npj | Quantum Information

www.nature.com/npjqi

ARTICLE OPEN

Check for updates

Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses

Xiaoqing Zhong[1✉], Wenyuan Wang[1,4], Li Qian[2] and Hoi-Kwong Lo[1,2,3]

Twin-field (TF) quantum key distribution (QKD) is highly attractive because it can beat the fundamental limit of secret key rate for point-to-point QKD without quantum repeaters. Many theoretical and experimental studies have shown the superiority of TFQKD in long-distance communication. All previous experimental implementations of TFQKD have been done over optical channels with symmetric losses. But in reality, especially in a network setting, the distances between users and the middle node could be very different. In this paper, we perform a proof-of-principle experimental demonstration of TFQKD over optical channels with asymmetric losses. We compare two compensation strategies, that are (1) applying asymmetric signal intensities and (2) adding extra losses, and verify that strategy (1) provides much better key rate. Moreover, the higher the loss, the more key rate enhancement it can achieve. By applying asymmetric signal intensities, TFQKD with asymmetric channel losses not only surpasses the fundamental limit of key rate of point-to-point QKD for 50 dB overall loss, but also has key rate as high as 2.918×10^{-6} for 56 dB overall loss. Whereas no keys are obtained with strategy (2) for 56 dB loss. The increased key rate and enlarged distance coverage of TFQKD with asymmetric channel losses guarantee its superiority in long-distance quantum networks.

npj Quantum Information (2021)7:8 ; https://doi.org/10.1038/s41534-020-00343-5

INTRODUCTION

Quantum key distribution (QKD) enables remote users to share secret keys with information-theoretic security[1,2]. However, due to the unavoidable losses of optical channels, there exists a fundamental limit on the achievable secret key rate of long-distance QKD. Without using quantum repeaters, the upper bound (also called repeaterless bound in this paper) of the secret key rate of QKD scales linearly with the channel transmittance η[3,4]. Remarkably, a new type of QKD, called twin-field (TF) QKD, has been proposed[5] and can practically overcome the repeaterless bound. In TFQKD, like in the measurement-device-independent (MDI) QKD[6], two users (Alice and Bob) send two coherent states to an un-trusted intermediate node, i.e. Charlie, who performs the measurement. Because TFQKD employs single-photon interference, rather than two-photon interference in MDIQKD, the secret key rate of TFQKD scales as $\sqrt{\eta}$, allowing for unprecedented distance coverage. Plenty of variations and security analysis of TFQKD[7–12] have been studied, followed by multiple experimental demonstrations[13–16]. More recently, TFQKD has been successfully implemented over more than 500 km fibers[17,18]. It has been shown that TFQKD is one of the most promising and practical solutions to long-distance QKD.

However, all the above-mentioned studies only consider TFQKD over optical channels with symmetric losses between each of the users and intermediate node, and let Alice and Bob use identical sets of operations in preparing their signals. However, this assumption on channel symmetry is seldom true in reality. TFQKD over asymmetric channels is important not only for practical point-to-point implementations, but also in a network setting where the optical distances between users and the middle node can be significantly different. For instance, as shown in Fig. 1, if we consider a Sagnac-loop set-up, multiple users can be placed on the same loop, where they share a common relay, to implement a TFQKD network. However, the users on the loop naturally will have different distances to the relay, thus making asymmetric channels a major characteristic for such a TFQKD network set-up. Similar problems also exist for star-shaped networks where users are placed arbitrary distances away from a central relay.

Unfortunately, because TFQKD depends on a good visibility of single-photon interference, it requires the two channels to have similar levels of loss. This means that current implementations of TFQKD will have sub-optimal or even zero key rate if channels are asymmetric. One intuitive solution is to deliberately add fibers/losses to compensate for the shorter distance[19]. But this solution is not the optimal strategy, because it would increase signal loss and thus lower the secret key rate.

Several recent papers have theoretically studied TFQKD with asymmetric channels[20–24]. Instead of physically adding fibers/losses, refs. [21–24] study the use of asymmetric intensities between Alice and Bob to compensate for channel asymmetry and obtain optimal secret key rate. The limitation of symmetric optical channels has been first observed and investigated for MDIQKD, whose visibility also requires symmetry between optical channels[25–27]. For TFQKD, refs. [21,22] are based on an asymmetric-intensity version of the "Sending-or-not-Sending (SNS)" Protocol[9], while refs. [23,24] are based on the protocol proposed in ref. [11] by Curty, Azuma, Lo (for simplicity, let us call the protocol "CAL19" protocol here).

