


Simple Multiuser Twin-Field Quantum Key Distribution Network

Xiaoqing Zhong,^{1,*} Wenyuan Wang,^{1,†} Reem Mandil^①,¹ Hoi-Kwong Lo,^{1,2,3} and Li Qian^②

¹*Center for Quantum Information and Quantum Control, Department of Physics, University of Toronto, Toronto, Ontario, M5S 1A7, Canada*

²*Center for Quantum Information and Quantum Control, Dept. of Electrical & Computer Engineering, University of Toronto, Toronto, Ontario, M5S 3G4, Canada*

³*Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong*

 (Received 14 June 2021; revised 6 November 2021; accepted 22 December 2021; published 21 January 2022)

Twin-field quantum key distribution (TFQKD) systems have shown great promise for implementing practical long-distance secure quantum communication due to its measurement-device-independent nature and its ability to offer fundamentally superior rate-loss scaling than point-to-point QKD systems. A surge of research and development effort in the last two years has produced many variants of protocols and experimental demonstrations. In terms of hardware topology, TFQKD systems interfering quantum signals from two remotely phase-locked laser sources are in essence giant Mach-Zehnder interferometers (MZIs) requiring active phase stabilization. Such configurations are inherently unsuitable for a TFQKD network, where more than one user pair share the common quantum measurement station, because it is practically extremely difficult, if not impossible, to stabilize MZIs of largely disparate path lengths, a situation that is inevitable in a multi-user-pair TFQKD network. On the other hand, Sagnac interferometer-based TFQKD systems exploiting the inherent phase stability of the Sagnac ring can implement asymmetric TFQKD, and are therefore eminently suitable for implementing a TFQKD network. In this work, we experimentally demonstrate a proof-of-principle multi-user-pair Sagnac TFQKD network where three user pairs sharing the same measurement station can perform pairwise TFQKD through time multiplexing, with channel losses up to 58.00 dB, and channel loss asymmetry up to 15.00 dB. In some cases, the secure key rates still beat the rate-loss bound for point-to-point repeaterless QKD systems, even in this network configuration. Our demonstration of this multi-user-pair TFQKD network is a step in advancing quantum-communication network technologies.

DOI: [10.1103/PhysRevApplied.17.014025](https://doi.org/10.1103/PhysRevApplied.17.014025)

I. INTRODUCTION

Quantum key distribution (QKD), a quantum technology that allows remote users to share encryption keys with information-theoretic security, has been well developed over the past few decades [1,2]. Various types of QKD protocols have been proposed and QKD experiments have been successfully performed over different systems [3]. A range of commercial QKD systems have also been developed and used in practical testbeds. More recently, an alternative type of QKD, called twin-field quantum key distribution (TFQKD), has shown great promise for implementing practical long-distance secure quantum communication [4]. For the conventional point-to-point QKD systems, the maximum key rate scales linearly with the channel transmittance η [5,6] without using quantum

repeaters [7]. This rate-loss limit is described by the repeaterless bounds in Refs. [5,6]. However, for TFQKD, the key rate scales linearly with $\sqrt{\eta}$, providing fundamentally superior rate-loss scaling than other repeaterless QKD systems. Moreover, TFQKD is inherently a measurement-device-independent QKD (MDIQKD) [8], where two remote users (conventionally called Alice and Bob) send encoded coherent states to an untrusted central node (conventionally called Charlie) who performs quantum measurements on the states. The measurements are only able to reveal the parity of the states sent by Alice and Bob, not the information encoded in the states, and the results are publicly announced. Hence, it is invulnerable to any attacks on detector side channels. Since the proposal of TFQKD, a surge of research and development effort in the last two years has produced many variants of protocols and security proofs [9–13]. Meanwhile, a number of TFQKD experiments have demonstrated the feasibility of its application in long-distance quantum communication [14–20].

*xzhong@physics.utoronto.ca

†Current address: Department of Physics, University of Hong Kong, Pokfulam Road, Hong Kong.

Despite the rapid development, demonstrated TFQKD systems have only two participants exchanging keys (Alice and Bob), as is the case for all other conventional point-to-point QKD systems. To make TFQKD widely applicable in quantum communication in the future, one has to extend the two-user scenario to a multiuser case, that is, a network setting. QKD network [21] is an essential step towards building a global quantum internet, which can enable more applications, such as cloud quantum computing [22]. There have been multiple QKD networks [23–30] built and tested all over the world, from small scales with a few users to large scales with more than a hundred users, such as the SECOQC network [25], the Tokyo QKD network [28], and China’s space-to-ground network [30]. In these networks, different QKD protocols and technologies have been used. In particular, in China’s space-to-ground network [30], two ground-to-satellite free-space QKD links are also integrated. All of these network building efforts have paved the way towards a global quantum internet. However, most existing QKD networks [25,27,28,30] are based on trusted central relays, which are undesirable for security. Any successful attacks of the central relays would break down the security of the network. There have been QKD networks using optical switches [23,24,26] or using untrusted relays [29], but their key rates are limited by the repeaterless bounds. In contrast, a TFQKD network can solve both the security issue and key-rate limit, due to its measurement-device-independent nature and its ability to outperform the repeaterless bounds, showing a remarkable advantage over existing QKD networks.

