Security analysis of orthogonal-frequency-division-multiplexing–based continuous-variable quantum key distribution with imperfect modulation

Hang Zhang, Yu Mao, Duan Huang, Jiawei Li, Ling Zhang,* and Ying Guo
School of Information Science and Engineering, Central South University, Changsha 410083, China

(Received 18 December 2017; published 29 May 2018)

We introduce a reliable scheme for continuous-variable quantum key distribution (CV-QKD) by using orthogonal frequency division multiplexing (OFDM). As a spectrally efficient multiplexing technique, OFDM allows a large number of closely spaced orthogonal subcarrier signals used to carry data on several parallel data streams or channels. We place emphasis on modulator impairments which would inevitably arise in the OFDM system and analyze how these impairments affect the OFDM-based CV-QKD system. Moreover, we also evaluate the security in the asymptotic limit and the Pirandola-Laurenza-Ottaviani-Banchi upper bound. Results indicate that although the emergence of imperfect modulation would bring about a slight decrease in the secret key bit rate of each subcarrier, the multiplexing technique combined with CV-QKD results in a desirable improvement on the total secret key bit rate which can raise the numerical value about an order of magnitude.

DOI: 10.1103/PhysRevA.97.052328

I. INTRODUCTION

Quantum key distribution (QKD), as a major practical application of quantum information, provides the interaction for two parties to share a secret key over an unsecure quantum channel [1–3]. Continuous-variable quantum key distribution (CV-QKD) offers the prospect of high-detection efficiency and the tantalizing promise of providing higher key distribution rates, which are the most highlighted advantages compared with discrete-variable quantum key distribution (DV-QKD) protocols [4–6]. The theoretical security of CV-QKD has been established against general collective Gaussian attacks [7,8], which have been shown to be optimal in the asymptotical limit [9]. However, the CV-QKD scheme was initially plagued with various kinds of problems regarding extending the secure communication distance and increasing secret key rates [10,11]. There are two major problems that limit the secret key rate. The first is the available bandwidth of shot-noise-limited homodyne detectors and the second is the limited speed and efficiency of classical reconciliation [12,13]. Recently, a CV-QKD experiment has been demonstrated over a 25-km fiber channel with a record secret key rate of 1 Mbps [14]. In order to increase the secure key rate, an approach is to improve the currently achievable transport frequencies. However, this requires faster data acquisition cards, wider bandwidth of quantum detectors, and a higher speed of postprocessing procedure, all of which will result in a cumbersome process in experiments.

In recent years, orthogonal frequency division multiplexing (OFDM) has attracted significant attention in fiberoptic communications due to its ability to provide higher spectral efficiency of transmission [15,16]. Many groups have demonstrated the suitability of OFDM and its variants for long-haul optical communication systems [17,18]. In this paper, we illustrate and analyze the use of the OFDM technique to improve the secret key rate and overcome the high-rate issues in the CV-QKD protocol. In our scheme, a modulated separate subcarrier after being overlapped by the OFDM system will form a multiplexing signal. Each individual secret key rate of its own subcarrier will be calculated independently. Moreover, the total secret key rate can be added up after homodyne or heterodyne detection at Bob's side.

However, the performance of OFDM systems is sensitively affected by in-phase and quadrature imbalance (I/Q imbalance) of down converter modulators [19]. The I/Q modulators usually have inevitable imperfections that would result in an imperfect match between the two baseband analog signals, I and Q, which represent the complex carrier [20]. In this paper, we address modulator impairments and discuss how these impairments affect OFDM-based CV-QKD systems. At the same time, We conduct the security analysis of the practical OFDM-based CV-QKD protocol with imperfect modulation and illustrate the secret key bit rate in the asymptotic limit for each subchannel and the whole system. Further, we review the Pirandola-Laurenza-Ottaviani-Banchi (PLOB) upper bound of the multiband quantum channel, and the comprehensive comparisons between the secret key capacity of OFDM CV-QKD and the PLOB bound scenario are employed.

