SCIENTIFIC REPORTS
nature research

OPEN

Phase Matching Quantum Key Distribution based on Single-Photon Entanglement

Wei Li[1,2,3], Le Wang[1,2] & Shengmei Zhao[1,2*]

Two time-reversal quantum key distribution (QKD) schemes are the quantum entanglement based device-independent (DI)-QKD and measurement-device-independent (MDI)-QKD. The recently proposed twin field (TF)-QKD, also known as phase-matching (PM)-QKD, has improved the key rate bound from $O(\eta)$ to $O(\sqrt{\eta})$ with η the channel transmittance. In fact, TF-QKD is a kind of MDI-QKD but based on single-photon detection. In this paper, we propose a different PM-QKD based on single-photon entanglement, referred to as single-photon entanglement-based phase-matching (SEPM)-QKD, which can be viewed as a time-reversed version of the TF-QKD. Detection loopholes of the standard Bell test, which often occur in DI-QKD over long transmission distances, are not present in this protocol because the measurement settings and key information are the same quantity which is encoded in the local weak coherent state. We give a security proof of SEPM-QKD and demonstrate in theory that it is secure against all collective attacks and beam-splitting attacks. The simulation results show that the key rate enjoys a bound of $O(\sqrt{\eta})$ with respect to the transmittance. SEPM-QKD not only helps us understand TF-QKD more deeply, but also hints at a feasible approach to eliminate detection loopholes in DI-QKD for long-distance communications.

Quantum key distribution (QKD), a secure communication method to enabling a secret random number string to be shared by two well-separated parties, says Alice and Bob, has been proven to be robust against channel attacks and against the power of quantum computation[1,2]. The random number string, known only to Alice and Bob, can be used to encrypt messages transmitted between them. In theoretical research, the work has focused on the security of QKD taking into consideration the imperfections of actual devices[3–7]. In practical applications, research on the extractable key rate has been categorized as focusing on improving the key rate, such as decoy state protocols[8–12], asymmetric coding[13,14], higher dimensional systems[15–20], and parameter optimization[21–24], or focusing on improving the key transmission distance[13,25,26].

In addition to the recent satellite QKD scheme[27], the current mainstream QKD is based on photon transmission over optical fiber. For a given QKD scheme, the factors that determine the key rate and transmission distance are the error rate and the transmittance η. In the initial stage of QKD research, a single-photon was used as the carrier of quantum information and secret key rate was bounded to $O(\eta)$[28,29], which is equal to the maximum probability of successful detection of a single-photon state. The measurement-device-independent (MDI)-QKD proposed latter is based on the correlation measurement of a two-photon state and closed all detection loopholes[25,30]. Regardless of the technical challenges of practical experiments, the transmission distance of MDI-QKD almost doubled compared with BB84. However, the transmittance for a single-photon in MDI-QKD is unchanged, and so the key rate is still bounded by $O(\eta)$.

In Lucamarini *et al.* (2018) the twin-field (TF)-QKD[31], also known as phase-matching (PM)-QKD by Ma *et al.*[32], was proposed to improve the key rate and was shown to beat the PLOB bound[29]. TF-QKD and PM-QKD are essentially identical, the former reflects what states are used to carry the keys, and the latter reflects how the keys are generated. After that, some variants of TF-QKD have been proposed, such as the sending or not sending protocol by Wang *et al.*[33,34] and removing of phase randomization and postselection in the coding mode by cui *et al.*[35]. TF-QKD is a single-photon version of MDI-QKD[36,37], in which a single count is used to extract the quantum key. In TF-QKD, the information carrier is no longer a single photon but a weak coherent field or wave state with

[1]Nanjing University of Posts and Telecommunications, Institute of Signal Processing and Transmission, Nanjing, 210003, China. [2]Nanjing University of Posts and Telecommunications, Key Lab Broadband Wireless Communication and Sensor Network, Ministy of Education, Nanjing, 210003, China. [3]National Laboratory of Solid State Microstructures, Nanjing University, Nanjing, 210093, China. *email: zhaosm@njupt.edu.cn

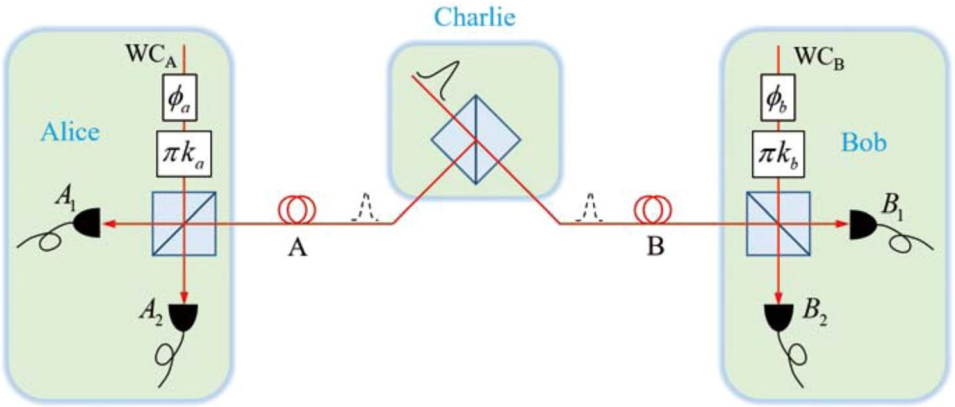

Figure 1. Schematic diagram of SEPM-QKD. An untrusted third party, Charlie, generates single-photon entanglement, by injecting a photon from a heralded single-photon source into a beam splitter. Alice and Bob generate a local weak coherent (WC) state $\left|\gamma e^{i\left(\phi_{a(b)}+k_{a(b)}\pi\right)}\right\rangle$ with $\phi_{a(b)} \in \left\{-\frac{\pi}{4}, 0, \frac{\pi}{4}, \frac{\pi}{2}\right\}$ and $k_{a(b)} \in \{0, 1\}$ to test the quantum nonlocal correlation in wave space and generate the final key. $\phi_{a(b)}$ is a random phase used to construct Bell inequality and is also used for phase matching measurement. Random bit $k_{a(b)}$ can be regarded as the measurement setup for homodyne detection of wave-state.

definite phase and amplitude[37]. Independent coherent states with locked global phase can interfere with each other, so they can be used in phase matching to extract keys. A weak coherent state can be approximated as a coherent superposition of a vacuum state and a single photon state. The detection probability has a $\sqrt{\eta}$ dependence on the channel transmittance, which leads to a bound for key rate of $O(\sqrt{\eta})$. Because η is a quantity less than 1, this protocol further enhances the transmission distance of rate keys in optical fibers.

Indeed, MDI-QKD itself may be regarded as a time-reversed version of an entanglement-based device-independent (DI)-QKD[38,39], and therefore conclude that TF-QKD is a time-reversed version of the single-photon entanglement-based DI-QKD. Over 30 years ago, scientists proposed and experimentally verified the existence of single-photon entanglement and confirmed the Bell inequalities for quantum correlations in different forms[40–45]. Subsequently, single-photon-entanglement-based DI-QKD was proposed in which the key is extracted according to whether Alice or Bob has detected that photon[46]. However, this work did not attract much attention, let alone the relationship between this protocol and TF-QKD. In our previous work[47], we proposed confirming Bell inequalities for single-photon entanglement from joint measurements in wave space-the conjugate space of the photon number space. As a new carrier of quantum information, the wave state has similar properties to the weak coherent state; both can be viewed as a coherent superposition of a vacuum state and a single-photon state. In this paper, we propose single-photon entanglement-based phase-matching (SEPM)-QKD, which is actually a TF-QKD with quantum entanglement. In this protocol, single-photon entanglement provides the quantum link in the communications between Alice and Bob, who choose the two groups of phases to encode the key. Monitoring Eve's eavesdropping is performed by detecting violations of Bell inequality. Security proofing against collective attacks and beam-splitting attacks is thereby established. We also compare the key rate of SEPM-QKD with the wave-state-based QKD, as for TF(PM)-QKD and single-photon-based QKD, like the BB84- and MDI-QKD protocols.