In this paper, we have implemented the protocol in ref. [24]. The key point of the protocol is that Alice and Bob can adjust their

[1]Center for Quantum Information and Quantum Control, Department of Physics, University of Toronto, Toronto, Ontario M5S 1A7, Canada. [2]Center for Quantum Information and Quantum Control, Department of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario M5S 3G4, Canada. [3]Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong, Hong Kong. [4]Present address: Institute for Quantum Computing and Department of Physics and Astronomy, University of Waterloo, Waterloo, Ontario N2L 3G1, Canada. ✉email: xzhong@physics.utoronto.ca

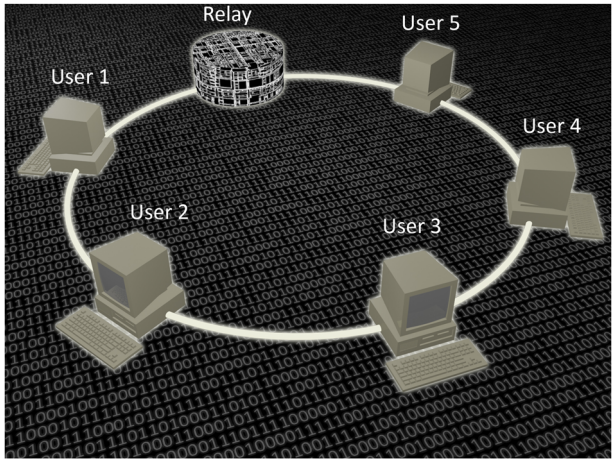

Fig. 1 Illustration of a Sagnac-loop-based twin-field quantum key distribution (TFQKD) network. Multiple users can be placed on the same loop to communicate via a single relay. As can be seen here, arbitrary pairs of users can have very different distances (channel losses) from the relay, which necessitate a TFQKD protocol that maintains good performance even in the presence of channel asymmetry. In this work, we present the experimental implementation of an asymmetric-intensity TFQKD protocol that maintains high rate through asymmetric channels, thus demonstrating the feasibility of such a Sagnac-loop-based TFQKD network.

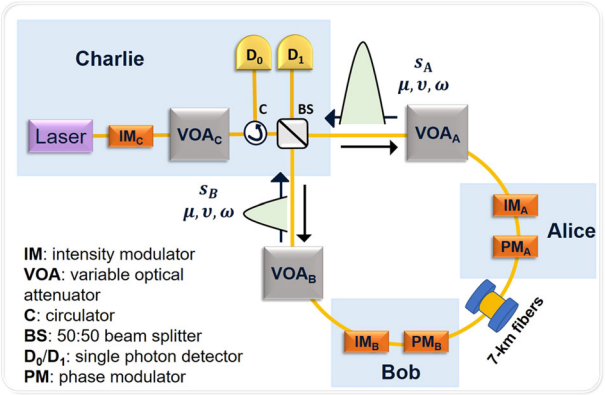

Fig. 2 Schematic set-up of twin-field quantum key distribution (TFQKD) over optical channels with asymmetric losses. Charlie produces un-modulated weak coherent pulses through his intensity modulator (IM_C) and variable optical attenuator (VOA_C) and distributes the pulses to Alice and Bob. The pulses enter the Sagnac loop through a circulator and a 50:50 beam splitter (BS) where they split into clockwise and counter-clockwise traveling pulses. The clockwise traveling pulses first pass through the attenuator VOA_A and Alice's station without being modulated. Then they go through a 7-km fiber spool and arrive at Bob's station. Based on the bases Bob chooses (signal basis or decoy basis), he modulates the phases and intensities of the pulses by his phase modulator and intensity modulator. Then Bob forwards the modulated pulses back to Charlie's BS though the attenuator VOA_B. The same process applies to the counter-clockwise traveling pluses, except that only Alice would modulate the phases and intensities of the counter-clockwise traveling pulses. The modulated pulses from Alice and Bob interfere with each other at Charlie's BS and are detected by Charlie's two single-photon detectors D_0 and D_1.

signal intensities independently, to effectively compensate for channel asymmetry. We choose CAL19 protocol because it provides higher key rate than SNS protocol except for extremely long distances. Also, while refs. [23,24] are both based on the CAL19 protocol, ref. [24] provides the additional convenience of only requiring signal states (and not decoy states) to be asymmetric. In this work, we for the first time experimentally demonstrate TFQKD over optical channels with asymmetric losses, and show that the new protocol provides much higher key rate and longer distance than previous strategies (adding extra loss or using no compensation at all). Importantly, this also shows the feasibility of a TFQKD-based quantum network. Note that for the CAL19 protocol we have implemented, the coding basis depends on interference visibility (which affects bit error rate and error-correction) but the decoy basis does not; for SNS protocol, the decoy basis depends on interference visibility (which affects bound on phase error rate and privacy amplification), while the coding basis does not. Therefore, overall, SNS protocol is similarly affected by channel asymmetry, and will benefit from asymmetric source intensities[21,22]. In principle, the technique we have demonstrated here is applicable to SNS protocol too.

