and one-photon in the Z basis, respectively, which can be given by $(\nu > \omega > 0)$[26,27]

$$
Y_{\text{TF}}^{0ZZ} = Y_0 = Q^0 = 2p_d(1-p_d),
\tag{29}
$$

and

$$
Y_{\text{TF}}^{1ZZ} \geq Y_{\text{TF}}^{1ZZL} = \frac{2\nu}{\nu\omega-\omega^2}\left(e^{\frac{\omega}{2}}Q^{\frac{\omega}{2}}-\frac{\omega^2}{\nu^2}e^{\frac{\nu}{2}}Q^{\frac{\nu}{2}}-\frac{\nu^2-\omega^2}{\nu^2}Q^0\right).
\tag{30}
$$

We assume that the optical error rate e_{opt} of X basis exists due to the single-photon interference. For simplicity, we assume that the optical error rate is introduced by the phase misalignment[12]. Here, a fixed phase difference between Alice's and Bob's global phase is $\delta_0 = \arccos(1-2e_{\text{opt}})$. By using the post-selected phase-matching method in practical TF-QKD with BB84 encoding, Q_{XX}^{ν} (Q_{XX}^{ω}) and E_{XX}^{ν} (E_{XX}^{ω}) are gain and QBER given that Alice chooses X basis with intensity $\frac{\nu}{2}\left(\frac{\omega}{2}\right)$ and Bob chooses X basis with intensity $\frac{\nu}{2}\left(\frac{\omega}{2}\right)$ in the case of $|k_B - k_A| = 0$ and $\frac{M}{2}$. They can be given by

$$
Q_{XX}^{\nu} = \frac{M^2}{4\pi^2}\int_{\delta_0}^{\delta_0+\frac{2\pi}{M}}\int_0^{\frac{2\pi}{M}}Q_{0,0}^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}d\theta_A d\theta_B, \quad Q_{XX}^{\omega} = \frac{M^2}{4\pi^2}\int_{\delta_0}^{\delta_0+\frac{2\pi}{M}}\int_0^{\frac{2\pi}{M}}Q_{0,0}^{\theta_A,\theta_B,\frac{\omega}{2},\frac{\omega}{2}}d\theta_A d\theta_B,
\tag{31}
$$

and

$$
\begin{aligned}
E_{XX}^{\nu}Q_{XX}^{\nu} &= \frac{M^2}{4\pi^2}\int_{\delta_0}^{\delta_0+\frac{2\pi}{M}}\int_0^{\frac{2\pi}{M}}E_{0,0}^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}Q_{0,0}^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}d\theta_A d\theta_B, \\
Q_{XX}^{\omega}Q_{XX}^{\omega} &= \frac{M^2}{4\pi^2}\int_{\delta_0}^{\delta_0+\frac{2\pi}{M}}\int_0^{\frac{2\pi}{M}}E_{0,0}^{\theta_A,\theta_B,\frac{\omega}{2},\frac{\omega}{2}}Q_{0,0}^{\theta_A,\theta_B,\frac{\omega}{2},\frac{\omega}{2}}d\theta_A d\theta_B.
\end{aligned}
\tag{32}
$$

Due to the random phase shifting, there is still an intrinsic QBER because the random phases are not perfectly matched. If $e_{\text{opt}} = 0.03$, we have $\delta_0 = 0.35$ and $E_{XX}^{\nu} \sim 3.6\%$. By using the decoy-state mentod[26,27], the yield Y_{TF}^{1XX} and QBER e_{XX}^{b1} can be given by

$$\begin{aligned} Y_{\mathrm{TF}}^{1XX} &\geq Y_{\mathrm{TF}}^{1XXL} = \frac{\nu}{\nu\omega - \omega^2}\left(e^{\omega}Q_{XX}^{\omega} - \frac{\omega^2}{\nu^2}e^{\nu}Q_{XX}^{\nu} - \frac{\nu^2-\omega^2}{\nu^2}Q^0\right), \\ e_{XX}^{b1} &\leq e_{XX}^{b1U} = \frac{e^{\omega}E_{XX}^{\omega}Q_{XX}^{\omega} - e^{b0}Q^0}{\omega Y_{\mathrm{TF}}^{1XXL}}, \end{aligned} \tag{33}$$

where $e^{b0} = \frac{1}{2}$ is the QBER of TF state with vacuum in phase-encoding basis.