Theory of Single Photon Entanglement

The physical basis of SEPM-QKD is the detection of single-photon entanglement in wave space, (Fig. 1). When a third-party Charlie directs a single-photon state onto an optical beam splitter, the photon states at the two output ports may be regarded as an entangled state of a vacuum state $|0\rangle$ and a single-photon state $|1\rangle$ in the two path modes[40]

$$|\Psi_{A,B}\rangle = \frac{\sqrt{2}}{2}[e^{i\theta}|1\rangle_A|0\rangle_B + |0\rangle_A|1\rangle_B], \tag{1}$$

where $e^{i\theta}$ is the accumulated phase difference between the two arms. Because the production of a single-photon from a single-photon source is probabilistic, a heralded single-photon source can be used to increase the proportion of effective counting. Equation (1) is a representation of single-photon entanglement in photon-number space. Based on the wave-particle duality in quantum mechanics, it is convenient to call the conjugate space of this photon number space the wave space. Applying a two-dimensional Fourier transformation, we obtain single-photon entanglement in the conjugate space

$$|\Psi_{A,B}\rangle = \frac{\sqrt{2}}{2}e^{i(\theta-\alpha)}[|\alpha_A\rangle_w|(\alpha-\theta)_B\rangle_w - |(\alpha+\pi)_A\rangle_w|(\alpha-\theta+\pi)_B\rangle_w], \tag{2}$$

where states with a subscript w denote wave states, α and $\alpha - \theta$ each with a value ranging from 0 to 2π denotes the phase characterizing Alice's and Bob's wave state. The pair of orthogonal bases states in wave space are

$$\begin{aligned} |\alpha\rangle_w &= \frac{\sqrt{2}}{2}[|0\rangle + e^{i\alpha}|1\rangle], \\ |\alpha + \pi\rangle_w &= \frac{\sqrt{2}}{2}[|0\rangle - e^{i\alpha}|1\rangle]. \end{aligned} \tag{3}$$

It is these states that are used to distribute the quantum correlation between Alice and Bob.

Next, we analyze single-photon entanglement in wave space. Here we refer to the photon states $|\alpha\rangle_w, |\alpha + \pi\rangle_w$ as the Z basis if $\alpha = 0$, and $|\alpha\rangle_w, |\alpha + \pi\rangle_w$ as the Y basis if $\alpha = \frac{\pi}{2}$; then the states $|0\rangle$ and $|1\rangle$ belong to the X basis. We can see that the entanglement between Alice and Bob in the wave space is entirely determined by the value of phase θ. Because the value of α is any real number, then, if we set the value of θ to zero, the initial single-photon entangled state is the Bell state $|\Phi^-_{A,B}\rangle_w$, which is rotationally symmetric in the ZY plane. It should be noted that θ can also be set to other values, but the way they generate keys will change accordingly.

In our previous work, we demonstrated that a wave state could be measured through interference with a reference weak coherent state[47], as shown in the measurement device at the sites of Alice and Bob. Assuming that the weak coherent states selected by Alice and Bob are $|\gamma e^{i\alpha}\rangle$ and $|\gamma e^{i\beta}\rangle$ where γ is a small amplitude far less than 1, the weak coherent state has the approximate form

$$|\gamma e^{i\alpha}\rangle \approx |0\rangle + \gamma e^{i\alpha}|1\rangle + O(\gamma)|\text{other}\rangle, \tag{4}$$

where α and β are the phase values of the wave states of Alice and Bob, the state $|\text{other}\rangle$ with an infinitesimal amplitude is a coherent combination of Fock states whose photon number is greater than or equal to 2. Taking into account the transmittance of a single photon η in the optical channel, the dependence of the measurement results on measurement settings α and β reads

$$p(A_i, B_j) = \frac{\gamma^2\eta}{4}[1 + (-1)^{i+j}\cos(\alpha - \beta)] + \frac{\gamma^4}{4}, \tag{5}$$

where $i, j \in \{1, 2\}$ are the ordinal numbers the single-photon detectors of Alice and Bob. The first term represents the wave-like correlation between Alice and Bob, while the second term represents the particle-like correlation between them[47]. If the intensity of the weak coherent field γ^2 is far less than the transmittance η, then the second term on the right-hand side of Eq. (4) may be omitted. Now the time reversal relationship between SEPM-QKD and TF-QKD can be clearly revealed in the wave-state representation. In TF-QKD, Alice and Bob send wave-states, i.e. weak coherent states, to the third party Charlie for Bell state measurements[31,37]. While in SEPM-QKD, Charlie sends the wave-entangled states to Alice and Bob to construct non-localized quantum correlations. In time order, the quantum state transmission and measurement of the two protocols are completely opposite. The key generation in both protocols comes from the wave-state correlation between Alice and Bob. According to the above analysis, the single-photon entanglement-based PM-QKD protocol is described as follows.

SEPM-QKD Protocol

State preparation. A single-photon state from a third untrusted party Charlie is sent to a 50:50 optical beam splitter to produce a single-photon entangled state close to the maximum entanglement. Next, he sends the photon states to Alice and Bob through two identical fibers with the same transmittance η. Because of channel noise and Eve's possible attack, the photon states reaching the terminals of Alice and Bob are not restricted to ideal single-photon entanglement.

Selection of measurement settings. With different phase-locking methods[48,49], the lase source of Alice and Bob are perfectly locked to achieve athe same global phase. Alice generates a random bit string k_a in which each bit takes value $k_a \in \{0, 1\}$ and a random phase $\phi_a \in \left\{-\frac{\pi}{4}, 0, \frac{\pi}{4}, \frac{\pi}{2}\right\}$ corresponding to the measurements $(\sigma_Z - \sigma_Y)/\sqrt{2}$, σ_Z, $(\sigma_Z + \sigma_Y)/\sqrt{2}$, σ_Y and then prepares the corresponding weak coherent state $|\gamma e^{i(\phi_a + k_a\pi)}\rangle$. Simultaneously, Bob generates a weak coherent state $|\gamma e^{i(\phi_b + k_b\pi)}\rangle$ in which $k_b \in \{0, 1\}$ and $\phi_b \in \left\{-\frac{\pi}{4}, 0, \frac{\pi}{4}, \frac{\pi}{2}\right\}$. Alice and Bob interfere their weak coherent states with the single-photon state distributed by Charlie to measure the wave states and the interference results are recorded as the joint counting of the single-photon detectors on both sides.

Announcement. When all measurements are completed, Alice and Bob announce their detection results, i.e., the ordinal numbers of the fired single-photon detectors, and the phase values ϕ_a and ϕ_b.

Sifting. A successful detection event is defined as having only one detector response on both sides at a given time. After they have announced the phases ϕ_a and ϕ_b, the secret key is extracted when $\phi_a = \phi_b$. If the sum of the ordinal number $i + j$ is an even number, Alice and Bob keep their raw key; if $i + j$ is an odd number, then Bob flips his key.