However, there are technical challenges to implement a TFQKD network. Because of the random phase fluctuations of signals over long distances, phase stabilization is required for the interference of coherent states in TFQKD. In most demonstrated TFQKD systems [14,16–19], two remote phase-locked laser sources are used to send quantum signals to the central node for interference measurement, which is in essence a giant Mach-Zehnder interferometer (MZI). Such a configuration, with the use of active phase stabilization or post phase selection, is suitable for demonstrating a two-user TFQKD system. However, it is inherently unsuitable for a TFQKD network, where more than two users are involved and share the common central node. First of all, it would be impractical to have all the remote laser sources phase locked, especially when a large number of users are connected to the network. Another difficulty is that, due to the laser phase noise, it would be very challenging to stabilize an unbalanced MZI of largely disparate path lengths. In other words, such a configuration would prefer that all the users have the same distances to the central node. While in a realistic network, the geographic distances between different users and the central node could be very different. In the most recent MZI-based TFQKD system [31], the demonstrated path-length difference is only 18 km. For

much larger path-length differences, users might have to add extra fiber to stabilize the system, which, however, would not only increase users’ operation complexity but also reduce the key rate [20].

On the other hand, there is another type of TFQKD configuration that is based on a Sagnac interferometer and has inherent system stability [15,20]. In such a TFQKD system, users share the same laser source that is held by the central node, thus removing the need of phase locking. Additionally, single-photon detectors (SPDs) are also placed in the central node. Each user requires only the components for information encoding, making it simple and low cost to add more users into the system to form a network. Due to its common path nature, the Sagnac TFQKD system not only has the ability of automatically compensating phase fluctuations, but also has high tolerance for channel asymmetry. In Ref. [20], the demonstrated TFQKD system has a channel-loss asymmetry of 10 dB, equivalent to 50 km of standard telecom fiber. In principle, users in a Sagnac TFQKD system could have any values of channel asymmetry without affecting the phase stability, even for the extreme case where one user is right next to the central node (still inside the Sagnac loop) and another user is farthest from the central node (at the middle point of the Sagnac loop). Therefore, the Sagnac-interferometer-based configuration is eminently suitable for implementing a TFQKD network.

In this work, we present the an experimental implementation of a TFQKD network that is based on a Sagnac interferometer. As shown in Fig. 1, three users, Alice, Bob, and David, are connected in the Sagnac loop. Any two of these users can perform pairwise TFQKD at a given time slot through an untrusted central node, Charlie. As a proof-of-principle demonstration, variable optical attenuators (VOAs) are used to simulate optical channel losses between users and the central node. To mimic real network situations, three user pairs in our network have three different channel-loss asymmetries, that are 0.00, 10.00, and 15.00 dB. We show that our Sagnac TFQKD network successfully enables all user pairs to share secret keys regardless of their channel-loss asymmetries. Moreover, without using quantum repeaters or trusted central relays, the obtained secret key rates in our network can still overcome the repeaterless bound [6] in some cases.

II. PROTOCOL

In our demonstration, two types of TFQKD protocols are adopted to optimize key rates for different user pairs with different channel-loss asymmetries. More specifically, for the user pair (Alice and Bob) with symmetric channel losses (0.00-dB channel-loss asymmetry), a TFQKD protocol (called “CAL19”) studied in Refs. [12,15] is used. The CAL19 protocol is composed of five steps. (1) Two users, Alice and Bob, randomly and independently choose

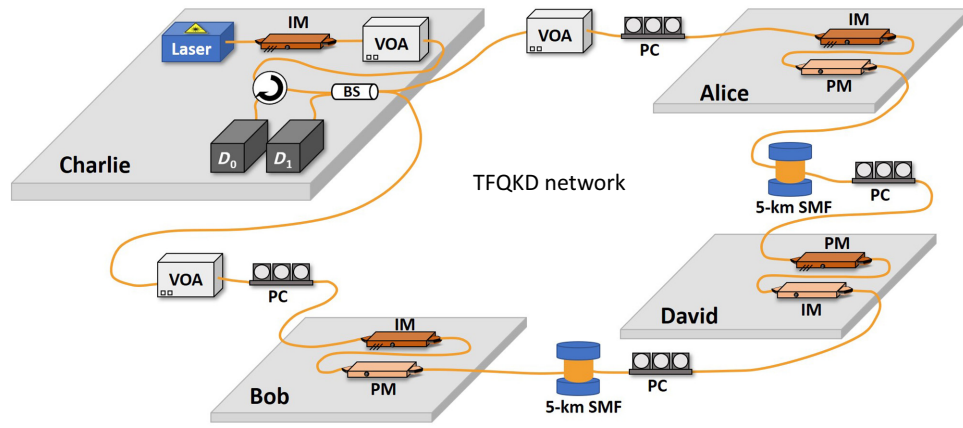


FIG. 1. Schematic diagram of our experimental setup of twin-field quantum key distribution network. On Charlie's station, that is located outside the Sagnac loop, a continuous-wave laser diode is used with the intensity modulator (IM) and variable optical attenuator (VOA) to generate the weak coherent pulses. Three users, Alice, Bob, and David, are connected in the Sagnac loop. When any pair of users want to use the network to generate secret keys, Charlie launches the coherent pulses into the loop through a circulator (C) and a 50:50 beam splitter (BS). When the pulses arrive at the designated users, they use their IMs and phase modulators (PMs) to set the intensities and add the phases to the pulses. Note that there are clockwise and counterclockwise traveling pulses in the loop. Each active user modulates only one of the pulses, the one that has already traveled through the other active user, while letting the other pulse pass through without modulation. After the modulation, the pulses will be forwarded back to Charlie for measurement and will be detected by two single-photon detectors D_0 and D_1 . As a proof-of-principle demonstration, VOAs are inserted between Alice and Charlie, and between Bob and Charlie, to simulate the optical channel losses. Between Alice and David, and between Bob and David, there are 5-km single-mode fibers (SMFs). The polarization controllers (PCs) are also used inside the loop for the polarization alignment.