RESULTS

Protocol

The key steps of the asymmetric-intensity TFQKD protocol[24] demonstrated in this paper are summarized as follows. Alice and Bob prepare weak coherent states and randomly choose X and Z bases. For signal states in X basis, Alice and Bob randomly add a 0 or π phase and set the intensities of states to s_A and s_B, respectively. For decoy states in Z basis, a random phase is added and the intensities are randomly chosen from $\{\mu, v, \omega\}$. The important difference from the CAL19 protocol in refs. [11,14] is that, signal intensities s_A and s_B can be set to different values, while the intensities of Alice's and Bob's decoy states are still kept symmetric. Such a choice of intensities is because, as explained in ref. [24], the X basis requires intensities arriving at Charles to be symmetric for a good interference visibility (hence s_A, s_B should be different, to compensate for channel asymmetry), while the Z basis does not have such a requirement (hence decoy states can simply be set to symmetric to simplify implementation). The latter is because the estimation of phase error rate is based on photon-number yields in the Z basis, which is little affected by asymmetry of intensities arriving at Charles. Then Alice and Bob send their states to the middle node Charlie, who measures the interference of the coming states and announces the results.

Experimental set-up

The experimental set-up used in our previous work of TFQKD over symmetric optical channels in ref. [14] can be simply adopted to implement the asymmetric-intensity TFQKD protocol, as shown in Fig. 2. As a proof-of-principle demonstration, we only use the optical variable attenuators (VOA_A and VOA_B) to simulate the optical channel losses between Alice/Bob and Charlie. The only difference from the set-up in ref. [14] is that VOA_A and VOA_B have different attenuation to mimic the asymmetric channel losses. As indicated in ref. [14], a two-way QKD system consisting of a Sagnac interferometer is applied to overcome the main challenge of implementing TFQKD, namely, the phase stabilization. The common-path nature of the Sagnac loop automatically compensates for phase fluctuations, thus maintaining long-term phase stability between the weak coherent states sent from Alice and Bob. Moreover, the laser located on Charlie's station is shared by Alice and Bob, to guarantee the matched global phase. The Sagnac[28] or Sagnac-like[29] interferometers have been exploited in QKD systems previously. It is similar to the "plug-and-play" system that has been widely used in QKD[30,31] in which photons travel bidirectionally, though information is carried only in one direction. Security proofs for such "plug-and-play" QKD systems have been developed in refs. [32,33]. To prevent possible attacks from eavesdroppers, more hardware is required. For example, in Alice's and Bob's stations, taps, photodiodes, and attenuators can be

added for them to monitor and limit the strong optical injections from the outside. Bandpass filters are also needed for Alice and Bob to filter out any side channels, so as to prevent eavesdropper from probing the sources. Note that the main goal of this work is to show the optimal compensation strategy for TFQKD with asymmetric channel losses. Therefore, we did not implement the above-mentioned elements, but they can be easily added to our current experimental set-up without invalidating any of the experimental results we have obtained.

Charlie uses his intensity modulator (IM_C) and VOA_C to create weak coherent pulses (10 MHz, 900 ps) from a continuous wave source and sends the pulses to Alice and Bob. The pulses go through an optical circulator and enter the Sagnac loop through a 50:50 beam splitter (BS), where the pulses split into clockwise traveling and counter-clockwise traveling pluses. Clockwise (counter-clockwise) pulses first go through VOA_A (VOA_B) and Alice's (Bob's) station without being modulated. Then the clockwise (counter-clockwise) pulses pass a 7-km fiber spool (with loss of about 7 dB) before reaching Bob's (Alice's) station. Note that no information is transmitted over the channel between Alice and Bob. On Bob's (Alice's) station, the pulses are modulated by a phase modulator PM_B (PM_A) and an intensity modulator IM_B (IM_A). Based on different bases Alice and Bob choose, the phases and intensities of the pulses are modulated accordingly. All the modulators in the set-up are driven and synchronized by a high-speed arbitrary waveform generator (AWG, Keysight M8195). The modulated pulses from Alice and Bob travel through the attenuators VOA_B and VOA_A and interfere at Charlie's BS. One output of the BS is directed to a single-photon detector (SPD) D_0 via the circulator, and the other output is followed directly by another SPD, D_1. Charlie then uses D_0 and D_1 to record the interference and publicly announces the results. The SPDs used in the set-up are the commercial free-run avalanche photodiodes (ID220), the dark count probability of which is about 7×10^{-7}.