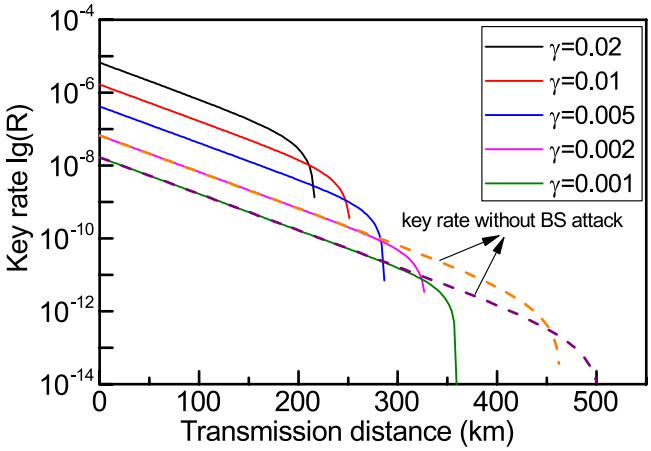

Figure 2. Simulation of SEPM-QKD under intensities of local coherent light. The key rate decreases with increasing attenuation of the coherent light intensity whereas the transmission distance increases as the attenuation increases. When the average photon-number of the coherent state is far less than 1, the key rate is approximately proportional to the square of the amplitude of the coherent state according to Eq. 14. For coherent states with high intensity, the proportion of the particle-like correlation between Alice and Bob will also increase (Eq. 5). This will increase the bit error rate of the final key, so the transmission distance will be reduced. In addition, there are two more key rate curves, orange and purple dotted lines, which correspond to the fitting results without considering beam-splitting (BS) attacks. It can be found that the BS attack will have an important effect on the key rate at long transmission distance.

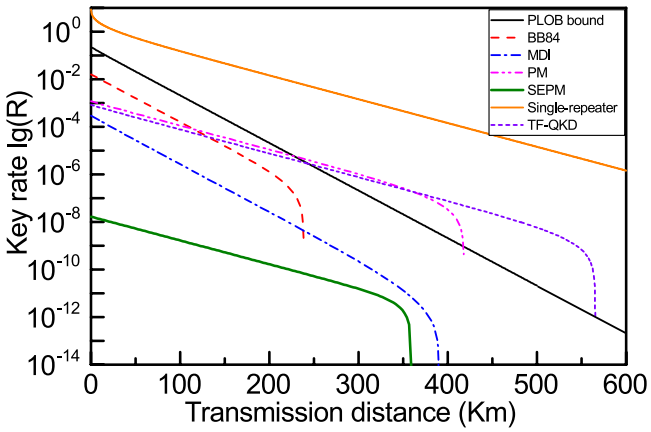

Figure 3. Key rate comparison between different QKD protocols. The simulation results of the other QKD are taken from refs[31,32]. Compared with single-photon based BB84- and MDI-QKD schemes which obey the PLOB bound by Pirandola *et al.* (PLOB bound)[29], SEPM-QKD has the same $\sqrt{\eta}$ dependence on transmission distance as PM-QKD and TF-QKD which obey the single-repeater bound[59]. In BB84- and MDI-QKD protocols, the carrier of information is a single-photon, and the detection probability is proportional to the transmission coefficient η, so the key rate has a η on the transmission distance. While for PM- and SEPM-QKD protocols, the carrier of information is a wave-photon, and the detection probability is proportional to the square root of the transmission coefficient $\sqrt{\eta}$, so the key rate has a $\sqrt{\eta}$ on the transmission distance. In the simulation of SEPM-QKD, the amplitude of coherent state is $\gamma = 0.001$. Its average intensity is several orders of magnitude lower than that in other QKD protocols and BS attack is also considered in SEPM-QKD, which results in the key rate of SEPM-QKD being much lower than that of other QKD protocols.

Parameter estimation. With a single-photon entanglement distribution, a bit-flipping error on the X basis can never happen, otherwise photon number conservation is violated. In addition to entanglement degradation caused by channel transmission loss, information loss is mainly caused by phase noise, i.e., bit flipping on Z and Y bases. During the measurement, the selection of the Z and Y bases is equivalent, so the bit error rates on the two bases, e_Z and e_Y, are equal. Alice and Bob agree on a random bit string with half the length of the sifted key to be check-bit to measure the bit error rate e. Next, they use part of the remaining data in which $|\phi_a - \phi_b| = \frac{\pi}{4}$ to construct the Bell function S on the ZY plane to estimate the maximal information that may have leaked to Eve.

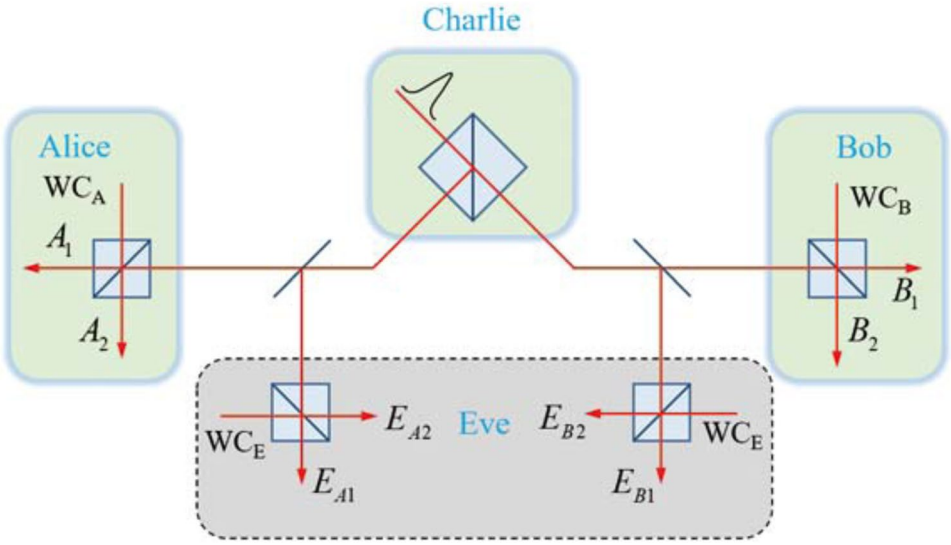

Figure 4. Schematic diagram of BS attack. Suppose that the transmission loss of a single-photon state is captured and stored by Eve in BS attack scheme. In this attack scheme, Eve synchronizes his light source with Alice and Bob's. After Alice and Bob publicly announce random phase values, selection of measurement bases and response results of detectors, Eve uses the same measurement method to measure the stored photon states. Eve finally infers Alice and Bob's keys based on his measurement result $E_{A,B}$.

Key distillation. In the post-processing, Alice and Bob perform error corrections in accordance with the bit error rate e and privacy amplification according to the Bell function S to generate the final secret key.

Security of SEPM-QKD

In SEPM-QKD, the key is distributed through a non-localized single-photon entangled state. Alice and Bob measure entangled states jointly. When entangled states are eigenstates of joint measurement operators, their measurements are perfectly correlated. They can extract keys based on joint measurement results or measurement settings. Eve's attack can be monitored based on violations of Bell's inequality. At first glance, this protocol belongs to DI-QKD. Although conventional DI-QKD is secured in theory, it is nevertheless difficult to distribute keys over long distances due to detection loopholes.

Here, we point out that the detection loophole in the standard Bell experiment will not be a factor affecting the key security of the protocol. Previously, it was found that the security of QKD can be related to entanglement purification[3,4]. The amount of security information that can be extracted between Alice and Bob is determined by the amount of purifiable entanglement. In DI-QKD, we certify that the bound of the accessible private key is determined by how much entanglement we can distill from the imperfect entangled state[50–52].

In a standard Bell experiment, to give a rigorous proof of quantum delocalization, all loopholes in the experiment need to be closed, including the efficiency of the detector and transmission loss[53]. For the DI-QKD protocol, we just need to accept quantum delocalization as rigorous and correct. After solving this issue, DI-QKD is equivalent to the BB84 protocol. In this protocol, we only focus on the data that can be measured successfully. In a conventional Bell experiment with polarization entanglement, the measurement in the Z– and X– bases needs the switching of the angle of the polarizers, which must be perfectly correlated with the secret key. This may leave Eve a chance to fabricate the measurement settings if she takes full control of the measurement setup. In the following, we need to establish whether in such an event Eve could fabricate a fake result of the Bell's inequality test given the limited information publicly announced by Alice and Bob.