x or z basis to prepare their weak coherent pulses with a preselected global phase. For the pulse in x (signal) basis, Alice and Bob randomly add a 0 or π phase and set the intensity to be signal intensity s . For the pulse in z (decoy) basis, they randomize the phase and set the intensity to be one of the decoy intensity settings $\{\mu, \nu, \omega\}$. (2) Alice and Bob then send their prepared weak coherent pulses to an untrusted central replay, Charlie, through optical channels. (3) Charlie performs the interference measurement with a 50:50 beam splitter and a pair of single-photon detectors. Only the successful measurement event, that is only one detector clicks, will be recorded. (4) After the measurement, Charlie announces the recorded events; Alice and Bob declare the bases they used. (5) Based on the information announced, Alice and Bob distill the secret key. For the user pair (Alice and David or Bob and David) with asymmetric channel losses, an asymmetric version of CAL19 protocol [13,20] is used for key generation. The only difference between the asymmetric and the original CAL19 protocol is the first step. In the asymmetric CAL19 protocol, users set asymmetric intensities of signal states to compensate for the channel-loss asymmetry. For decoy states, which are used for phase-error-rate estimation, the intensities can be either symmetric or asymmetric, since the channel asymmetry has little effects on the phase error rate [13]. As shown in Ref. [20], with the use of asymmetric signal intensities, the users can obtain a better key rate than of simply padding loss to make channels symmetric.

III. EXPERIMENT

The experimental setup of our demonstration is shown in Fig. 1. On Charlie's station, a continuous-wave laser diode is used with the intensity modulator and variable optical attenuator (VOA) to generate the weak coherent pulses at a repetition rate of 10 MHz with 900-ps pulse width. Inside the Sagnac loop, there are three users, Alice, Bob, and David. As a proof-of-principle demonstration, we use VOAs between Alice and Charlie, and between Bob and Charlie, to simulate the optical channel losses. Between Alice and David, and between Bob and David, there are 5 km of single-mode fibers. On each user's station, there are phase modulator and intensity modulator installed for information encoding. The polarization controllers are also used inside the loop for the polarization alignment.

When any two users want to start the QKD protocol for key generation (the two users are called active users), Charlie launches weak coherent pulses into the loop through a circulator and a 50:50 beam splitter. As shown in Fig. 2, there are clockwise and counterclockwise traveling pulses in the loop. Each active user modulates only one of the pulses, the one that has already traveled through the other active user, while letting the other pulse pass through without modulation. For instance, when Alice and Bob are the active users, Alice (Bob) modulates only the pulses traveling in counterclockwise (clockwise) direction.

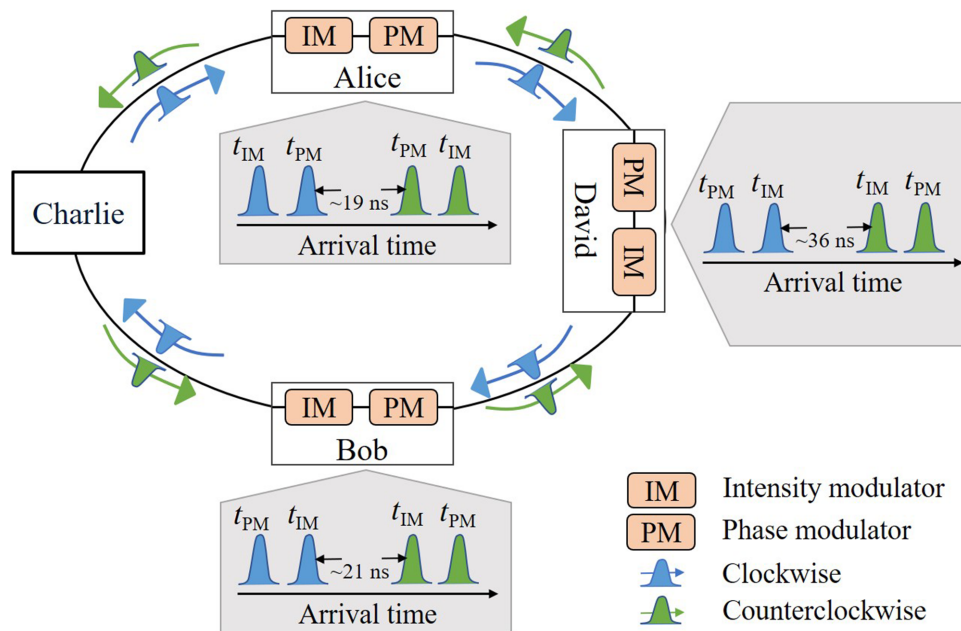


FIG. 2. Illustration of different arrival times of clockwise and counterclockwise traveling pulses at different users' stations. Inside the loop, the pulse launched by Charlie at a rate of 10 MHz are divided into two beams, one traveling in clockwise direction (marked in blue) while another one traveling in counterclockwise direction (marked in green). To avoid the collisions between clockwise and counterclockwise traveling pulses at any modulators, an individual user can add a small amount of fiber at one end of his or her station so that the arrival times of two counterpropagating pulses at each user's station are different. On Alice's station, the counterclockwise traveling pulse arrives at Alice's PM in about 19 ns after the clockwise traveling pulse passing through Alice's PM. On Bob's station, the arrival time of the counterclockwise pulse at Bob's IM is about 21 ns later than that of the clockwise pulse. On David's station, the difference between the arrival times of the clockwise and counterclockwise traveling pulses at David's IM is about 36 ns. Note that it takes about 13 ns for a pulse traveling from Alice's and Bob's IM to PM and about 15 ns for a pulse traveling from David's IM to PM. The large difference of the arrival times guarantees that each user can modulate only the pulse traveling in one direction without making any changes to the other pulse, since the modulation window is only about 1 ns.