This paper is organized as follows. In Sec. II, we mainly introduce the OFDM-based CV-QKD protocol with imperfect modulation. In Sec. III, we give the security analysis of the OFDM CV-QKD protocol with imperfect modulation, and we give the calculations for the secret key rate. In Sec. IV, the bit error rates and the secret key rates of the modified protocol and the original protocol are compared for performance analysis. The PLOB bound is plotted and discussed as a comparison with the OFDM CV-QKD scenario. Furthermore, we also illustrate the impact on the loss ratio of the secret key bit rate versus the transmission distance under the situation of I/Q imbalance. Our conclusions are drawn in Sec. V.

*lingzhang2017@foxmail.com

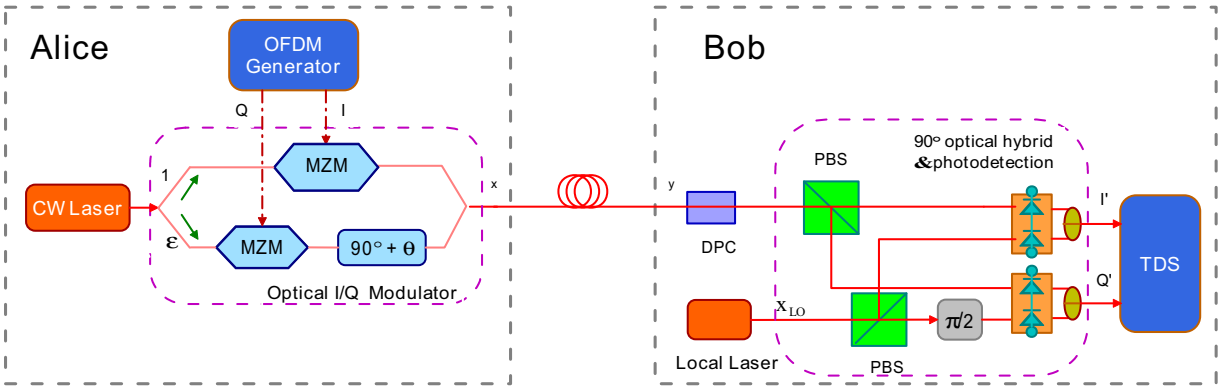

FIG. 1. Schematic of OFDM-based CV-QKD protocol for the transmitter and the receiver. CW Laser, continuous-wave laser; MZM, Mach-Zehnder modulator; DPC, dynamic polarization controller; PBS, polarizing beam splitter; TDS, time-domain-sampling scope.

II. THE CV-QKD PROTOCOL WITH OFDM SYSTEMS

A. OFDM-based CV-QKD protocol

The schematic diagram of the OFDM-based CV-QKD scheme is depicted in Fig. 1. At the transmitter, Alice randomly chooses one of the four coherent states $\alpha_k = \alpha e^{i\pi(2k+1)/4}$, $k \in (1,2,3,4)$, and sends it to Bob with the probability $1/4$ through a quantum channel [21,22]. During the communication between Alice and Bob, the optical signals go through the OFDM system to be modulated and carry the information about the encoded key bits in each subchannel, which is mainly different from the scheme in Ref. [12]. So Bob receives a mixture state ρ_4 that has been modulated by the OFDM technique with the form

$$\rho_4 = \frac{1}{4}\sum_{k=0}^{3} |\alpha_k\rangle\langle\alpha_k|. \tag{1}$$

The OFDM system under investigation consists of a real-time transmitter and an offline-processing-based receiver [23]. The basic block diagram of the OFDM transmission system is shown in Fig. 2, a data source generates serial data which has a high bit rate. After the operation of serial to parallel conversion (S/P), the input high-bit-rate serial data are converted to the low-bit-rate parallel block of a bit stream which is transmitted over a number of overlapped subcarriers. The bitloading mask is then extracted from the data stream and used by the M-QAM mapper [24]. After the QAM mapping, an inverse fast Fourier transform (IFFT) is used to modulate data onto orthogonal subcarriers for transmission and the cyclic prefix (CP) is appended to the time domain OFDM signal to facilitate channel equalization at the receiver. The real and complex valued outputs are then passed to the respective digital to analog conversion modules [25].