In SEPM-QKD, Alice and Bob encode the key information in the phases of the weak coherent states. The encoding is equivalent to the measurement settings, and no switch of the measurement basis is needed. If this initial key information had been leaked to Eve, all QKD protocols would fail. From Eq. (5), the quantum measurement of the protocol may be considered to consist of three systems: the single-photon entangled state $|\Phi^{-}_{A,B}\rangle$, the joint states of the single-photon detector D, and the corresponding joint key states K. The initial state of the total system is written

$$\rho_{(A,B)DK} = \rho_{A,B}|N_{in}\rangle\langle N_{in}||\kappa_{in}\rangle\langle\kappa_{in}|, \tag{6}$$

which is a tensor product of the three subsystems, with $\rho_{A,B}$ the single-photon entangled state sent by Charlie, and $|N_{in}\rangle$ and $|\kappa_{in}\rangle$ the initial joint states of the two-sided single-photon detectors and the key state with $N = i + j$ and $\kappa = |k_a - k_b|$. Measurement is in general regarded as a unitary operation of the system; the joint measurement performed by Alice and Bob with two POVM elements $\{E_\kappa\}$ may be written as

$$\varepsilon(\rho_{(A,B)DK}) = E_0^+\rho_{A,B}E_0|even\rangle\langle even||0\rangle\langle 0| + E_1^+\rho_{A,B}E_1|odd\rangle\langle odd||1\rangle\langle 1|. \tag{7}$$

Once the QKD-protocol is determined, after the announcement of N publicly, the information of κ may be revealed by Eve. However, she still does not know the exact value of k_a and k_b. At this stage, we find SEPM-QKD is equivalent to MDI-QKD. Eve barely gets any information about the measurement settings of Alice and Bob, so it is almost impossible for her to successfully fabricate the measurement results to cheat Alice and Bob.

With the presence of channel transmission losses and the imperfections in detection, Eve has the opportunity to implement various attack schemes. Even though a purification scheme for single-photon entanglement regarding phase noise have been provided[54,55], the reality is more complicated. Alice and Bob's extractable fully secure key rate has a lower bound given by[24,50,56]

$$r \geq I(A{:}B) - \chi(AB{:}E), \tag{8}$$

where $I(A{:}B) = H(A) - H(A|B)$ is the mutual information between Alice and Bob, which is equal to $1 - H(e)$, and $\chi(AB{:}E) = S\left(\rho_{AB|i,j}\right) - \sum_c p(c)S\left(\rho^c_{AB|i,j}\right)$ the Holevo quantity between Eve and Alice and Bob after the ordinal numbers i, j have been announced publicly, here, the quantity $H(e)$ is the amount of information loss due to bit flipping errors, and $\chi(AB{:}E)$ is the maximum amount of information Eve obtains from ρ_{AB} at a given error rate e, and for values of i, j and ϕ_a, ϕ_b.

There are two kinds of attack schemes on Alice and Bob that Eve could implement; they correspond to the two Holevo quantities $\chi(AB{:}E)$. One is a collective attack in which Eve correlates her system with the joint system of Alice and Bob and produces a total quantum state ρ_{ABE}. In this protocol, Eve can not get any information about the measurement settings, so she can't control the measurement process effectively. Her only freedom is to generate the joint quantum state, in which the results of Alice and Bob's reduced states are consistent with predictions from theory, taking into account the imperfections in the equipment.

Under the idea of coherent attack, Eve uses weak measurements to obtain information of quantum states. The limitation of the attack is that the delocalized quantum correlation between Alice and Bob is within the acceptable range of them. For uniformly random marginals in the ZY plane, Eve's maximal collective attack will be saturated by sending the entangled single-photon state of which he holds a purification[50]

$$|\Psi_{ABE}\rangle = \frac{1}{2}(I + H_AH_B)\left[\sqrt{1-2e}\,|E_0\rangle|\Phi^-_{AB}\rangle_z + \sqrt{2e}\,|E_1\rangle|\Phi^+_{AB}\rangle_z\right], \tag{9}$$

where I is the identity density operator, H_A and H_B are Hadamard matrices operated on Alice's and Bob's wave states in ZY plane, which transform Z basis to Y basis, $|E_0\rangle$ and $|E_1\rangle$ are the two orthogonal states hold by Eve, $|\Phi^{\pm}_{AB}\rangle_z$ are the Bell states under the representation of Z basis. A simple derivation of Eve's maximum collective attack is given in the method section. We find that the maximum violation of the CHSH-Bell inequality is $S = 2\sqrt{2}(1 - 2e)$.

We readily find that $\chi_1(AB{:}E) \leq 2e$, which means that whenever Alice and Bob negotiate one bit of information, Eve can successfully steal $2e$ bit of information. Next, we examine the scope of the Bell-inequality verification. Assume that Eve intercepts the single-photon entangled state and induce a certain amount of error rate. The maximum error rate that Bell inequality tolerates is 14.6%, which is larger than 11%[4], the maximum error rate that Alice and Bob can tolerate in extracting finite information against Eve's collective attacks. Therefore, violation tests of Bell's inequality violation are a feasible scheme for monitoring Eve's collective attack.

The other possible attack scenario for Eve is the beam-splitting (BS) attack, in which the loss of a single-photon entangled state in optical channels can be considered to be stored by Eve and measured after Alice and Bo have announced publicly their measurement basis and random phase, as shown in Fig. 4. Thus, the BS attack is an individual attack that is independent of a collective attack and can not be found with Bell's inequality tests. Considering channel loss, the single-photon state between Alice, Bob, and Eve is written

$$\begin{aligned}|\Psi_{ABE}\rangle = \frac{\sqrt{2}}{2}\Big[&\sqrt{\eta}(|1_A0_B\rangle + |0_A1_B\rangle)\left|0_{E_A}0_{E_B}\right\rangle \\ &+ \sqrt{1-\eta}|0_A0_B\rangle\left(\left|1_{E_A}0_{E_B}\right\rangle + \left|0_{E_A}1_{E_B}\right\rangle\right)\Big],\end{aligned} \tag{10}$$

which is a single-photon multi-mode asymmetric W-state[57,58], where $\frac{\sqrt{2}}{2}\left(\left|1_{E_A}0_{E_B}\right\rangle + \left|0_{E_A}1_{E_B}\right\rangle\right)$ is the state responsible for channel loss, which is assumed to be stored by Eve, whose system is entangled with the systems of Alice and Bob. Suppose Eve uses weak coherent light of the same intensity as Alice and Bob to measure the wave state. After Alice and Bob announce their random phases ϕ_a, ϕ_b as well as the ordinal numbers i, j of the single-photon detectors, for a given channel transmittance η and local coherent field amplitude γ, the maximum information that Eve can gain from Alice and Bob is

$$\chi_2(AB{:}E) = \frac{\gamma^4(1 + 3\eta + 2\gamma^2)}{4}[1 - H(p(\eta, \gamma))], \tag{11}$$

where the quantity $p(\eta, \gamma)$ is the normalized probability that Eve uses to guess the key of Alice and Bob; its expression is

$$p(\eta) = \frac{1 + 3\eta - 4\sqrt{\eta(1-\eta)} + 2\gamma^2}{2 + 6\eta + 4\gamma^2}. \tag{12}$$

See the derivation in the method section. Now, if the BS attack is not considered, the key rate in Eq. (8) is found to be equal to the amount of entanglement that can be distilled between Alice and Bob. This security proof is equivalent to the security proof of BB84 QKD based on entanglement purification[3,4]. The loss of these two parts of the information corresponds to an error correction and private amplification in post-processing. After considering Eve's two attack schemes, the lost information for private amplification should be recalibrated.