When the counterpropagating pulses are phase and intensity modulated by the active users and are forwarded back to Charlie, they interfere at the beam splitter and are measured by Charlie's two SPDs (ID220) D_0 and D_1 with a detection window of 900 ps. The dark-count probability of both detectors is about 7×10^{-7} . Note that when the protocol is running, the third inactive user will simply let the pulses go through his or her station without any modulation. We remark that this implementation does not compromise security, since the pulses will always undergo the optical channels that are exposed to Eve.

In our TFQKD network, with the use of Sagnac interferometer, the laser source and SPDs are required only by the central node Charlie. This configuration not only reduces the cost, but also remarkably simplifies the operations for users in the network. Neither phase locking nor phase stabilization is necessary in this network setting, since a single laser is shared by the users and interfering pulses travel through a common path. The only operation left for the users is information encoding (intensity and phase modulations). Therefore, users can be also easily added into or removed from our network. We note that the phase stability of a Sagnac interferometer is dependent on

the fiber length of the loop. As long as the phase fluctuations of signals over the light transit time through half the loop is small, the automatic phase stability could be guaranteed. Reference [15] has estimated that for a loop length of 300 km, the Sagnac-interferometer configuration without active phase stabilization is still applicable for TFQKD.

Even though there are pulses traveling bidirectionally in our setup, each user will modulate only the pulses in one direction. Therefore, it is necessary for us to ensure that the clockwise and counterclockwise traveling pulses would not collide at any modulators of the users inside the loop. To achieve this condition, fiber segments with well-calibrated lengths are added on different users' stations to avoid the pulse collision at each user's station. As shown in Fig. 2, the difference of arrival times of the counterpropagating pulses at each user's station is at least 19 ns in our experiment, which adequately ensures that the modulation applied to the pulse in one direction will not affect the pulse in the other direction. Note that when a new user is later added into the network, fiber length calibration will be managed by the new user and would not require adjustment from the existing users. The new user

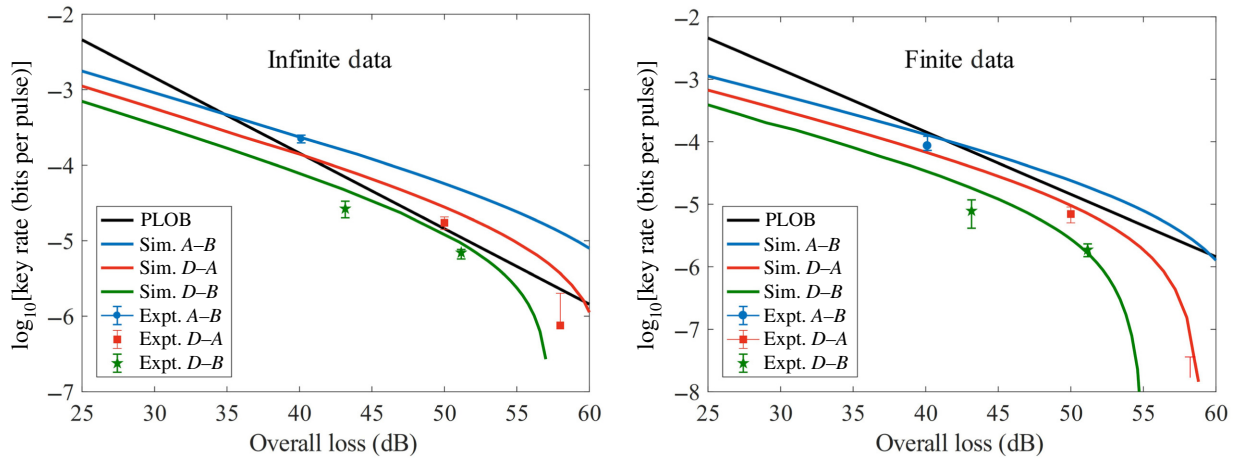


FIG. 3. Log-log plot of the key rates of different users in the network as a function of the overall loss. The overall loss represents the sum of the channel losses of two users to the central node Charlie. Different pairs of users have tested the network and the experimental key rates are calculated in both (a) infinite-data scenario and (b) finite-data scenario. For Alice and Bob who have symmetric channel losses, one overall loss point is tested, that is 40.12 dB. The experimental key rates are shown as blue circles. For David and Alice, who have 10.00 dB channel-loss asymmetry, they have tested the network over both 50.00 and 58.00 dB overall channel losses. Their experimental key rates are represented by red squares. For David and Bob, who have 15.00 dB channel-loss asymmetry, they have tested the network over both 43.16 and 51.16 dB overall channel losses. Their experimental key rates are shown as green stars. The vertical bar of each data point indicates the best and worst key rates when intensity fluctuation is taken into consideration. Note that at the overall loss is 58.00 dB, the worst key rate for David and Alice is 0 in the infinite-data scenario. While in the finite-data scenarios, both the average key rate and the worst key rate are 0. The solid curves show the simulated key rates for different pairs of users. The black solid line is the PLOB bound [6], which is one representative of the repeaterless bound.

needs only to make his or her station with the right fiber length so that the time for the signal traveling through the station is an integral multiple of the signal period. In this case, this station can be added into or removed out of the network without requiring any further calibration. It is also necessary to guarantee that the active users will impose modulation only when the designated pulses arrive. In our demonstration, all the intensity and phase modulators are synchronized and driven by a high-speed multichannel arbitrary waveform generator (Keysight M8195). The delay time of the electrical signal to each modulator is carefully adjusted such that the designated pulses will exactly fall into the modulation window when they pass through the modulators.