In a practical OFDM CV-QKD scheme, there are still some issues that deserve attention, in particular the nonlinear gain of electrical amplifiers, the control of phase shifts in optical waveguides, and cable lengths or circuit paths on printed boards [26,27]. For all these reasons the resulting signal may present amplitude imbalance, angular imbalance, or timing skew, globally referred to as the I/Q imbalance [28]. In the following, we use a suitable model for I/Q imbalance distortion and investigate the effects of the I/Q imbalance on OFDM transmission.

B. Effects of I/Q imbalance distortion on the OFDM system

We first consider an ideal I/Q modulator. As shown in Fig. 3, a cw laser signal (at the carrier frequency) is fed into a power splitter, producing two signals which differ in phase by 90°. This phase relationship is called "quadrature" [29]. These signals are fed to the local oscillator (LO) ports of two identical mixers. The IF ports (or low-frequency/dc ports) of these mixers are fed by the I and Q inputs, respectively. These I/Q signals are referred to as baseband signals. The RF outputs of the two mixers are summed together, with ideally no phase shift between them. The resulting output from this structure is an I/Q modulated signal at the same carrier frequency as the LO port. Whereas, in practical circumstances, the gains of two splitter fed by the cw laser are not going to be absolutely equal, which would cause the I signal to be slightly smaller than the Q signal. At the same time, quadrature skew occurs when the

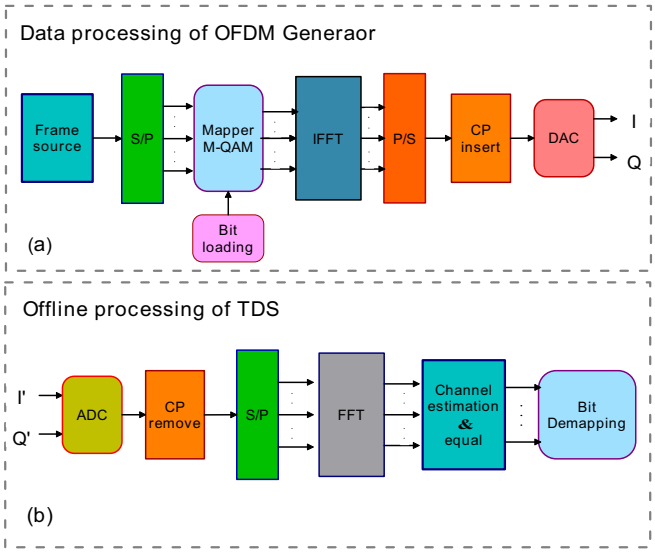

FIG. 2. (a) The schematic of the OFDM transmitter. (b) The offline processing of TDS at the receiver. S/P, serial to parallel conversion; M-QAM, M-ary quadrature amplitude modulation; IFFT, inverse fast Fourier transform; P/S, parallel to serial conversion; CP, cyclic prefix; DAC, digital to analog conversion; ADC, analog to digital conversion; FFT, fast Fourier transform.

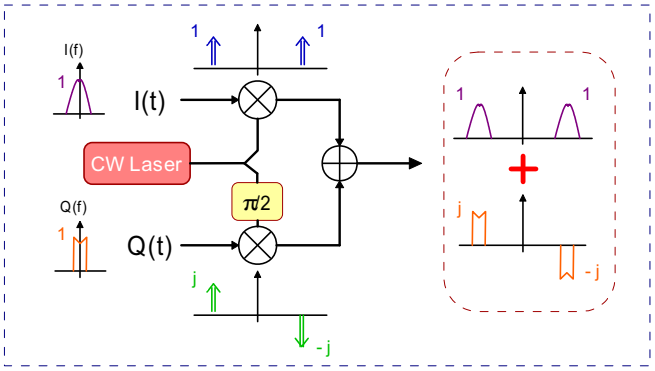

FIG. 3. General description of the I/Q modulator block diagram. CW Laser represents the continuous-wave laser, and $I(t)$ and $Q(t)$ represent the in-phase input and the quadrature input, respectively.

two oscillators used in an I/Q modulator do not differ by 90°. For a small angular error θ, it can be shown that the resulting error is nonorthogonal to the data.