Simulation and Discussion

Next, we simulate the distance-dependent key rate in a practical situation. Among all the successful detection events, there are three kinds of false detection events, which constitute the detection error rate e. These events come from dark counting of detectors, phase insensitive interference, and phase misalignment. For all single-photon detectors with the same dark count rate p_{dark}, the rate of successful detection events $p_{r,dark}$ and false detection events $p_{e,dark}$ caused by dark counting are both equal to $2p_{dark}^2$. For the joint measurement of wave states, there is a small portion of detection events stemming from phase-insensitive interference, a HOM-type of interference. The rate for joint HOM interference is $p_{HOM} = \gamma^4\eta_d^2/4$ with η_d the detection efficiency of the single-photon detectors, and gives rise to a correct detection rate $p_{r,HOM} = \gamma^4\eta_d^2/8$ and a false detection rate $p_{e,HOM} = \gamma^4\eta_d^2/8$. In the last false detection event, the misalignment error rate is e_d, the contribution to the total error rate being $p_d e_d$, where $p_d = \gamma^2\eta_d^2\eta/2$ is the probability of a joint measurement of wave states in ideal single-photon entanglement. Then the error rate e in terms of these parameters is expressed as

$$e \approx \frac{p_{e,dark} + p_{e,HOM} + p_d e_d}{p_{dark} + p_{HOM} + p_d}. \tag{13}$$

After taking into account all practical factors, such as error correction and privacy amplification, we obtain a final lower bound of the key rate of

$$r \geq Q\left[1 - fH(e) - 2e - \frac{\gamma^2(1 + 3\eta + 2\gamma^2)}{\eta}[1 - H(p(\eta, \gamma))]\right], \tag{14}$$

where $Q = p_{dark} + p_{HOM} + p_d$ is the rate of the joint measurement of the wave states, $\eta = \exp(-\alpha_f x)$ the channel transmittance with α_f the coefficient of absorption and x the transmission distance, and f the inefficiency of error correction, which always takes the value between 1.2 and 2 in accordance with the error correction protocol[25]. In this formula, we have assumed the transmittance of the optical fibers, the amplitude of the local oscillator fields, and the detector efficiency are the same for Alice and Bob.

The simulation results of our SEPM-QKD under different intensities of local coherent fields is shown in Fig. 2. The coefficient of transmission loss for the optical fiber at 1550 nm is $\beta_l = 0.2\ dB/km$ and the coefficient of absorption is $\alpha_f = (\beta_l \ln 10)/10$. Also, the detection efficiency at this frequency η_d is 14.5% for a commercial single-photon detector, the dark count rate is $p_{dark} = 8 \times 10^{-8}$ for all detectors, and the misalignment error e_d is 1.5%[32], the value for the inefficiency of error correction is set at $f = 1.2$[25]. From this figure, the key rate is seen to that the key rate decrease as the intensity of the local coherent light field decreases; because the probability of successful joint detection events is lower as the amplitude γ decreases. However, the transmission distance shows an opposite trend in its dependence on intensity. The dependence of the transmission distance on the amplitude γ arises from the false detection of phase insensitive joint counts p_{HOM}, which is proportional to the square of the light intensity, yielding γ^4. For a specified QKD protocol, the transmission distance is a compromise between the signal rate and the error rate. As the amplitude γ decreases, the phase-insensitive joint count-induced error plays little role in the key distillation. Therefore, a longer transmission distance obtains. We also compare the performance of SEPM-QKD for $\gamma = 0.002$ and $\gamma = 0.001$ with and without BS attacks. For short transmission distance, BS attack has negligible effect on the key rate, but for long transmission distance, the effect of BS attack should not be ignored.

Here, we make a clear comparison between different QKD protocols (Fig. 3), in which $\gamma = 0.001$ is chosen for the SEPM-QKD scheme. For traditional single-photon based BB84- and MDI-QKD schemes, their key rate obey the well-known linear bound by Pirandola *et al.* (PLOB bound)[29]. However, we see that, like PM-QKD and TF-QKD, SEPM-QKD displays a quadratic increase in the key rate with respect to the transmission distance which obey the single-repeater bound[59]. For short transmission distances, the key rate of SEPM-QKD is not only less than that of PM-QKD and TF-QKD, but also lower than particle-state based QKDs, like BB84- and MDI-QKD. There are two reasons for this result. The first reason is that the average intensity of the light source in SEPM-QKD is far lower than all other QKD protocols. The second reason is that BS attack is considered in SEPM-QKD, but not in other protocols.

It can clearly be seen that SEPM-QKD clarifies in principle the essential difference between TF-QKD and its variants which violate PLOB linear bound and BB84- and MDI-QKD proposed previously. In these QKD protocols, due to the different properties of information carrier and the different quantum states for distributing quantum keys, their implementation also has different technical challenges. In SEPM-QKD, a single-photon source is needed to generate wave-state entanglement. The single-photon produced in current experiments is probabilistic, which will reduce the quantum correlation between Alice and Bob. Under the current technical conditions, the

heralded single-photon source is an effective solution to this problem. In addition, we can see from Eq. (5) that the phase insensitive interference, i.e. particle space interference, exists in coincidence counting, which results in the inability to use strong light intensity in SEPM-QKD, and the key rate is much lower than other QKD protocols. In our future work, we will propose a de-localized detection scheme to the performance of SEPM-QKD.

Conclusion

We have reported a phase matching QKD based on single-photon entanglement. This SEPM-QKD is a time-reversed version of TF-QKD, in which the secret key is encoded in wave space characterized by the phase value. Measurement settings in SEPM-QKD, like quantum keys, are encoded in the phase of the locally coherent state, so the detection loophole is closed. This contrasts that for conventional DI-QKD. For a given light source intensity, just like TF-QKD, SEPM-QKD improves the bound of key rate from $O(\eta)$ to $O(\sqrt{\eta})$. In the proof of security, we find that BS attacks will have a significant impact on the performance of the protocol for long-distance transmission. By comparison with single-photon QKD schemes, we found that in SEPM-QKD and TF-QKD the wave state can be used as a new information carrier that has different properties due to interference-induced detection enhancement, which allows photons to travel in fibers without obeying the PLOB bound. In the future, we wish to reduce the impact of the phase-insensitive coincidence counting rate on the key rate and to improve the key rate and transmission distance of SEPM-QKD.

Methods

We present the methods for deriving the key rate formula in the main text. These methods theoretically give the upper limit of key rate obtained by Eve under the eavesdropping scheme of collective attack and beam-splitting attack.