IV. RESULTS

In our demonstration, we vary the channel losses for different users and test the key rates over different cases. For Alice and Bob who have symmetric channel losses to Charlie, one overall loss (the sum of two users' channel losses) is tested, that is 40.12 dB. For David and Alice who always have 10.00-dB channel-loss asymmetry, the tested overall losses are 50.00 and 58.00 dB. For David and Bob who have 15.00-dB channel-loss asymmetry, they have exchanged keys over both 43.16 and 51.16 dB. All the signal (s) and decoy (μ, ν, ω) intensities as well as the probabilities of users sending signal and decoys states

during each test are listed in Table I. For Alice and Bob who perform the original CAL19 protocol [12] to share secret keys, their signal and decoy states have symmetric intensities as shown in Table I. While for another two pairs of users with channel-loss asymmetry, they follow the asymmetric CAL19 protocol [13] to optimize their key rates. As shown in Table I, the intensities of their signal and decoy states are asymmetric. The user with higher channel loss always sends out stronger signals than the other user. Note that the ratio of optimal intensities for signal states slightly deviates from the inverse ratio of their channel transmittance [13].

The observed quantum bit error rate (QBER) for each test is shown in Table II. As the overall loss and channel-loss asymmetry between the users increase, the observed QBER also increases. We remark that in our demonstration, no active phase or polarization compensation is applied during each test. Due to the long-term stability of our TFQKD network system, the largest QBER observed in our experiment is still less than 5%. The secret key rate (bit per pulse) for each test is calculated based on the experimental gains and QBERs and is listed in Table II as well. In our experiment, all pairs of users always send 1×10^{11} pulses to the central node during each test. But in our key-rate analysis, we consider both the infinite-data scenario and the finite-data scenario. We also take intensity fluctuations into consideration and calculate the best and worst key rates for each test.

TABLE I. List of intensities and sending probabilities of signal and decoy states used in our experiments. s is the signal intensity, μ , ν , and ω are the decoy intensities. For the pair of users who have the same channel loss, both their signal intensities and decoy intensities are symmetric. For the pair of users who have different channel losses, their signal and decoy intensities are asymmetric. The probabilities of sending signal state (P_s) or one of the decoy states (P_μ, P_ν, P_ω) are always the same for a pair of users.

Pair	User	Channel loss (dB)	s	μ	ν	ω	P_s	P_μ	P_ν	P_ω
Pair 1	Alice	20.06	0.0242 ± 0.0002	0.1009 ± 0.0003	0.0241 ± 0.0002	$(2.1 \pm 0.3) \times 10^{-4}$	0.86	0.035	0.033	0.072
	Bob	20.06	0.0242 ± 0.0002	0.1009 ± 0.0003	0.0241 ± 0.0002	$(2.1 \pm 0.3) \times 10^{-4}$				
Pair 2	David	30.00	0.0350 ± 0.0014	0.798 ± 0.002	0.168 ± 0.002	$(3.50 \pm 0.63) \times 10^{-4}$	0.84	0.032	0.036	0.092
	Alice	20.00	0.00421 ± 0.00003	0.0798 ± 0.0002	0.0168 ± 0.0002	$(3.50 \pm 0.63) \times 10^{-5}$				
Pair 3	David	34.00	0.0246 ± 0.0007	0.656 ± 0.002	0.1403 ± 0.0008	$(1.17 \pm 0.19) \times 10^{-3}$	0.32	0.125	0.147	0.408
	Alice	24.00	0.00436 ± 0.00004	0.0656 ± 0.0002	0.01403 ± 0.00008	$(1.17 \pm 0.19) \times 10^{-4}$				
Pair 3	David	29.08	0.050 ± 0.002	0.769 ± 0.002	0.1587 ± 0.0009	$(7.3 \pm 0.6) \times 10^{-4}$	0.83	0.034	0.043	0.093
	Bob	14.08	0.00228 ± 0.000001	0.02517 ± 0.00006	0.00502 ± 0.00003	$(2.3 \pm 0.2) \times 10^{-5}$				
Pair 3	David	33.08	0.0200 ± 0.0002	0.783 ± 0.002	0.1533 ± 0.0008	$(3.1 \pm 1.2) \times 10^{-4}$	0.71	0.050	0.065	0.175
	Alice	18.08	0.00113 ± 0.00002	0.02476 ± 0.00006	0.00485 ± 0.00003	$(0.98 \pm 0.38) \times 10^{-5}$				