It is very important to ensure that Alice and Bob only modulate the pulses traveling in designed directions. That is to say, the clockwise and counter-clockwise traveling pulses should never overlap with each other at any of Alice's and Bob's modulators. Therefore, the fiber lengths among the users and middle node are carefully calibrated to avoid the overlap of the arriving time at any modulators between the clockwise and counter-clockwise traveling pulses. Another challenge in our experiment is that the limited extinction ratio of a single intensity modulator is not sufficient to generate the vacuum state (ω), especially on Alice's station where the power of the injected pulse (that should be modulated) is always 10 dB higher than that on Bob's station. To create the vacuum state, we use two intensity modulators to achieve more than 65 dB extinction ratio. The resulting pulse is suppressed below the dark count noise of the detectors. Multiple polarization controllers are used for the initial polarization alignment but no active polarization control is needed. Because of the auto compensation of phase fluctuation of Sagnac interferometer, our system is stable and the interference visibility is kept as high as 99.8%. In this paper, the main objective is to study the optimal compensation strategy for TFQKD over asymmetric channels. Therefore, variable optical attenuators are used instead of real fibers. Since the ability of Sagnac loop withstanding phase fluctuations is a function of its total length and the characteristic frequencies of the fluctuations, when hundred of kilometers of real fibers are inserted into the loop to replace VOAs, the phase stability and polarization stability of the current system would be affected. However, previous study in ref. [14] has found that a Sagnac loop with 300 km loop length, corresponding to 60 dB of loss, is adequate in maintaining phase stability required for TFQKD.

Experimental results

The experiment has been performed over three overall channel losses between Alice and Bob, 40 dB, 50 dB, and 56 dB. The channel losses between Alice and charlie are always 10 dB higher than the losses between Bob and Charlie, i.e., $\eta_B = \eta_A \times 10$. The detector efficiency (11.7%) is included in the overall loss. To test the asymmetric-intensity strategy, we allow Alice and Bob to choose asymmetric signal intensities s_A and s_B, but keep their decoy intensities symmetric. We have also tested the strategy where all the intensities are symmetric but another 10 dB attenuation is added on Bob's side to compensate the channel asymmetry. Additionally, at the overall loss of 40 dB, we have conducted the experiment where Alice and Bob use identical sets of operations as they do for TFQKD with symmetric channels (no compensation at all). All the signal intensities $s_{A/B}$ and decoy intensities $\mu_{A/B}, \nu_{A/B}$ used in the experiment are close to the optimal values and are listed in Table 1. (ω is the vacuum state and therefore is not listed.) Note that when Alice and Bob test the asymmetric-intensity strategy, the intuitive way is to set $s_A/s_B = \eta_B/\eta_A = 10$. However, as indicated in Table 1, the ratio of the optimal s_A to s_B slightly deviates from 10. This is because, as described in ref. [24], although the interference visibility (which affects X basis QBER) favors $s_A/s_B = \eta_B/\eta_A$, there are other factors affecting s_A, s_B—namely, a tight estimation of the phase error rate favors small values of both s_A and s_B (which determine the cat state coefficients) and makes optimal s_A/s_B deviate from exactly η_B/η_A. As for the experimental implementation, we would like to point out that it is more convenient to use the intensities that fulfill $s_A/s_B = \eta_B/\eta_A$, especially for the Sagnac-loop-based system which automatically provides such intensity compensation. Considering

Table 1. List of intensity sets and experimental secret key rates for the overall system losses of 40 dB, 50 dB, and 56 dB.

Overall loss	Strategy	Intensity						Key rate	
		s_A	μ_A	ν_A	s_B	μ_B	ν_B	Infinite data	Finite data
25 + 15 dB	Asym.	0.0448	0.300	0.120	0.00529	0.300	0.120	1.017×10^{-4}	5.013×10^{-5}
25 + 15 dB	Adding loss	0.0213	0.481	0.146	0.0213	0.481	0.146	3.727×10^{-5}	1.688×10^{-5}
25 + 15 dB	No comp.	0.0036	0.247	0.0923	0.0036	0.247	0.0923	7.163×10^{-6}	0
30 + 20 dB	Asym.	0.030	0.514	0.108	0.00373	0.514	0.108	1.666×10^{-5}	6.971×10^{-6}
30 + 20 dB	Adding loss	0.0147	0.444	0.133	0.0147	0.444	0.133	2.382×10^{-6}	2.677×10^{-7}
33 + 23 dB	Asym.	0.0274	0.401	0.120	0.0035	0.401	0.120	2.918×10^{-6}	3.174×10^{-7}

The loss between Alice and Charlie is always 10 dB higher than the loss between Bob and Charlie; $s_{A/B}$ is Alice's/Bob's signal intensity; $\mu_{A/B}$ and $\nu_{A/B}$ are the decoy intensities. The vacuum state ω is not listed here. The secret key rate is calculated based on the observed gains and quantum bit error rates. The size of the total data sent to Charlie is 3×10^{10}. Both infinite-data case and finite-data case are considered. For each loss, the first row shows intensities and key rates with asymmetric signal intensities; the second row (if exists) gives the intensities and key rates with adding extra losses; the third row (if exists) is the case where no compensation is applied.