For six-state encoding[28], the probability that both bit flip and phase shift occurs can be given by[38]

$$a = (e_{ZZ}^{b1} + e_{XX}^{b1} - e_{YY}^{b1})/2. \tag{34}$$

To simplify, we assume that those cases of qubit preparation with relative phase modulation are symmetrical since the random phase is unknown before Charlie performs single-photon BSM. Therefore, we abtain $a = e_{ZZ}^{b1}/2$. Interestingly, the QBER $e_{ZZ}^{b1} \equiv 0$, which means that the key rate of practical TF-QKD with six-state encoding has no advantage compared with BB84 encoding.

For the RFI scheme[29], the Z basis is always well defined, which is $Z_A = Z_B = Z$ for Alice and Bob. The other two bases may vary with the slow phase shifting β, the relation can be given by $X_B = \cos\beta X_A + \sin\beta Y_A$, $Y_B = \cos\beta Y_A - \sin\beta Y_B$ and $\beta = \beta_B - \beta_A$, where Z_A and Z_B, X_A and X_B, Y_A and Y_B are the location reference frames for Z, X and Y basis of Alice and Bob, respectively. β_A (β_B) is the deviation between the practical and standard reference frame for Alice (Bob). Therefore, the eigenstates of X_A (X_B) and Y_A (Y_B) can be written as $|\pm\rangle_A = (|0\rangle \pm e^{i\beta_A}|1\rangle)/\sqrt{2}$ ($|\pm\rangle_B = (|0\rangle \pm e^{i\beta_B}|1\rangle)/\sqrt{2}$) and $|\pm i\rangle_A = (|0\rangle \pm ie^{i\beta_A}|1\rangle)/\sqrt{2}$ ($|\pm i\rangle_B = (|0\rangle \pm ie^{i\beta_B}|1\rangle)/\sqrt{2}$). Note that β_A and β_B are the phases of intrinsic degree of freedom between 0 and 1 and can vary slowly in the virtual protocol with RFI theory. The key rate of single-photon with RFI theory is given by[29]

$$R_{\mathrm{RFI}} = 1 - H(e_b) - I_E(C). \tag{35}$$

Here, $I_E(C) = (1 - e_b)H\left(\frac{1+\mu}{2}\right) + e_bH\left(\frac{1+\nu}{2}\right)$ quantifies the information of Eve's knowledge, parameters $\nu = \sqrt{C/2 - (1-e_b)^2u^2}/e_b$ and $u = \min[\sqrt{C/2}/(1-e_b),\ 1]$. We have $I_E(C) = H((1+\sqrt{C/2})/2)$ if the QBER $e_b = 0$. The value C can be defined as

$$\begin{aligned} C &= \langle X_AX_B\rangle^2 + \langle X_AY_B\rangle^2 + \langle Y_AX_B\rangle^2 + \langle Y_AY_B\rangle^2 \\ &= (1-2E_{XX})^2 + (1-2E_{XY})^2 + (1-2E_{YX})^2 + (1-2E_{YY})^2, \end{aligned} \tag{36}$$

which is independent of phase drifting β_A (β_B) and can just be used to bound Eve's information. However, the phase drifting will add the QBER of X basis, which will decrease the key rate of BB84 encoding. Thereinto, $E_{XX(YY,XY,YX)}$ is the QBER given that Alice and Bob choose $X-X(Y-Y, X-Y, Y-X)$ basis, which can be written as

$$\begin{aligned} E_{XX} &= E_{YY} = \frac{1}{2}(1 - \cos\beta), \\ E_{XY} &= \frac{1}{2}(1 + \sin\beta),\ E_{YX} = \frac{1}{2}(1 - \sin\beta). \end{aligned} \tag{37}$$

One can acquire the maximum value $C = 2$ in the ideal case and $I_E(C=2) = 0$ if the phase difference β is fixed. For phase change from β to $\beta + \Delta\beta$, $\Delta\beta \in [0, 2\pi]$ (uniformity variation), we have

$$C = \frac{2}{(\Delta\beta)^2}\{[\sin(\beta+\Delta\beta) - \sin\beta]^2 + [\cos(\beta+\Delta\beta) - \cos\beta]^2\} = \frac{4(1-\cos\Delta\beta)}{(\Delta\beta)^2}. \tag{38}$$

We can see that C is only related to phase change $\Delta\beta$ and is not related to phase difference β in theory. The value C will decrease with $\Delta\beta$ increasing.