The results are also presented as scattered points in Fig. 3, which is a plot of the secret key rate in logarithmic scale as a function of the overall channel loss. To compare the performance of our TFQKD network with the rate-loss limit of conventional QKD networks without trusted central relays, we also plot out one representative of the repeaterless bounds, that is the PLOB bound [6] (represented by the solid black line). Figure 3(a) shows key rates of different user pairs when infinite-data size is assumed. Note that the simulation curves in Fig. 3(a) are based on intensities optimized against asymptotic key rate, while the experimental key rates are calculated with intensities optimized for finite-data case. That is to say, the experimental intensity settings are not optimal in the infinite-data case. Therefore, overall, the experimental key rates are a bit lower than the simulation curves. As shown in Fig. 3(a), the observed secret key rate for Alice and Bob is 2.227×10^{-4} at 43.16 dB (equivalent to 216 km), which is significantly higher than the PLOB bound, even when the worse key rate is considered. For the other two user pairs, due to the presence of channel-loss asymmetry, their secret key rates are lower than the key rates of Alice and Bob. However, with our strategy of using asymmetric intensities, they can still obtain optimal key rates compared with other compensation strategies [20]. As depicted in Fig. 3(a), even with 15.00-dB channel-loss asymmetry, David and Bob still successfully share secret keys over both overall losses. For the high loss of 51.16 dB (equivalent to 256 km), the key rate is as high as 6.946×10^{-6} , which is close to the PLOB bound. For David and Alice who have 10.00-dB channel-loss asymmetry, their secret keys rate at 50.00-dB loss (equivalent to 250 km) is 1.728×10^{-5} , still higher than the PLOB bound. When the overall loss is as high as 58.00 dB (equivalent to 290 km), the pulses that are launched into the loop by Charlie are the strongest compared with the previous cases. So, the backscattering noise is relatively high and affects the performance of our system. This is reflected in the large range of the secret key rate. Even though, the best key rate David and Alice can obtain in our test is as high as 2.014×10^{-6} . Even when the finite-size effect is considered, as shown in Fig. 3(b), the experimental key rates are consistent with the simulations, showing that our TFQKD network still allows different users to share secret keys. As explained before, the only exception is that, when the overall loss between David and Alice is 58.00 dB, due to the backscattering noise, the average key rate is 0. But when intensity fluctuation is considered, secret keys can still be shared between David and Alice at a positive key rate.

V. DISCUSSION

In summary, we propose and demonstrate a TFQKD network, which serves three users through an untrusted central node. A configuration based on a Sagnac interferometer is

TABLE II. List of observed QBERs and secret key rate for different pairs of users. Here, A represents Alice, B is for Bob, and D is for David. The QBERs observed in both detector D_0 and D_1 are given. The secret key rates are calculated in both infinite-data scenario and finite-data scenario. For the latter case, the total data size is 1×10^{11} . In both scenarios, intensity fluctuations are considered to find the best and worst key rates.

User	Overall loss (dB)	QBER		Key rate (infinite-data)			Key rate (finite-data)		
		D_0	D_1	Mean	Best	Worst	Mean	Best	Worst
Pair 1	40.12	0.26%	0.25%	2.27×10^{-4}	2.502×10^{-4}	1.976×10^{-4}	8.587×10^{-5}	1.003×10^{-4}	7.261×10^{-5}
Pair 2	50.00	1.75%	1.73%	1.728×10^{-5}	2.063×10^{-5}	1.411×10^{-5}	6.961×10^{-6}	9.012×10^{-6}	5.047×10^{-6}
	58.00	4.34%	4.60%	7.551×10^{-7}	2.014×10^{-6}	0	0	3.262×10^{-8}	0
Pair 3	43.16	2.15%	1.96%	2.653×10^{-5}	3.334×10^{-5}	2.010×10^{-5}	7.827×10^{-6}	1.174×10^{-5}	4.144×10^{-6}
	51.16	3.80%	3.73%	6.946×10^{-6}	7.644×10^{-6}	5.729×10^{-6}	1.872×10^{-6}	2.321×10^{-6}	1.450×10^{-6}

used in our demonstration. Compared with the MZI-based system, the Sagnac TFQKD network is inherently stable, allowing users to have asymmetric channel distances to the central node. In our proof-of-principle demonstration, three user pairs have three different channel-loss asymmetries, that are 0.00, 10.00, and 15.00 dB. Additionally, neither phase locking nor active phase stabilization is needed in our implementation, significantly reducing the operation complexity for users in the network. Different versions of the CAL19 TFQKD protocol are used to optimize key rates for user pairs with different channel-loss asymmetries. We remark that while we choose the CAL19 protocol in our experimental demonstration, the basic principle of our design of a Sagnac TFQKD network works well for other classes of TFQKD protocols such as the sending or not sending protocol [10]. The experimental results show that, all users in our network are able to share secure keys with each other at a positive rate over an overall channel loss ranging from 40.12 to 58.00 dB. Moreover, without the use of any trusted central relay or quantum repeater, the users in our TFQKD network can still share secure keys at a rate that is higher than the repeaterless bound [6] for some cases.

In this work, we focus on showing the feasibility of building a TFQKD network that enables multipair of users to share encryption keys through an untrusted central node. Our proof-of-principle implementation is simple but adequate for this purpose. But there are limitations of our current implementation when it comes to applications in practice. We would like to discuss some of them here. The first issue is the security concern. Our demonstrated Sagnac TFQKD network has only the crucial components of information encoder for each user, leaving the user's station vulnerable to Trojan-horse attacks [32]. To secure the system, intensity monitors and filters should have been added on each user's station [32]. Note that the Sagnac TFQKD system has a similar structure of a plug-and-play QKD system [33,34]. The vulnerabilities of these bidirectional QKD systems and corresponding countermeasure techniques have been studied in Refs. [32,35,36]. We remark that adding these security-related components would not affect the feasibility of building a Sagnac TFQKD network. The extra losses introduced to each user's station would reduce the performance of the system, which, however, could be minimized by choosing commercially available products with low losses.