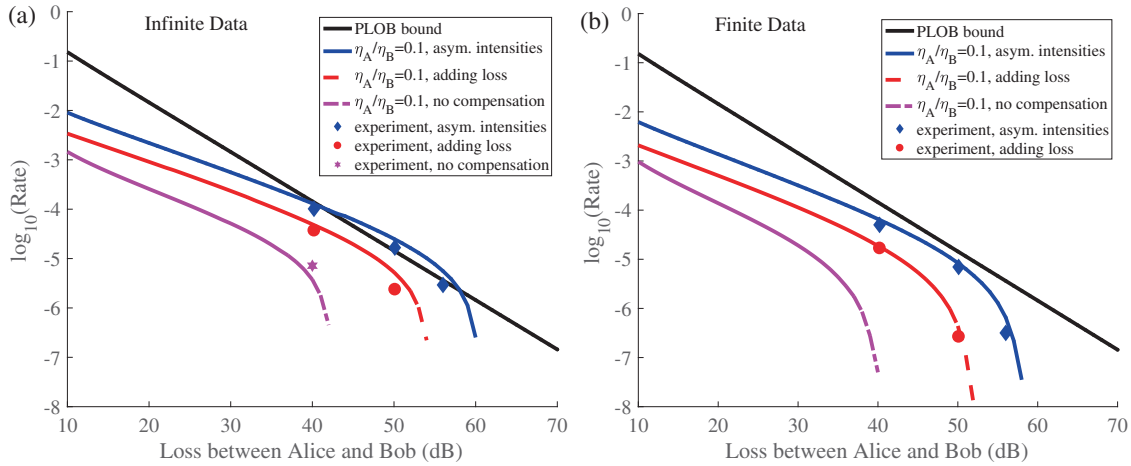

Fig. 3 Secret key rate (bit per pulse) in logarithmic scale as a function of the overall loss between Alice and Bob. The secret key rate is calculated for two cases, i.e., **a** the case where infinite data size is assumed and **b** the case where the data size is 3×10^{10} and finite size effects are considered. The solid black line represents one representative of the repeaterless bound (PLOB bound). The blue solid curve is the simulated key rate with asymmetric signal intensities; the red dash curve is the simulated key rate with adding extra losses; the purple dash-dotted curve is the simulated key rate with no compensation. All the scattered points are the experimental secret key rates. The blue rhombi represent the case with asymmetric signal intensities; the red circles represent the case where extra 10 dB attenuation is added on Bob's side; the purple hexagon is the key rate obtained when no compensation is applied. As observed, the strategy of applying asymmetric signal intensities always provides better key rates than the other two strategies.

the experimental fluctuations, the tested key rate with the exact ratio $s_A/s_B = 10$ can be even higher than the rate with optimal ratio. The size of the total data that Alice and Bob send to Charlie in each run is 3×10^{10}. Due to the limit of the available AWG channels, the signal state and decoy state are not randomly switched in our experiment. But this random switch can be easily accomplished with more resources. As a proof-of-principle demonstration, our current implementation is feasible to study the optimal compensation strategies for TFQKD with asymmetric channel losses.

The secret key rate is calculated based on the observed gains and quantum bit error rates. Both infinite-data case and finite-data case are considered and the experimental results are depicted in Fig. 3, which shows the secret key rate (bit per pulse) in logarithmic scale as a function of the overall loss between Alice and Bob. The blue rhombi are the experimental key rates obtained with asymmetric signal intensities; the red circles are the key rates of the case where extra 10 dB attenuation is added on Bob's side; the purple hexagon is the key rate obtained when no compensation is applied. The corresponding simulated secret key rates of the above three cases are also shown in Fig. 3, represented by blue solid curve, red dash curve, and purple dash-dotted curve, respectively. Additionally, we use the solid black line in the figure to show the repeaterless bound[4]. As shown in Fig. 3a where the infinite-data case is considered, applying asymmetric signal intensities can always help generate positive key rates for all tested losses. Moreover, at the total loss of 50 dB, the experimental key rate with asymmetric signal intensities is as high as 1.67×10^{-5}, even beating the repeaterless bound. However, the key rates of the other two strategies are always lower than the bound. Even worse, no secret keys can be extracted at 56 dB total loss in the adding-loss scenario. If no compensation is applied, there exists positive key rate only when the total loss is 40 dB. In the finite-data case, as shown in Fig. 3b, again, the key rates with asymmetric signal intensities are always higher than the key rates with adding extra losses or applying no compensation. At the total loss of 56 dB, the experimental key rate with asymmetric signal intensities is 3.17×10^{-7} while no keys can be generated with the other two strategies. At 50 dB, the experimental key rate with asymmetric intensities is 6.97×10^{-6}, about 30 times of the key rate in the adding-loss scenario. At 40 dB, the key rate with no compensation is still positive but very small in simulation. However, due to fluctuations in experiment, we could not obtain any keys in the finite-data scenario if no compensation is applied. Note that in Fig. 3a, the experiment key rates are always lower than the simulations (except at 40 dB loss). This is due to the fact that all the experimental intensities are optimized based on finite-data scenario, while the simulations take the intensities optimized for infinite-data scenario.