In the practical TF-QKD with RFI scheme, we define that Q_{XXk}^{ν} and E_{XXk}^{ν} are gain and QBER when Alice chooses X basis with intensity $\frac{\nu}{2}$ and Bob chooses X basis with intensity $\frac{\nu}{2}$ in the case of set D_k by using the post-selected phase-matching method. Therefore, the gain Q_{XXk}^{ν}, Q_{XYk}^{ν}, Q_{YXk}^{ν} and Q_{YYk}^{ν} of set D_k are

$$\begin{aligned} Q_{XXk}^{\nu} &= \frac{M^2}{4\pi^2}\int_{\delta_0+\frac{2\pi}{M}k}^{\delta_0+\frac{2\pi}{M}(k+1)}\int_0^{\frac{2\pi}{M}} Q_{0,0}^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}d\theta_Ad\theta_B, \\ Q_{XYk}^{\nu} &= \frac{M^2}{4\pi^2}\int_{\delta_0+\frac{2\pi}{M}k}^{\delta_0+\frac{2\pi}{M}(k+1)}\int_0^{\frac{2\pi}{M}} Q_{0,1}^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}d\theta_Ad\theta_B, \\ Q_{YXk}^{\nu} &= \frac{M^2}{4\pi^2}\int_{\delta_0+\frac{2\pi}{M}k}^{\delta_0+\frac{2\pi}{M}(k+1)}\int_0^{\frac{2\pi}{M}} Q_{1,0}^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}d\theta_Ad\theta_B, \\ Q_{YYk}^{\nu} &= \frac{M^2}{4\pi^2}\int_{\delta_0+\frac{2\pi}{M}k}^{\delta_0+\frac{2\pi}{M}(k+1)}\int_0^{\frac{2\pi}{M}} Q_{1,1}^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}d\theta_Ad\theta_B. \end{aligned} \tag{39}$$

The QBER E_{XXk}^{ν}, E_{XYk}^{ν}, E_{YXk}^{ν} and E_{YYk}^{ν} of set D_k can be written as

$$
\begin{aligned}
E^{\nu}_{XXk}Q^{\nu}_{XXk} &= \frac{M^2}{4\pi^2}\int_{\delta_0+\frac{2\pi}{M}k}^{\delta_0+\frac{2\pi}{M}(k+1)}\int_0^{\frac{2\pi}{M}} E^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}_{0,0}Q^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}_{0,0}d\theta_A d\theta_B,\\
E^{\nu}_{XYk}Q^{\nu}_{XYk} &= \frac{M^2}{4\pi^2}\int_{\delta_0+\frac{2\pi}{M}k}^{\delta_0+\frac{2\pi}{M}(k+1)}\int_0^{\frac{2\pi}{M}} E^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}_{0,1}Q^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}_{0,1}d\theta_A d\theta_B,\\
E^{\nu}_{YXk}Q^{\nu}_{YXk} &= \frac{M^2}{4\pi^2}\int_{\delta_0+\frac{2\pi}{M}k}^{\delta_0+\frac{2\pi}{M}(k+1)}\int_0^{\frac{2\pi}{M}} E^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}_{1,0}Q^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}_{1,0}d\theta_A d\theta_B,\\
E^{\nu}_{YYk}Q^{\nu}_{YYk} &= \frac{M^2}{4\pi^2}\int_{\delta_0+\frac{2\pi}{M}k}^{\delta_0+\frac{2\pi}{M}(k+1)}\int_0^{\frac{2\pi}{M}} E^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}_{1,1}Q^{\theta_A,\theta_B,\frac{\nu}{2},\frac{\nu}{2}}_{1,1}d\theta_A d\theta_B.
\end{aligned}
\tag{40}
$$