The major challenge of implementing a Sagnac TFQKD network in practice comes from the noise induced by Rayleigh backscattering, which would travel back to Charlie's detectors and increase the detection error rate. In our proof-of-principle demonstration, the backscattering noise is not significant since only 10 km of fibers are inserted. For real-world applications, VOAs should be replaced by long-distance optical fibers. In this case, the backscattering noise would be non-negligible. But there are viable

strategies to alleviate this issue. As discussed in Ref. [20], one way to limit the backscattering noise is to lower the intensity of pulses launched into the loop. Bidirectional amplifiers can be inserted between the users to compensate for the fiber loss. Another way to deal with the backscattering noise is to use bursts of pulses. As studied in Ref. [37], one can exploit the time dependence of the backscattering noise and design the duration of each burst such that, when pulses travel back to the detectors, the backscattering noise decays to a tolerable level. The study of managing backscattering noise is out of the scope of this work and will be carried out in the future. When a large number of users are connected into the network, the high loss of the entire Sagnac loop would aggravate the backscattering issue. Besides the solutions mentioned above, one can divide the large Sagnac loop into smaller ones by adding fiber connections between different user pairs. Each user pair can choose the loop with the lowest loss to perform TFQKD. The increased path choices could also improve the robustness of the network.

Another limitation of our current implementation is that, time multiplexing is used to allow different user pairs in the network to share keys at different time slots. It would be inefficient when more users are added into the network. To improve the efficiency of the Sagnac TFQKD network, a wavelength multiplexing technique could be applied. Different wavelength channels can be assigned to different user pairs so that all users can perform TFQKD to share keys with each other simultaneously. Note that in this case, the untrusted central node would need multiple pairs of detectors for detecting signals in different wavelength channels, which will add complexity to the system.

In conclusion, while our demonstration of a Sagnac-interferometer-based TFQKD network has yet to be improved, it has shown the feasibility of applying a Sagnac-based TFQKD system to enhance the development of QKD networks. Comparing to the MZI-based system, the inherent system stability and the simple operation of the Sagnac-based TFQKD system make it eminently suitable for implementing a practical and low-cost TFQKD network. Comparing to the existing QKD networks, the TFQKD network can extend the communication coverage beyond the repeaterless bounds with an untrusted central node. We hope that our exploration of the TFQKD network can pave the way towards metropolitan TFQKD networks. With more research in the future, TFQKD networks can evolve into a promising approach in advancing the development of global quantum communication.

ACKNOWLEDGMENTS

This work is supported by funding from NSERC, MITACS, CFI, ORF, Royal Bank of Canada, Huawei Technology Canada, CRCEF, and the University of Hong Kong start-up grant.

- [1] C. H. Bennett and G. Brassard, Quantum cryptography: Public key distribution and coin tossing. In *Proc. of IEEE Int. Conf. on Comp., Syst. and Signal Proc.*, (Bangalore, India, 1984).
- [2] A. K. Ekert, Quantum Cryptography Based on Bell's Theorem, *Phys. Rev. Lett.* **67**, 661 (1991).
- [3] F. Xu, X. Ma, Q. Zhang, H.-K. Lo, and J. W. Pan, Secure quantum key distribution with realistic devices, *Rev. Mod. Phys.* **92**, 025002 (2020).
- [4] M. Lucamarini, Z. L. Yuan, J. F. Dynes, and A. J. Shields, Overcoming the rate–distance limit of quantum key distribution without quantum repeaters, *Nature* **557**, 400 (2018).
- [5] M. Takeoka, S. Guha, and M. M. Wilde, Fundamental rate-loss tradeoff for optical quantum key distribution, *Nat. Commun.* **5**, 5235 (2014).
- [6] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Fundamental limits of repeaterless quantum communications, *Nat. Commun.* **8**, 15043 (2017).
- [7] H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication, *Phys. Rev. Lett.* **81**, 5932 (1998).
- [8] H.-K. Lo, M. Curty, and B. Qi, Measurement-Device-Independent Quantum key Distribution, *Phys. Rev. Lett.* **108**, 130503 (2012).
- [9] X. Ma, P. Zeng, and H. Zhou, Phase-Matching Quantum key Distribution, *Phys. Rev. X* **8**, 031043 (2018).
- [10] X. B. Wang, Z. W. Yu, and X. L. Hu, Twin-field quantum key distribution with large misalignment error, *Phys. Rev. A* **98**, 062323 (2018).
- [11] J. Lin and N. Lütkenhaus, Simple security analysis of phase-matching measurement-device-independent quantum key distribution, *Phys. Rev. A* **98**, 042332 (2018).
- [12] M. Curty, K. Azuma, and H.-K. Lo, Simple security proof of twin-field type quantum key distribution protocol, *Npj Quantum Inf.* **5**, 1 (2019).
- [13] W. Wang and H.-K. Lo, Simple method for asymmetric twin-field quantum key distribution, *New J. Phys.* **22**, 013020 (2019).
- [14] M. Minder, M. Pittaluga, G. L. Roberts, M. Lucamarini, J. F. Dynes, Z. L. Yuan, and A. J. Shields, Experimental quantum key distribution beyond the repeaterless secret key capacity, *Nat. Photonics* **13**, 334 (2019).
- [15] X. Zhong, J. Hu, M. Curty, L. Qian, and H.-K. Lo, Proof-Of-Principle Experimental Demonstration of Twin-Field Type Quantum key Distribution, *Phys. Rev. Lett.* **123**, 100506 (2019).
- [16] Y. Liu, Z. W. Yu, W. Zhang, J. Y. Guan, J. P. Chen, and C. Zhang *et al.*, Experimental Twin-Field Quantum Key Distribution Through Sending-Or-Not-Sending, *Phys. Rev. Lett.* **123**, 100505 (2019).
- [17] S. Wang, D. Y. He, Z. Q. Yin, F. Y. Lu, C. H. Cui, W. Chen, Z. Zhou, G. C. Guo, and Z. F. Han, Beating the Fundamental Rate-Distance Limit in a Proof-Of-Principle Quantum key Distribution System, *Phys. Rev. X* **9**, 021046 (2019).
- [18] X. T. Fang, P. Zeng, H. Liu, M. Zou, W. Wu, and Y. L. Tang *et al.*, Implementation of quantum key distribution surpassing the linear rate-transmittance bound, *Nat. Photonics* **14**, 422 (2020).
- [19] J. P. Chen, C. Zhang, Y. Liu, C. Jiang, W. Zhang, and X. L. Hu *et al.*, Sending-Or-Not-Sending with Independent