DISCUSSION

Overall, the experimental results are consistent with the simulations. As indicated in Fig. 3, the distance coverage of TFQKD over optical channels with asymmetric losses is significantly diminished if no compensation is made. Deliberately adding extra losses to compensate the asymmetry could help increase the key rate to some extent, but is not comparable to the strategy of using asymmetric signal intensities. This is because with extra losses added, Alice and Bob pessimistically assume that the losses can be controlled by Eve, while in practice this part of the loss (e.g. from a tailored length of fiber or an attenuator) is securely inside Bob's lab. This is not a limitation with the asymmetric-intensity strategy, which accounts for the asymmetry of source intensities and channels. Therefore, despite that, observable-wise, the arriving intensities at Charles are similar in the two cases, the adding-loss case actually has a more pessimistic assumption (that the added loss is controlled by Eve) in its security analysis, hence resulting in lower key rate. While by allowing Alice and Bob to set asymmetric intensities, the secure key rate of TFQKD with asymmetric channel losses can be dramatically increased. The higher the loss, the more key rate enhancement the asymmetric-intensity strategy can achieve. Besides the advantage of providing higher key rate, the asymmetric-intensity strategy is also more convenient and efficient to implement. Especially in a network setting, the adding-loss strategy requires that every user should prepare different compensation losses inside his/her station for different connections. While for the asymmetric-intensity strategy, the users only have to adjust their signal intensities for all different connections. Even when new users join the network, no system modifications are required for the old users. Therefore, a straightforward

application of our demonstration in this work can be the study of Sagnac-loop-based QKD network.

As a proof-of-principle demonstration, the primary goal of this work is to find out the optimal compensation strategy for TFQKD with asymmetric channels, rather than implementing a complete TFQKD system. The current limitations in our experimental set-up can be potentially removed given more time and resources. For example, optical filters and power monitors can be added in Alice's and Bob's stations to limit Trojan horse attacks from eavesdropper. In our current set-up, attenuators are used to simulate the optical channel loss. When long spans of fibers are used instead of attenuators, the noise induced by the back-scattering (especially the Rayleigh backscattering) of strong pulses would definitely worsen the performance of our system. There are also some possible solutions. Since the intensity of the back-scattered signal is proportional to the input power, one way to limit the backscattering is to lower the intensity of the pulses sent out by Charlie into the loop. To compensate for fiber loss, bidirectional amplifiers can be inserted between Alice and Bob to amplify the signal as long as the power of the signal is higher than the minimum input power of the amplifier. This is a viable strategy as it was used in ref. [18]. Another way to mitigate the back-scattering issue is to exploit the time dependence of the backscattering. Due to fiber loss, if a single short pulse is launched into the fiber at time $t = 0$, the backscattering is strongest at $t = 0$, and subsequently decays with time. One could use a very low repetition rate such that the detection window can be moved to the end of the period where the backscattered signals decay to a tolerable value. Alternatively, one can use bursts of pulses. More specifically, bursts of pulses are sent out by Charlie with a very low repetition rate R, while in each burst, n pulses with very short time interval δt are sent into the Sagnac loop. The parameters R, n, and δt can be well designed such that the detection window can be moved to the low noise point. The drawback is that both strategies (low repetition rate or pulse bursts) will decrease the overall key rate. More study on the decay rate of the back-scattering and careful design of the burst timing will be carried out in future. In addition, the above two strategies can be combined to combat backscattering.

In summary, we have demonstrated the proof-of-principle experiment of TFQKD over optical channels with asymmetric losses. Sagnac interferometer is applied for the auto phase stabilization. Our experiment shows that, compensation strategies are necessary for TFQKD with asymmetric channel losses. Two strategies have been tested, that are applying asymmetric signal intensities or adding extra losses to make the channel loss symmetric again. Compared with the latter strategy, applying asymmetric signal intensities provides much better secure key rate for TFQKD with asymmetric channel losses. It keeps the major advantage of TFQKD, i.e., surpassing the repeaterless bound, and significantly enlarges the distance coverage. Our implementation provides the experimental study of TFQKD with asymmetric channel losses and shows the feasibility of applying TFQKD to build the long-distance quantum network in reality.