By using the decoy-state method, the lower and upper bounds of yield Y^{1XXk}_{TF}, Y^{1XYk}_{TF}, Y^{1YXk}_{TF} and Y^{1YYk}_{TF} will be

$$
\begin{aligned}
Y^{1XXk}_{\mathrm{TF}} &\geq Y^{1XXkL}_{\mathrm{TF}} = \frac{\nu}{\nu\omega-\omega^2}\left(e^{\omega}Q^{\omega}_{XXk} - \frac{\omega^2}{\nu^2}e^{\nu}Q^{\nu}_{XXk} - \frac{\nu^2-\omega^2}{\nu^2}Q^0\right),\\
Y^{1XYk}_{\mathrm{TF}} &\geq Y^{1XYkL}_{\mathrm{TF}} = \frac{\nu}{\nu\omega-\omega^2}\left(e^{\omega}Q^{\omega}_{XYk} - \frac{\omega^2}{\nu^2}e^{\nu}Q^{\nu}_{XYk} - \frac{\nu^2-\omega^2}{\nu^2}Q^0\right),\\
Y^{1YXk}_{\mathrm{TF}} &\geq Y^{1YXkL}_{\mathrm{TF}} = \frac{\nu}{\nu\omega-\omega^2}\left(e^{\omega}Q^{\omega}_{YXk} - \frac{\omega^2}{\nu^2}e^{\nu}Q^{\nu}_{YXk} - \frac{\nu^2-\omega^2}{\nu^2}Q^0\right),\\
Y^{1YYk}_{\mathrm{TF}} &\geq Y^{1YYkL}_{\mathrm{TF}} = \frac{\nu}{\nu\omega-\omega^2}\left(e^{\omega}Q^{\omega}_{YYk} - \frac{\omega^2}{\nu^2}e^{\nu}Q^{\nu}_{YYk} - \frac{\nu^2-\omega^2}{\nu^2}Q^0\right),
\end{aligned}
\tag{41}
$$

and

$$
\begin{aligned}
Y^{1XXk}_{\mathrm{TF}} &\leq Y^{1XXkU}_{\mathrm{TF}} = \frac{e^{\omega}Q^{\omega}_{XXk} - Q^0}{\omega}, \quad Y^{1XYk}_{\mathrm{TF}} \leq Y^{1XYkU}_{\mathrm{TF}} = \frac{e^{\omega}Q^{\omega}_{XYk} - Q^0}{\omega},\\
Y^{1YXk}_{\mathrm{TF}} &\leq Y^{1YXkU}_{\mathrm{TF}} = \frac{e^{\omega}Q^{\omega}_{YXk} - Q^0}{\omega}, \quad Y^{1YYk}_{\mathrm{TF}} \leq Y^{1YYkU}_{\mathrm{TF}} = \frac{e^{\omega}Q^{\omega}_{YYk} - Q^0}{\omega}.
\end{aligned}
\tag{42}
$$

The lower and upper bounds of QBER e^{b1}_{XXk}, e^{b1}_{XYk}, e^{b1}_{YXk} and e^{b1}_{YYk} can be given by

$$
\begin{aligned}
e^{b1}_{XXk} &\geq e^{b1L}_{XXk} = \frac{\nu}{(\nu\omega-\omega^2)Y^{1XXkU}_{\mathrm{TF}}}\left(e^{\omega}E^{\omega}_{XXk}Q^{\omega}_{XXk} - \frac{\omega^2}{\nu^2}e^{\nu}E^{\nu}_{XXk}Q^{\nu}_{XXk} - \frac{\nu^2-\omega^2}{\nu^2}e^{b0}Q^0\right),\\
e^{b1}_{XYk} &\geq e^{b1L}_{XYk} = \frac{\nu}{(\nu\omega-\omega^2)Y^{1XYkU}_{\mathrm{TF}}}\left(e^{\omega}E^{\omega}_{XYk}Q^{\omega}_{XYk} - \frac{\omega^2}{\nu^2}e^{\nu}E^{\nu}_{XYk}Q^{\nu}_{XYk} - \frac{\nu^2-\omega^2}{\nu^2}e^{b0}Q^0\right),\\
e^{b1}_{YXk} &\geq e^{b1L}_{YXk} = \frac{\nu}{(\nu\omega-\omega^2)Y^{1YXkU}_{\mathrm{TF}}}\left(e^{\omega}E^{\omega}_{YXk}Q^{\omega}_{YXk} - \frac{\omega^2}{\nu^2}e^{\nu}E^{\nu}_{YXk}Q^{\nu}_{YXk} - \frac{\nu^2-\omega^2}{\nu^2}e^{b0}Q^0\right),\\
e^{b1}_{YYk} &\geq e^{b1L}_{YYk} = \frac{\nu}{(\nu\omega-\omega^2)Y^{1YYkU}_{\mathrm{TF}}}\left(e^{\omega}E^{\omega}_{YYk}Q^{\omega}_{YYk} - \frac{\omega^2}{\nu^2}e^{\nu}E^{\nu}_{YYk}Q^{\nu}_{YYk} - \frac{\nu^2-\omega^2}{\nu^2}e^{b0}Q^0\right),
\end{aligned}
\tag{43}
$$