Collective attack. Collective attack is considered to be the most powerful side-channel attack through using the imperfection of Alice and Bob's experimental devices. Eve's attack operation must obey the law of quantum mechanics, and the bit error rate between Alice and Bob caused by eavesdropping should be within the predetermined range. Under the idea of collective attack, Eve obtains the quantum state information shared between Alice and Bob as much as possible through weak measurements. In BB84 protocol, collective attack can be described as Eve attaching his probe to each of the states sent by Alice to Bob, and performing unitary operation, so that his probe can be quantum correlated with the transmitted quantum states[60,61]. Suppose that the interaction occurs in a two-dimensional space formed by a pair of orthogonal states $|p\rangle$ and $|q\rangle$. Eve's initial quantum state is $|E\rangle$, the interaction is represented by unitary operator U,

$$U|E\rangle|p\rangle = \left|E_p\right\rangle\left|\alpha_p\right\rangle,\ U|E\rangle|q\rangle = \left|E_q\right\rangle\left|\beta_q\right\rangle, \tag{15}$$

where α and β are the rotation angles of the transmitted quantum states with respect to $|p\rangle$ and $|q\rangle$, respectively, $\left|E_p\right\rangle$ and $\left|E_q\right\rangle$ are the corresponding states owned by Eve. According to the unitarity of operator, we have the following equality

$$\langle E|E\rangle\langle p|q\rangle = 0 = \langle p|\langle E|U^{+}U|E\rangle|q\rangle = \left\langle E_p|E_q\right\rangle\left\langle\alpha_p|\beta_q\right\rangle. \tag{16}$$

For any quantum states $\left|E_p\right\rangle, \left|E_q\right\rangle$, we have $\left\langle\alpha_p|\beta_q\right\rangle = 0$. Therefore, the quantum states $|p\rangle$ and $|q\rangle$ are rotated at the same angle under weak measurements. Eve can reverse-rotate the transmitted quantum state after the unitary operation,

$$T|E\rangle|p\rangle = RU|E\rangle|p\rangle = \left|E_p\right\rangle|p\rangle,\ T|E\rangle|q\rangle = RU|E\rangle|q\rangle = \left|E_q\right\rangle|q\rangle. \tag{17}$$

The relation between $|p\rangle, |q\rangle$ and the bases in Z space and X space can be written as

$$\begin{aligned} |p\rangle &= a|0\rangle + b|1\rangle, \\ |q\rangle &= b|0\rangle - a|1\rangle; \\ |p\rangle &= \frac{\sqrt{2}}{2}[(a+b)|+\rangle + (a-b)|-\rangle], \\ |q\rangle &= \frac{\sqrt{2}}{2}[(a+b)|-\rangle - (a-b)|+\rangle], \end{aligned} \tag{18}$$

where coefficients a and b satisfy normalization conditions $a^2 + b^2 = 1$. Then the weak measurements on these states can be described as

$$\begin{cases} T|E\rangle|0\rangle = |0\rangle\left(a^2\left|E_p\right\rangle + b^2\left|E_q\right\rangle\right) + |1\rangle\left(ab\left|E_p\right\rangle - ab\left|E_q\right\rangle\right), \\ T|E\rangle|1\rangle = |0\rangle\left(ab\left|E_p\right\rangle - ab\left|E_q\right\rangle\right) + |1\rangle\left(b^2\left|E_p\right\rangle + a^2\left|E_q\right\rangle\right); \end{cases} \tag{19}$$

and

$$\begin{cases} T|E\rangle|+\rangle = \frac{1}{2}\Big[|+\rangle\Big((a+b)^2\big|E_p\big\rangle + (a-b)^2\big|E_q\big\rangle\Big) + |-\rangle(a^2-b^2)\Big(\big|E_q\big\rangle - \big|E_p\big\rangle\Big)\Big], \\ T|E\rangle|-\rangle = \frac{1}{2}\Big[|+\rangle(a^2-b^2)\Big(\big|E_q\big\rangle - \big|E_p\big\rangle\Big) + |-\rangle\Big((a-b)^2\big|E_p\big\rangle + (a+b)^2\big|E_q\big\rangle\Big)\Big]. \end{cases} \tag{20}$$

After all the unitary operations, Eve perform unambiguous discrimination measurements on his states $\big|E_p\big\rangle$ and $\big|E_q\big\rangle$ to obtain the information between Alice and Bob. Alice and Bob's pre-agreed system bit error rate is p_e. A bit error occurs when Alice sends state $|0\rangle$ and Bob receives $|1\rangle$ or Alice sends state $|1\rangle$ and Bob receives $|0\rangle$. The total bit error rate is bounded by

$$1 - \big\langle E_p|E_q\big\rangle = 4p_e. \tag{21}$$

We will demonstrate in our forthcoming paper that Eve could obtain the largest information when he sets $a = 0$ and $b = 1$ or $a = 1$ and $b = 0$. Eve's maximal information is bounded by $\frac{1-\langle E_p\,|\,E_q\rangle}{2} = 2p_e$.

According to conclusion from BB84, Eve could also performs the same collective attack on entangled state. Suppose Alice and Bob share singlet state Φ^-_{AB}. Eve's collective attack on the entangled state can be formulated as

$$T|\Phi^-_{AB}\rangle|E_A\rangle|E_B\rangle = \frac{\sqrt{2}}{2}[|0\rangle_A|0\rangle_B|E_0\rangle_A|E_0\rangle_B - |1\rangle_A|1\rangle_B|E_1\rangle_A|E_1\rangle_B]. \tag{22}$$

Here we may set the joint state $|E_0\rangle_A|E_0\rangle_B$ to $|E_0\rangle_Z$, and the joint state $|E_1\rangle_A|E_1\rangle_B$ to $|E_1\rangle_Z$. A pair of orthogonal bases can be constructed from these two states

$$\begin{aligned} \big|E_\parallel\big\rangle &= \frac{1}{\sqrt{2(1+\langle E_0|E_1\rangle_Z)}}[|E_0\rangle_Z + |E_1\rangle_Z], \\ |E_\perp\rangle &= \frac{1}{\sqrt{2(1-\langle E_0|E_1\rangle_Z)}}[|E_0\rangle_Z - |E_1\rangle_Z]. \end{aligned} \tag{23}$$

Thus, under collective attack, the joint quantum state between Eve and Alice and Bob is

$$\begin{aligned} |\Psi_{ABE}\rangle &= \frac{\sqrt{2}}{2}[|0\rangle_A|0\rangle_B|E\rangle_0 - |1\rangle_A|1\rangle_B|E\rangle_1] \\ &= \frac{\sqrt{2}}{2}[\sqrt{1+\langle E_0|E_1\rangle_Z}\,|\Phi^-_{AB}\rangle + \sqrt{1-\langle E_0|E_1\rangle_Z}\,|\Phi^+_{AB}\rangle]. \end{aligned} \tag{24}$$

From Eq. (23), we can find that Eve could steals $1 - \langle E_0|E_1\rangle_Z$ information in Z space without causing any bit flipping error, while he steals nothing in X space bu causing a bit error rate of $\frac{1}{2}(1 - \langle E_0|E_1\rangle_Z)$. In order to balance the bit error rate of Z space and Y space, Eve will rotate the transmitted entangled state, and get the result of Eq. (9) in the main text.

Beam-splitting attack. In the beam separation attack, we assume that the transmission loss of a single photon is all intercepted and stored by Eve, and finally an asymmetric W-state between Eve and Alice and Bob is formed, as shown in Eq. (10). The details of BS attack is shown in Fig. 4. Compared with collective attack, beam-splitting attack can be regarded as a passive attack scheme. After Alice and Bob announce their bases publicly, Eve conducts a homodyne on the stored quantum state by using the coherent state with the same intensity as Alice and Bob. The joint detection can be expressed as

$$\begin{aligned} |\Psi_{ABE}\rangle &= [|0\rangle_A + \gamma e^{i\theta_A}|1\rangle_A][|0\rangle_B + \gamma e^{i\theta_B}|1\rangle_B] \\ &\quad \times \Big[|0\rangle_{E_A} + \gamma e^{i\theta_{E_A}}|1\rangle_{E_A}\Big]\Big[|0\rangle_{E_B} + \gamma e^{i\theta_{E_B}}|1\rangle_{E_B}\Big] \\ &\quad \times \frac{\sqrt{2}}{2}\Big[\sqrt{\eta}(|1_A0_B\rangle + |0_A1_B\rangle)\big|0_{E_A}0_{E_B}\big\rangle \\ &\quad + \sqrt{1-\eta}\,|0_A0_B\rangle\Big(\big|1_{E_A}0_{E_B}\big\rangle + \big|0_{E_A}1_{E_B}\big\rangle\Big)\Big], \end{aligned} \tag{25}$$