METHODS

Finite size analysis

In this paper, we have used a standard error analysis[34] for finite-size effects. Here we consider only individual attacks and assume each signal is identically and independently distributed. This means we can assume a normal distribution for the observables, and upper/lower bound it with a confidence interval (measured by the number of standard deviations, γ) given a failure probability ϵ. Specifically, for a given observed value x, the expected value $\bar{x}$ satisfies:

$$x - \gamma\sqrt{x} \le \bar{x} \le x - \gamma\sqrt{x} \tag{1}$$

where γ satisfies $\gamma = \sqrt{2}\mathrm{erf}^{-1}(1-\epsilon)$ (here erf^{-1} is the inversed error function).

The focus of this work is to demonstrate a realistic validation on asymmetric signal intensities being able to compensate for channel asymmetry, while the finite-size analysis (especially on the decoy states) is not really the focus, so we have adopted a relatively simple finite-size model just to perform an estimation on the real-world performance of the protocol. Nonetheless, we would like to point out that, should a more rigorous finite-size analysis be applied (such as applying Chernoff's bound[35] or alternative bounds[36–38]), our method demonstrated in this paper would still be compatible. This is because the performance gain in asymmetric channels comes from the asymmetric signal states compensating for signal QBER, which is a process independent from the finite-size analysis that largely involves the decoy states and the phase error rate.

Parameter optimization

In this paper, we perform parameter optimization using the same local search algorithm "coordinate descent" in refs. [24,26]. In this algorithm, we search a parameter list $\vec{p} = \{p_1, p_2, ..., p_N\}$ by maximizing the target (key rate) function along one coordinate at a time (and fixing the other components):

$$p_k^{i+1} = \underset{p_k}{\mathrm{argmax}}\, R(p_1^{i+1}, p_2^{i+1}, ..., p_k, p_{k+1}^{i}..., p_N^{i}) \tag{2}$$

where as an illustration we are updating the k-th component at iteration i, and all components expect p_k are fixed such that the search is one-dimensional. After all components are updated, we stop the algorithm when either optimality is met, or the max iteration number is reached, otherwise we continue into the next iteration. Such an algorithm is a type of local search (and other algorithms such as gradient descent are in principle applicable here too), and global search is not needed, since we observe that for this protocol the key rate is a convex function with respect to the parameters (as is observed in ref. [24] for TF-QKD and also in refs. [26,34] for MDI-QKD when the coordinates of parameters are appropriately defined).

DATA AVAILABILITY

All the data that support the findings in this work are available from the corresponding author upon reasonable request.

CODE AVAILABILITY

All the codes used in this work are available from the corresponding author upon reasonable request.

Received: 3 February 2020; Accepted: 25 November 2020;
Published online: 26 January 2021

REFERENCES

1. Bennett, C. H. & Brassard, G. Quantum cryptography: public key distribution and coin tossing. *Theor. Comput. Sci.* **560**, 7–11 (2014).
2. Ekert, A. K. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.* **67**, 661 (1991).
3. Takeoka, M., Guha, S. & Wilde, M. M. Fundamental rate-loss tradeoff for optical quantum key distribution. *Nat. Commun.* **5**, 5235 (2014).
4. Pirandola, S., Laurenza, R., Ottaviani, C. & Banchi, L. Fundamental limits of repeaterless quantum communications. *Nat. Commun.* **8**, 15043 (2017).
5. 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).
6. Lo, H.-K., Curty, M. & Qi, B. Measurement-device-independent quantum key distribution. *Phys. Rev. Lett.* **108**, 130503 (2012).
7. Tamaki, K., Lo, H.-K., Wang, W., & Lucamarini, M. Information theoretic security of quantum key distribution overcoming the repeaterless secret key capacity bound. Preprint at https://arxiv.org/abs/1805.05511 (2018).
8. Ma, X., Zeng, P. & Zhou, H. Phase-matching quantum key distribution. *Phys. Rev. X* **8**, 031043 (2018).
9. Wang, X. B., Yu, Z. W. & Hu, X. L. Twin-field quantum key distribution with large misalignment error. *Phys. Rev. A* **98**, 062323 (2018).
10. Lin, J. & Lütkenhaus, N. Simple security analysis of phase-matching measurement-device-independent quantum key distribution. *Phys. Rev. A* **98**, 042332 (2018).