The output I/Q signals of the OFDM generator then drive an I/Q optical modulator biased at the null point and modulate an ideal cw laser, as shown in Fig. 2. Under the circumstances, practically, the different driving electrical signal amplitudes between the in-phase (I) and quadrature (Q) arms of the modulator and the imperfect biasing are respectively referred to as the transmitter gain imbalance, ε_i, and the quadrature skew, θ_i, where i refers to the ith subcarrier transmission [26]. On account of the symmetry of the I and Q components, we assume $0 \leqslant \varepsilon \leqslant 1$ and $0 \leqslant \theta \leqslant \frac{\pi}{2}, i \in [1,2,\ldots,n]$. Under the impact of the I/Q imbalance, the transmitted signal, $x(t)$, can be expressed as

$$x(t) = \mathrm{Re}[X(t)] = \mathrm{Re}\left[\sum_{i=1}^{n} s(t)\left(G_1 e^{j\omega_S t} + G_2 e^{-j\omega_S t}\right)\right], \tag{2}$$

$$G_1 = (1 + \varepsilon_i e^{j\theta_i})/2, \quad G_2 = (1 + \varepsilon_i e^{-j\theta_i})/2, \tag{3}$$

in which $s(t)$ and ω_S denote the baseband signal to be transmitted and the cw laser frequency, respectively. Re is the real part operator. It should be noted that $(\varepsilon,\theta) = (1,0)$ implies that the I/Q imbalance is absent in the system.

The OFDM system has N subchannels. In each of the OFDM subchannels, the information is carried by subcarrier $|\phi_i\rangle$. After the resulting signals and laser are modulated in the optical I/Q modulator, the distorted signals are then transmitted over a optical fiber. When Bob receives the signal, he first makes the signal be combined with the signal emitted by a local oscillator laser, $x_{\mathrm{LO}}(t)$, in a coherent receiver and experience the effect of carrier frequency offset. The received I_R and Q_R components after balanced photo detection, can be written as

$$\begin{aligned} I_R &= \mathrm{Re}(y x_{\mathrm{LO}}^* e^{-j\omega_0 t}), \\ Q_R &= \mathrm{Im}(y x_{\mathrm{LO}}^* e^{-j\omega_0 t}), \end{aligned} \tag{4}$$

where $y(t)$ is the transmitted signal that has experienced the optical fiber channel, and $\omega_0 = \omega_L - \omega_S$ (being the local-oscillator laser angular frequency). Im denotes the imaginary part operator, and $(\cdot)^*$ is the complex conjugation operation.

After digitizing the signals at the outputs of the orthogonal optical hybrid and balanced photodiodes, the signals are collected by using the time-domain-sampling scope (TDS). The TDS steps are as follows: perform operations of analog to digital conversion (ADC), and demodulation and demultiplexing using a fast Fourier transform (FFT) which efficiently separates the subchannels and channel estimation to recover the signals. The channel equalization complexity in the receiver is reduced dramatically by using IFFT at the transmitter and FFT at the receiver [27].

The transmitter input signals at Alice's side in the OFDM generator can be modulated as N subcarriers, whose dimensionless operator is derived by [30]

$$\hat{a}_k = \hat{X}_k + i\hat{P}_k, \tag{5}$$

where k refers to the serial numbers of N subcarriers in the frequency domain; $\hat{X}_k$ and $\hat{P}_k$ respectively represent the regular location and the momentum operator. The modulated quantum signals operating in the OFDM generator can be expressed as

$$\hat{X}_m(t) = \sum_{n=0}^{N-1} \hat{a} e^{\frac{j2\pi kt}{N}} \sum_{n=0}^{N-1} e^{\frac{j2\pi n(m-k)}{N}}. \tag{6}$$

After the IFFT operation, the signals are converted in the time-domain OFDM signal as follows:

$$F^{-1}(\mathbf{z}) = e^{\frac{1}{2}\sigma_{\tau_0}^2 (g_1^2 + g_2^2 + \cdots + g_n^2)}, \tag{7}$$

where $\sigma_{\tau_0}^2$ refers to the modulation variance. Similarly, the ith transmittance vector of the multicarrier transmission can be denoted by T_{N_i}. In consequence, the received signals at Bob's side can be expressed as

$$Y_m(t) = \alpha \cdot \hat{X}_m(t) + \gamma \cdot \hat{X}_m^*(t) + \sum_{i=1}^{n} F^{-1}(T_{N_i}), \tag{8}$$

where α and γ denote a gain imbalance and phase imbalance between the I and Q branches, respectively, and can be derived as [31]

$$\alpha = \cos\theta + j\varepsilon \sin\theta, \tag{9}$$

$$\gamma = \varepsilon \cos\theta - j \sin\theta. \tag{10}$$

At the receiver, subcarrier signals $\hat{c}_m(k)$ are restored with the operation of FFT that can be calculated as

$$\hat{c}_m(k) = \sum_{n=0}^{N-1} \hat{Y}_m(t) e^{-\frac{2ik\pi n}{N}}. \tag{11}$$