where $\big|1_{E_A}\big\rangle$ and $\big|1_{E_B}\big\rangle$ represent the photon states stored by Eve on Alice's and Bob's sides. The single-photon W-state then interferes with the coherent state on the beam splitter

$$
\begin{aligned}
|\Psi_{ABE}\rangle \;=\; & \left[|0\rangle + \gamma e^{i\theta_A}\frac{\sqrt{2}}{2}\left[i|1\rangle_{A_1} + |1\rangle_{A_2}\right]\right] \\
& \times \left[|0\rangle + \gamma e^{i\theta_B}\frac{\sqrt{2}}{2}\left[i|1\rangle_{B_1} + |1\rangle_{B_2}\right]\right] \\
& \times \left[|0\rangle + \gamma e^{i\theta_{E_A}}\frac{\sqrt{2}}{2}\left[i|1\rangle_{E_{A1}} + |1\rangle_{E_{A2}}\right]\right] \\
& \times \left[|0\rangle + \gamma e^{i\theta_{E_B}}\frac{\sqrt{2}}{2}\left[i|1\rangle_{E_{B1}} + |1\rangle_{E_{B2}}\right]\right] \\
& \times \frac{1}{2}\Big[\sqrt{\eta}\Big(\left[|1\rangle_{A_1} + i|1\rangle_{A_2}\right] + \left[|1\rangle_{B_1} + i|1\rangle_{B_2}\right]\Big) \\
& + \sqrt{1-\eta}\Big(\left[|1\rangle_{E_{A1}} + i|1\rangle_{E_{A2}}\right] + \left[|1\rangle_{E_{B1}} + i|1\rangle_{E_{B2}}\right]\Big)\Big].
\end{aligned} \tag{26}
$$

When Alice, Bob and Eve have coincidence counts, Eve has a certain probability of stealing Alice and Bob's key information. Without losing generality, we assume that Alice and Bob's measurement bases are in Z space at one moment, and their fired detectors are A_1 and B_1, which means $\theta_A = \theta_B = \theta \in \{0, \pi\}$. By expanding Eq. (25), the terms satisfying the above conditions are

$$
\begin{aligned}
& -\frac{\gamma^2}{4}[\sqrt{1-\eta}e^{i(\theta_A+\theta_B)} + \sqrt{\eta}e^{i\theta_{E_A}}(e^{i\theta_A} + e^{i\theta_B})]\left|1_{A_1}1_{B_1}1_{E_{A1}}\right\rangle; \\
& i\frac{\gamma^2}{4}[-\sqrt{1-\eta}e^{i(\theta_A+\theta_B)} + \sqrt{\eta}e^{i\theta_{E_A}}(e^{i\theta_A} + e^{i\theta_B})]\left|1_{A_1}1_{B_1}1_{E_{A2}}\right\rangle.
\end{aligned} \tag{27}
$$

When Eve synchronizes the light source with Alice and Bob's measurements, he randomly sets the value of θ_{E_A} to 0 or π, and infers the value of θ from the detection results. Here by setting $\theta_{E_A} = 0$, then we have the joint detection probabilities

$$
\begin{aligned}
P(\theta, E_{A1}) &= \frac{\gamma^4}{16}(1 + 3\eta + 4\sqrt{\eta(1-\eta)}\cos\theta); \\
P(\theta, E_{A2}) &= \frac{\gamma^4}{16}(1 + 3\eta - 4\sqrt{\eta(1-\eta)}\cos\theta).
\end{aligned} \tag{28}
$$

There are phase-independent joint detection events between Alice, Bob and Eve, whose probability is equal to $\frac{\gamma^6}{8}$. The joint probability matrix between Alice and Bob's phase θ and Eve's detection results E_A is

$$
p(\theta, E_A) = \frac{\gamma^4(1+3\eta+2\gamma^2)}{8}\begin{bmatrix} \frac{1+3\eta+4\sqrt{\eta(1-\eta)}+2\gamma^2}{2+6\eta+4\gamma^2} & \frac{1+3\eta-4\sqrt{\eta(1-\eta)}+2\gamma^2}{2+6\eta+4\gamma^2} \\ \frac{1+3\eta-4\sqrt{\eta(1-\eta)}+2\gamma^2}{2+6\eta+4\gamma^2} & \frac{1+3\eta+4\sqrt{\eta(1-\eta)}+2\gamma^2}{2+6\eta+4\gamma^2} \end{bmatrix}, \tag{29}
$$

where $2 + 6\eta + 4\gamma^2$ is the normalization constant. Of course, Eve can also carry out similar beam-splitting attacks on E_B and get the same results.

Received: 10 July 2019; Accepted: 25 September 2019;
Published online: 29 October 2019

References

1. Ekert, A. K. Quantum cryptography based on bell's theorem. *Physical review letters* **67**, 661 (1991).
2. Pirandola, S. *et al*. Advances in quantum cryptography. *arXiv preprint arXiv:1906.01645* (2019).
3. Lo, H.-K. & Chau, H. F. Unconditional security of quantum key distribution over arbitrarily long distances. *science* **283**, 2050–2056 (1999).
4. Shor, P. W. & Preskill, J. Simple proof of security of the bb84 quantum key distribution protocol. *Physical review letters* **85**, 441 (2000).
5. Mayers, D. Unconditional security in quantum cryptography. *Journal of the ACM (JACM)* **48**, 351–406 (2001).
6. Gottesman, D., Lo, H.-K., Lutkenhaus, N. & Preskill, J. Security of quantum key distribution with imperfect devices. In *International Symposium onInformation Theory, 2004. ISIT 2004. Proceedings.*, 136 (IEEE, 2004).
7. Xu, F., Ma, X., Zhang, Q., Lo, H.-K. & Pan, J.-W. Quantum cryptography with realistic devices. *arXiv preprint arXiv:1903.09051* (2019).
8. Wang, X.-B. Beating the photon-number-splitting attack in practical quantum cryptography. *Physical review letters* **94**, 230503 (2005).
9. Lo, H.-K., Ma, X. & Chen, K. Decoy state quantum key distribution. *Physical review letters* **94**, 230504 (2005).
10. Ma, X., Qi, B., Zhao, Y. & Lo, H.-K. Practical decoy state for quantum key distribution. *Physical Review A* **72**, 012326 (2005).
11. Wang, X.-B. Three-intensity decoy-state method for device-independent quantum key distribution with basis-dependent errors. *Phys. Rev. A* **87**, 012320 (2013).
12. Wang, L., Zhao, S.-M., Gong, L.-Y. & Cheng, W.-W. Free-space measurement-device-independent quantum-key-distribution protocol using decoy states with orbital angular momentum. *Chinese Physics B* **24**, 120307 (2015).