and

$$
\begin{aligned}
e^{b1}_{XXk} &\leq e^{b1U}_{XXk} = \frac{e^{\omega}E^{\omega}_{XXk}Q^{\omega}_{XXk} - e^{b0}Q^0}{\omega Y^{1XXkL}_{\mathrm{TF}}}, \quad e^{b1}_{XYk} \leq e^{b1U}_{XYk} = \frac{e^{\omega}E^{\omega}_{XYk}Q^{\omega}_{XYk} - e^{b0}Q^0}{\omega Y^{1XYkL}_{\mathrm{TF}}},\\
e^{b1}_{YXk} &\leq e^{b1U}_{YXk} = \frac{e^{\omega}E^{\omega}_{YXk}Q^{\omega}_{YXk} - e^{b0}Q^0}{\omega Y^{1YXkL}_{\mathrm{TF}}}, \quad e^{b1}_{YYk} \leq e^{b1U}_{YYk} = \frac{e^{\omega}E^{\omega}_{YYk}Q^{\omega}_{YYk} - e^{b0}Q^0}{\omega Y^{1YYkL}_{\mathrm{TF}}}.
\end{aligned}
\tag{44}
$$

For the practical TF-QKD with RFI scheme, we need to calculate the minimum value of C^1_k. Therefore, for the value

$$
C^1_k = (1-2e^{b1}_{XXk})^2 + (1-2e^{b1}_{XYk})^2 + (1-2e^{b1}_{YXk})^2 + (1-2e^{b1}_{YYk})^2,
\tag{45}
$$

we have

$$
e^{b1}_{XXk} = \begin{cases} e^{b1U}_{XXk}, & e^{b1U}_{XXk} \leq \frac{1}{2},\\ e^{b1L}_{XXk}, & e^{b1L}_{XXk} \geq \frac{1}{2},\\ \frac{1}{2}, & e^{b1L}_{XXk} \leq \frac{1}{2} \leq e^{b1U}_{XXk}, \end{cases}
\tag{46}
$$

the parameters e^{b1}_{XYk}, e^{b1}_{YXk} and e^{b1}_{YYk} are similar with the case of e^{b1}_{XXk}.