And Bob performs homodyne detection or heterodyne detection on the received FFT-operated quantum signals. In the next section we analyze the effects of the proposed OFDM CV-QKD method with I/Q imbalance in the case of asymptotic security.

III. SECURITY ANALYSIS

In this section, we consider the security of the OFDM-based CV-QKD protocol with reverse reconciliation. The modified

protocol could be regarded as simultaneous transmission of N distinct systems. Each of the subcarriers is theoretically independent for orthogonality by the OFDM technique. In practice, imperfect modulation may lead to nonlinearity. Therefore the quadrature of a certain subcarrier will be affected by the nonlinear mixing from other subcarriers, which will bring extra noise ϵ_i of intermodulation distortion for the ith subchannel [12].

In the channel communication, Eve performs the collective Gaussian attack strategy on each of the subchannel simultaneously [32]. The transmittance $T_{\mathrm{Eve}_{(i)}}$ of each subchannel N_i can be derived as

$$|T_{\mathrm{Eve}_{(i)}}|^2 = 1 - |T_{N_i}|, \tag{12}$$

where the T_N transmittance vector of N in the multicarrier transmission is $T_N = [T_{N_1}, \ldots, T_{N_n}]^T$. The covariance matrix $\xi_{\mathrm{Eve}_{(i)}}$ of the ith subchannel in the OFDM system is

$$\xi_{\mathrm{Eve}_{(i)}} = \begin{bmatrix} V_{\mathrm{Eve}_{(i)}}\mathbf{I}_2 & \sqrt{T_{N_i}}Z\sigma_z \\ \sqrt{T_{N_i}}Z\sigma_z & V_{\mathrm{Eve}_{(i)}}\mathbf{I}_2 \end{bmatrix}, \tag{13}$$

where $\mathbf{I}_2$ is the 2×2 identity matrix and $\sigma_z = \mathrm{diag}(1, -1)$. $V_{\mathrm{Eve}_{(i)}}$ indicates the covariance of Eve's attack on the ith subchannel, and $\mathbf{Z}$ refers to the Pauli Z matrix.

At the transmitter, the N coherent states sent from Alice through the corresponding subchannels can be expressed as $|x_i\rangle$, where $i = 1,2,\ldots,n$. Accordingly, Bob's collecting of the states can be denoted by $|x_i^{'}\rangle$ at the receiver. For the ith subcarrier, the secret key rate (bit/pulse) can be expressed as

$$K_{(i)} = \beta I_{\mathrm{AB}_{(i)}} - S_{\mathrm{BE}_{(i)}}, \tag{14}$$

where β is the efficiency of reverse reconciliation assumed to be constant for each subchannel. Reconciliation efficiency $\beta = 97\%$, which could be achieved by using an irregular low density parity check (LDPC) technique, i.e., MET-LDPC code [33] and multiedge quasicyclic LDPC codes [34].

Furthermore, since failure to decode a message is usually associated with data loss in conventional data transmission scenarios, we take the frame error rate (FER) into consideration, which is usually one of the most regarded characteristics of an error-correcting code. The FER is defined as the ratio of the number of bits frames in error to the total detected bits frames in CV-QKD system. Error codes due to loss, dispersion, imperfect sources, and detectors are lumped together as dark count. The secret key rates would be affected by the factor (1 − FER).