13. Yin, H.-L. *et al*. Measurement-device-independent quantum key distribution over a 404 km optical fiber. *Physical review letters* **117**, 190501 (2016).
14. Zhou, Y.-H., Yu, Z.-W. & Wang, X.-B. Making the decoy-state measurement-device-independent quantum key distribution practically useful. *Physical Review A* **93**, 042324 (2016).
15. Wang, F.-X. *et al*. High-dimensional quantum key distribution with twisted photon. *arXiv preprint arXiv:1810.02067* (2018).
16. Bouchard, F. *et al*. Experimental investigation of high-dimensional quantum key distribution protocols with twisted photons. *Quantum* **2**, 111 (2018).
17. Mower, J. *et al*. High-dimensional quantum key distribution using dispersive optics. *Physical Review A* **87**, 062322 (2013).
18. Cañas, G. *et al*. High-dimensional decoy-state quantum key distribution over multicore telecommunication fibers. *Physical Review A* **96**, 022317 (2017).
19. Ding, Y. *et al*. High-dimensional quantum key distribution based on multicore fiber using silicon photonic integrated circuits. *npj Quantum Information* **3**, 25 (2017).
20. Etcheverry, S. *et al*. Quantum key distribution session with 16-dimensional photonic states. *Scientific reports* **3**, 2316 (2013).
21. Ma, X., Fung, C.-H. F. & Razavi, M. Statistical fluctuation analysis for measurement-device-independent quantum key distribution. *Physical Review A* **86**, 052305 (2012).
22. Xu, F., Xu, H. & Lo, H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Physical Review A* **89**, 052333 (2014).
23. Yu, Z.-W., Zhou, Y.-H. & Wang, X.-B. Statistical fluctuation analysis for measurement-device-independent quantum key distribution with three-intensity decoy-state method. *Physical Review A* **91**, 032318 (2015).
24. Cai, R. Y. & Scarani, V. Finite-key analysis for practical implementations of quantum key distribution. *New Journal of Physics* **11**, 045024 (2009).
25. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Physical review letters* **108**, 130503 (2012).
26. Liu, Y. *et al*. Experimental measurement-device-independent quantum key distribution. *Physical review letters* **111**, 130502 (2013).
27. Liao, S.-K. *et al*. Satellite-to-ground quantum key distribution. *Nature* **549**, 43 (2017).
28. Pirandola, S., Garca-Patrón, R., Braunstein, S. L. & Lloyd, S. Direct and reverse secret-key capacities of a quantum channel. *Physical review letters* **102**, 050503 (2009).
29. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nature communications* **8**, 15043 (2017).
30. Braunstein, S. L. & Pirandola, S. Side-channel-free quantum key distribution. *Physical review letters* **108**, 130502 (2012).
31. Lucamarini, M., Yuan, Z. L., Dynes, J. F. & Shields, A. J. Overcoming the rate–distance limit of quantum key distribution without quantum repeaters. *Nature* **557**, 400 (2018).
32. Ma, X., Zeng, P. & Zhou, H. Phase-matching quantum key distribution. *Physical Review X* **8**, 031043 (2018).
33. Wang, X.-B., Yu, Z.-W. & Hu, X.-L. Twin-field quantum key distribution with large misalignment error. *Physical Review A* **98**, 062323 (2018).
34. Yu, Z.-W., Hu, X.-L., Jiang, C., Xu, H. & Wang, X.-B. Sending-or-not-sending twin-field quantum key distribution in practice. *Scientific reports* **9**, 3080 (2019).
35. Cui, C. *et al*. Twin-field quantum key distribution without phase postselection. *Physical Review Applied* **11**, 034053 (2019).
36. Lin, J. & Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Physical Review A* **98**, 042332 (2018).
37. Yin, H.-L. & Fu, Y. Measurement-device-independent twin-field quantum key distribution. *Scientific reports* **9**, 3045 (2019).
38. Bennett, C. H., Brassard, G. & Mermin, N. D. Quantum cryptography without bell's theorem. *Physical Review Letters* **68**, 557 (1992).
39. Rubenok, A., Slater, J. A., Chan, P., Lucio-Martinez, I. & Tittel, W. Real-world two-photon interference and proof-of-principle quantum key distribution immune to detector attacks. *Physical review letters* **111**, 130501 (2013).
40. Tan, S., Walls, D. & Collett, M. Nonlocality of a single photon. *Physical review letters* **66**, 252 (1991).
41. Banaszek, K. & Wódkiewicz, K. Testing quantum nonlocality in phase space. *Physical review letters* **82**, 2009 (1999).
42. Lee, H.-W. & Kim, J. Quantum teleportation and bell's inequality using single-particle entanglement. *Physical Review A* **63**, 012305 (2000).
43. Babichev, S., Appel, J. & Lvovsky, A. Homodyne tomography characterization and nonlocality of a dual-mode optical qubit. *Physical review letters* **92**, 193601 (2004).
44. Van Enk, S. Single-particle entanglement. *Physical Review A* **72**, 064306 (2005).
45. Morin, O. *et al*. Witnessing trustworthy single-photon entanglement with local homodyne measurements. *Physical review letters* **110**, 130401 (2013).
46. Kamaruddin, S. & Shaari, J. S. Device-independent quantum key distribution using single-photon entanglement. *EPL (Europhysics Letters)* **110**, 20003 (2015).
47. Li, W. & Zhao, S. Wave-particle duality in single-photon entanglement. *arXiv preprint arXiv:1908.04552* (2019).
48. Ma, X. & Razavi, M. Alternative schemes for measurement-device-independent quantum key distribution. *Physical Review A* **86**, 062319 (2012).
49. Santarelli, G., Clairon, A., Lea, S. & Tino, G. Heterodyne optical phase-locking of extended-cavity semiconductor lasers at 9 ghz. *Optics communications* **104**, 339–344 (1994).
50. Acn, A. *et al*. Device-independent security of quantum cryptography against collective attacks. *Physical Review Letters* **98**, 230501 (2007).
51. Masanes, L., Pironio, S. & Acn, A. Secure device-independent quantum key distribution with causally independent measurement devices. *Nature communications* **2**, 238 (2011).
52. Lim, C. C. W., Portmann, C., Tomamichel, M., Renner, R. & Gisin, N. Device-independent quantum key distribution with local bell test. *Physical Review X* **3**, 031006 (2013).
53. Shalm, L. K. *et al*. Strong loophole-free test of local realism. *Physical review letters* **115**, 250402 (2015).
54. Sangouard, N., Simon, C., Coudreau, T. & Gisin, N. Purification of single-photon entanglement with linear optics. *Physical Review A* **78**, 050301 (2008).
55. Salart, D. *et al*. Purification of single-photon entanglement. *Physical review letters* **104**, 180504 (2010).
56. Devetak, I. & Winter, A. Distillation of secret key and entanglement from quantum states. *Proceedings of the Royal Society A: Mathematical, Physical and engineering sciences* **461**, 207–235 (2005).
57. Heaney, L., Cabello, A., Santos, M. F. & Vedral, V. Extreme nonlocality with one photon. *New Journal of Physics* **13**, 053054 (2011).
58. Sheng, Y.-B., Ou-Yang, Y., Zhou, L. & Wang, L. Protecting sing-photon multi-mode w state from photon loss. *Quantum information processing* **13**, 1595–1605 (2014).
59. Pirandola, S. End-to-end capacities of a quantum communication network. *Commun. Phys* **2**, 51 (2019).
60. Biham, E. & Mor, T. Security of quantum cryptography against collective attacks. *Physical Review Letters* **78**, 2256 (1997).
61. Biham, E., Boyer, M., Brassard, G., van de Graaf, J. & Mor, T. Security of quantum key distribution against all collective attacks. *Algorithmica* **34**, 372–388 (2002).

Acknowledgements
This work is supported by Young fund of Jiangsu Natural Science Foundation of China (SJ216025), National fund incubation project (NY217024), Scientific Research Foundation of Nanjing University of Posts and Telecommunications (NY215034), the National Natural Science Foundation of China (No. 61475075), the open subject of National Laboratory of Solid State Microstructures of Nanjing University (M31021).

Author contributions
Wei Li devised the theoretical scheme, Wei Li and Le Wang provided the theoretical analysis. Wei Li and Sheng-Mei Zhao co-wrote the paper.

Competing interests
The authors declare no competing interests.

Additional information
Correspondence and requests for materials should be addressed to S.Z.

Reprints and permissions information is available at www.nature.com/reprints.

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