References

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. In *Proceedings of the Conference on Computers, Systems and Signal Processing*, 175–179 (IEEE Press, New York, 1984).
2. Scarani, V. *et al*. The security of practical quantum key distribution. *Rev. Mod. Phys.* **81**, 1301–1350 (2009).
3. Weedbrook, C. *et al*. Gaussian quantum information. *Rev. Mod. Phys.* **84**, 621–669 (2012).
4. Boaron, A. *et al*. Secure quantum key distribution over 421 km of optical fiber. *Phys. Rev. Lett.* **121**, 190502 (2018).
5. Liao, S.-K. *et al*. Satellite-to-ground quantum key distribution. *Nature* **549**, 43 (2017).
6. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nature Commun.* **5**, 5235 (2014).
7. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nature Commun.* **8**, 15043 (2017).
8. Duan, L.-M., Lukin, M., Cirac, J. I. & Zoller, P. Long-distance quantum communication with atomic ensembles and linear optics. *Nature* **414**, 413 (2001).
9. Sangouard, N., Simon, C., de Riedmatten, H. & Gisin, N. Quantum repeaters based on atomic ensembles and linear optics. *Rev. Mod. Phys.* **83**, 33–80 (2011).
10. Azuma, K., Tamaki, K. & Munro, W. J. All-photonic intercity quantum key distribution. *Nature Commun.* **6**, 10171 (2015).
11. Qiu, J. *et al*. Quantum communications leap out of the lab. *Nature* **508**, 441–442 (2014).
12. Lucamarini, M., Yuan, Z., Dynes, J. & Shields, A. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400–403 (2018).
13. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
14. Tamaki, K., Lo, H.-K., Wang, W. & Lucamarini, M. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. *arXiv:1805.05511* (2018).
15. Ma, X., Zeng, P. & Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **8**, 031043 (2018).
16. Wang, X.-B., Yu, Z.-W. & Hu, X.-L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **98**, 062323 (2018).
17. Cui, C. *et al*. Phase-matching quantum key distribution without phase post-selection. *arXiv:*1807.*02334* (2018).
18. Curty, M., Azuma, K. & Lo, H. -K. Simple security proof of twin-field type quantum key distribution protocol. *arXiv*:*1807*.07667 (2018).
19. Lin, J. & Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **98**, 042332 (2018).
20. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *Science* **283**, 2050–2056 (1999).
21. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Phys. Rev. Lett.* **85**, 441 (2000).
22. Kraus, B., Gisin, N. & Renner, R. Lower and upper bounds on the secret-key rate for quantum key distribution protocols using one-way classical communication. *Phys. Rev. Lett.* **95**, 080501 (2005).
23. Tomamichel, M. & Renner, R. Uncertainty relation for smooth entropies. *Phys. Rev. Lett.* **106**, 110506 (2011).
24. Gottesman, D., Lo, H.-K., Lütkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. *Quantum Inf. Comput.* **4**, 325 (2004).
25. Hwang, W.-Y. Quantum key distribution with high loss: toward global secure communication. *Phys. Rev. Lett.* **91**, 057901 (2003).
26. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Phys. Rev. Lett.* **94**, 230503 (2005).
27. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Phys. Rev. Lett.* **94**, 230504 (2005).
28. Lo, H.-K. Proof of unconditional security of six-state quantum key distribution scheme. *Quantum Inf. Comput.* **1**, 81 (2001).
29. Laing, A., Scarani, V., Rarity, J. G. & OBrien, J. L. Reference-frame-independent quantum key distribution. *Phys. Rev. A* **82**, 012304 (2010).
30. Sciarrino, F., Lombardi, E., Milani, G. & De Martini, F. Delayed-choice entanglement swapping with vacuum–one-photon quantum states. *Phys. Rev. A* **66**, 024309 (2002).
31. Lombardi, E., Sciarrino, F., Popescu, S. & De Martini, F. Teleportation of a vacuum–one-photon qubit. *Phys. Rev. Lett.* **88**, 070402 (2002).
32. Pawłowski, M. *et al*. Information causality as a physical principle. *Nature* **461**, 1101 (2009).
33. Wang, C. *et al*. Phase-reference-free experiment of measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **115**, 160502 (2015).
34. Yin, H.-L. *et al*. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Phys. Rev. Lett.* **117**, 190501 (2016).
35. Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Phys. Rev. A* **93**, 042324 (2016).
36. Guan, J.-Y. *et al*. Observation of quantum fingerprinting beating the classical limit. *Phys. Rev. Lett.* **116**, 240502 (2016).
37. Zhao, Y., Qi, B., Lo, H.-K. & Qian, L. Security analysis of an untrusted source for quantum key distribution: passive approach. *New J. Phys.* **12**, 023024 (2010).
38. Yin, H.-L., Fu, Y., Mao, Y. & Chen, Z.-B. Security of quantum key distribution with multiphoton components. *Sci. Rep.* **6**, 29482 (2016).

Acknowledgements

We thank W. Zhu for the help with the figure. H.-L. Yin gratefully acknowledges support from the National Natural Science Foundation of China under Grant No. 61801420, the Fundamental Research Funds for the Central Universities.

Author Contributions

H.-L.Y. and Y.F. have the main idea. All results are acquired through the discussion among all authors. All authors contribute to the writing and reviewing of the manuscript.

Additional Information

Competing Interests: The authors declare no competing interests.

Publisher's note: Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.