- Lasers: Secure Twin-Field Quantum Key Distribution Over 509 km, *Phys. Rev. Lett.* **124**, 070501 (2020).
- [20] X. Zhong, W. Wang, L. Qian, and H.-K. Lo, Proof-of-principle experimental demonstration of twin-field quantum key distribution over optical channels with asymmetric losses, *Npj Quantum Inf.* **7**, 1 (2021).
- [21] P. D. Townsend, S. J. D. Phoenix, K. J. Blow, and S. M. Barnett, Design of quantum cryptography systems for passive optical networks, *Electron. Lett.* **30**, 1875 (1994).
- [22] D. Castelvecchi, IBM's quantum cloud computer goes commercial, *Nat. News* **543**, 159 (2017).
- [23] C. Elliott, A. Colvin, D. Pearson, O. Pikalo, J. Schlafer, and H. Yeh, Current status of the DARPA quantum network. *Proc. SPIE 5815, Quantum Information and Computation III* (2005).
- [24] W. Chen, Z. F. Han, T. Zhang, H. Wen, Z. Q. Yin, and F. X. Xu *et al.*, Field experiment on a “star type” metropolitan quantum key distribution network, *IEEE Photonics Technol. Lett.* **21**, 575 (2009).
- [25] M. Peev, C. Pacher, R. Alléaume, C. Barreiro, J. Bouda, W. Boxleitner, T. Debuisschert, E. Diamanti, M. Dianati, J. F. Dynes, and S. Fasel, The SECOQC quantum key distribution network in Vienna, *New J. Phys.* **11**, 075001 (2009).
- [26] S. Wang, W. Chen, Z. Q. Yin, Y. Zhang, T. Zhang, H. W. Li, F. X. Xu, Z. Zhou, Y. Yang, D. J. Huang, and L. J. Zhang, Field test of wavelength-saving quantum key distribution network, *Opt. Lett.* **35**, 2454 (2010).
- [27] D. Stucki, M. Legre, F. Buntschu, B. Clausen, N. Felber, N. Gisin, L. Henzen, P. Junod, G. Litzistorf, P. Monbaron, and L. Monat, Long-term performance of the swissQuantum quantum key distribution network in a field environment, *New J. Phys.* **13**, 123001 (2011).
- [28] M. Sasaki, M. Fujiwara, H. Ishizuka, W. Klaus, K. Wakui, M. Takeoka, S. Miki, T. Yamashita, Z. Wang, A. Tanaka, and K. Yoshino, Field test of quantum key distribution in the Tokyo QKD network, *Opt. Express* **19**, 10387 (2011).
- [29] Y. L. Tang, H. L. Yin, Q. Zhao, H. Liu, X. X. Sun, and M. Q. Huang *et al.*, Measurement-Device-Independent Quantum key Distribution Over Untrustful Metropolitan Network, *Phys. Rev. X* **6**, 011024 (2016).
- [30] Y. A. Chen, Q. Zhang, T. Y. Chen, W. Q. Cai, S. K. Liao, J. Zhang, K. Chen, J. Yin, J. G. Ren, Z. Chen, and S. L. Han, An integrated space-to-ground quantum communication network over 4, 600 kilometres, *Nature* **589**, 214 (2021).
- [31] H. Liu, C. Jiang, H. T. Zhu, M. Zou, Z. W. Yu, and X. L. Hu *et al.*, Field Test of Twin-Field Quantum Key Distribution through Sending-Or-Not-Sending Over 428 km, *Phys. Rev. Lett.* **126**, 250502 (2021).
- [32] N. Gisin, S. Fasel, B. Kraus, H. Zbinden, and G. Ribordy, Trojan-horse attacks on quantum-key-distribution systems, *Phys. Rev. A* **73**, 022320 (2006).
- [33] A. Müller, T. Herzog, B. Huttner, W. Tittel, H. Zbinden, and N. Gisin, “Plug and play” systems for quantum cryptography, *Appl. Phys. Lett.* **70**, 793 (1997).
- [34] D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, Quantum key distribution over 67 km with a plug&play system, *New J. Phys.* **4**, 41 (2002).
- [35] Y. Zhao, B. Qi, and H.-K. Lo, Quantum key distribution with an unknown and untrusted source, *Phys. Rev. A* **77**, 052327 (2008).
- [36] Y. Zhao, B. Qi, H.-K. Lo, and L. Qian, Security analysis of an untrusted source for quantum key distribution: Passive approach, *New J. Phys.* **12**, 023024 (2010).
- [37] R. Mandil, L. Qian, and H.-K. Lo, Managing backscattering noise in Sagnac-loop twin-field quantum key distribution. *In Conference on Lasers and Electro-Optics*, p. JTU3A-43 (2021).