11. Curty, M., Azuma, K. & Lo, H.-K. Simple security proof of twin-field type quantum key distribution protocol. *npj Quantum Inf.* **5**, 1–6 (2019).
12. Cui, C. et al. Twin-field quantum key distribution without phase postselection. *Phys. Rev. Appl.* **11**, 034053 (2019).
13. Minder, M. et al. Experimental quantum key distribution beyond the repeaterless secret key capacity. *Nat. Photonics* **13**, 334–338 (2019).
14. Zhong, X., Hu, J., Curty, M., Qian, L. & Lo, H.-K. Proof-of-principle experimental demonstration of twin-field type quantum key distribution. *Phys. Rev. Lett.* **123**, 100506 (2019).
15. Liu, Y. et al. Experimental twin-field quantum key distribution through sending-or-not-sending. *Phys. Rev. Lett.* **123**, 100505 (2019).
16. Wang, S. et al. Beating the fundamental rate-distance limit in a proof-of-principle quantum key distribution system. *Phys. Rev. X* **9**, 021046 (2019).
17. Fang, X. T. et al. Implementation of quantum key distribution surpassing the linear rate-transmittance bound. *Nat. Photonics* **14**, 1–4 (2020).
18. Chen, J. P. et al. Sending-or-not-sending with independent lasers: secure twin-field quantum key distribution over 509 km. *Phys. Rev. Lett.* **124**, 070501 (2020).
19. 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. *Phys. Rev. Lett.* **111**, 130501 (2013).
20. Yin, H. L. & Chen, Z. B. Coherent-state-based twin-field quantum key distribution. *Sci. Rep.* **9**, 1–7 (2019).
21. Zhou, X. Y., Zhang, C. H., Zhang, C. M. & Wang, Q. Asymmetric sending or not sending twin-field quantum key distribution in practice. *Phys. Rev. A* **99**, 062316 (2019).
22. Hu, X. L., Jiang, C., Yu, Z. W. & Wang, X. B. Sending-or-not-sending twin-field protocol for quantum key distribution with asymmetric source parameters. *Phys. Rev. A* **100**, 062337 (2019).
23. Grasselli, F., Navarrete, Á. & Curty, M. Asymmetric twin-field quantum key distribution. *New J. Phys.* **21**, 113032 (2019).
24. Wang, W. & Lo, H.-K. Simple method for asymmetric twin-field quantum key distribution. *New J. Phys.* **22**, 013020 (2019).
25. Xu, F., Curty, M., Qi, B. & Lo, H.-K. Practical aspects of measurement-device-independent quantum key distribution. *New J. Phys.* **15**, 113007 (2013).
26. Wang, W., Xu, F. & Lo, H.-K. Asymmetric protocols for scalable high-rate measurement-device-independent quantum key distribution networks. *Phys. Rev. X* **9**, 041012 (2019).
27. Liu, H. et al. Experimental demonstration of high-rate measurement-device-independent quantum key distribution over asymmetric channels. *Phys. Rev. Lett.* **122**, 160501 (2019).
28. Qi, B., Huang, L. L., Lo, H.-K. & Qian, L. Polarization insensitive phase modulator for quantum cryptosystems. *Opt. Express* **14**, 4264–4269 (2006).
29. Yin, H. L. & Fu, Y. Measurement-device-independent twin-field quantum key distribution. *Sci. Rep.* **9**, 3045 (2019).
30. Muller, A. et al. "Plug and play" systems for quantum cryptography. *Appl. Phys. Lett.* **70**, 793–795 (1997).
31. Stucki, D., Gisin, N., Guinnard, O., Ribordy, G. & Zbinden, H. Quantum key distribution over 67 km with a plug&play system. *New J. Phys.* **4**, 41 (2002).
32. Zhao, Y., Qi, B. & Lo, H.-K. Quantum key distribution with an unknown and untrusted source. *Phys. Rev. A* **77**, 052327 (2008).
33. 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).
34. Xu, F., Xu, H. & Lo, H.-K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. *Phys. Rev. A* **89**, 052333 (2014).
35. Curty, M. et al. Finite-key analysis for measurement-device-independent quantum key distribution. *Nat. Commun.* **5**, 1–7 (2014).
36. Lorenzo, G. C. et al. Tight finite-key security for twin-field quantum key distribution. Preprint at https://arxiv.org/abs/1910.11407 (2019).
37. Maeda, K., Sasaki, T. & Koashi, M. Repeaterless quantum key distribution with efficient finite-key analysis overcoming the rate-distance limit. *Nat. Commun.* **10**, 1–8 (2019).
38. Kato, G. Concentration inequality using unconfirmed knowledge. Preprint at https://arxiv.org/abs/2002.04357 (2020).

ACKNOWLEDGEMENTS

We thank Marcos Curty, Feihu Xu, and Reem Mandil for their helpful discussion. We thank funding from NSERC, MITACS, CFI, ORF, the Royal Bank of Canada, Huawei Technology Canada Inc., and the start-up funding at the University of Hong Kong.

AUTHOR CONTRIBUTIONS

X.Z., W.W., L.Q., and H.K.L. proposed this project. X.Z. designed and performed the experiment. W.W. provided the theoretical analysis and calculation. L.Q. and H.K.L. supervised this project. All the authors contributed to the discussion of the results. X.Z. wrote the manuscript. All the authors commented and revised the manuscript.

COMPETING INTERESTS

The authors declare no competing interests.

ADDITIONAL INFORMATION

Correspondence and requests for materials should be addressed to X.Z.

Reprints and permission information is available at http://www.nature.com/reprints

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