Taking into account the previously discussed imperfections in the QKD case, the final key rate is [35]

$$K_{(i)} = (1 - \mathrm{FER})(\beta I_{\mathrm{AB}_{(i)}} - S_{\mathrm{BE}_{(i)}}), \tag{15}$$

where the Shannon mutual information between Alice and Bob, $I_{\mathrm{AB}_{(i)}}$, for homodyne detection can be evaluated from Bob's measured variance $V_{\mathrm{A}_{(i)}}$ and the conditional variance $V_{\mathrm{A|B}}$ as

$$\begin{aligned} I_{\mathrm{AB}_{(i)}} &= \frac{1}{2}\log_2 \frac{(V_{\mathrm{A}_{(i)}} + 1)g}{V_{\mathrm{A|B}} + 1} \\ &= \frac{1}{2}\log_2 \frac{\varepsilon\cos\theta(\langle e^2_{\mathrm{A}_{(i)}}\rangle + 1)}{|F(T_{N_i})|^2(\sigma^2_{N_i} + \delta_i)V_N + 1}, \end{aligned} \tag{16}$$

where V_N is the shot-noise variance and δ_i is the excess noise of ith subchannel N_i. In addition, $\langle e^2_{\mathrm{A}_{(i)}}\rangle$ represents Alice's conditional variance of Bob's received subcarrier $|x_i^{'}\rangle$. $g = \varepsilon\cos\theta$ is the imbalance degree of I/Q modulation.

Eve's information on Bob's measurement $S_{\mathrm{BE}_{(i)}}$ is given by the Holevo bound:

$$\begin{aligned} S_{\mathrm{BE}_{(i)}} &= \frac{1}{2}\log_2 \frac{gV_{\mathrm{B}_{(i)}}}{V_{\mathrm{B|E}}} \\ &= \frac{1}{2}\log_2 \frac{\varepsilon\cos\theta\langle e^2_{\mathrm{B}_{(i)}}\rangle|F(T_{N_i})|^2\left(\sigma^2_{N_i} + \delta_i + \sigma^{-2}_{v_i}\right)}{V_N}, \end{aligned} \tag{17}$$

in which $\sigma^2_{v_i}$ refers to the modulation variance. The OFDM-based CV-QKD protocol is secure under the circumstance that the secret key rate $K_{(i)} > 0$. More details about the calculation are given in Appendix A.

Moreover, we also analyze the upper bound of the secret key rate which is affiliated with the original CV-QKD protocol. The process of calculation is shown in Appendix B. The performance analyses of the modified CV-QKD scheme are compared with the original CV-QKD protocol in next section.

IV. PERFORMANCE ANALYSIS

It has been demonstrated and the experimental results show that the modulation level satisfies $M = 4$ of the M-QAM mapping at the OFDM transmitter system, producing a relatively good robustness against I/Q imbalance, detailed in Ref. [26]. Therefore, the data analysis and simulation in our OFDM-based CV-QKD protocol will satisfy the conclusion. Moreover, the transmittance $T = 10^{-ad/10}$, where $a = 0.2$ dB/km is the loss coefficient of the optical fibers and d is the quantum channel transmission distance. We assume that the system repetition rate is $f = 1$ MHz, fitting in with the current state-of-the-art experimental technology.

SNR is the signal to noise ratio, which is a crucial indicator that measures the ratio between the transmitted signal power and the background noise power. In our scheme, SNR_i of ith subchannel can be denoted by

$$\mathrm{SNR}_i = \frac{[\sigma^2_{v_i}\varepsilon\cos\theta|F(T_{N_i})|^2 - 1][1 - (\sigma^2_{N_i} + \delta_i)]}{1 + \sigma^2_{v_i}|F(T_{N_i})|^2\left(\sigma^2_{N_i} + \delta_i\right)}. \tag{18}$$

And thus, the total signal to noise ratio, $\mathrm{SNR}_{\mathrm{Tol}}$, of the OFDM-based CV-QKD system can be expressed as

$$\mathrm{SNR}_{\mathrm{Tol}} = \frac{1}{n}\sum_{i=1}^{n}\mathrm{SNR}_i. \tag{19}$$

After the signals sent from Alice pass through the channels, the parallel data can be converted to serial data by parallel to serial (P/S) conversion at Bob's side. During the quantum channel, the bits of a data stream can be altered due to noise, interference, and distortion. The bit error rate (BER), which is defined as the number of bit errors divided by the total number of transferred bits, needs to be considered. The BER

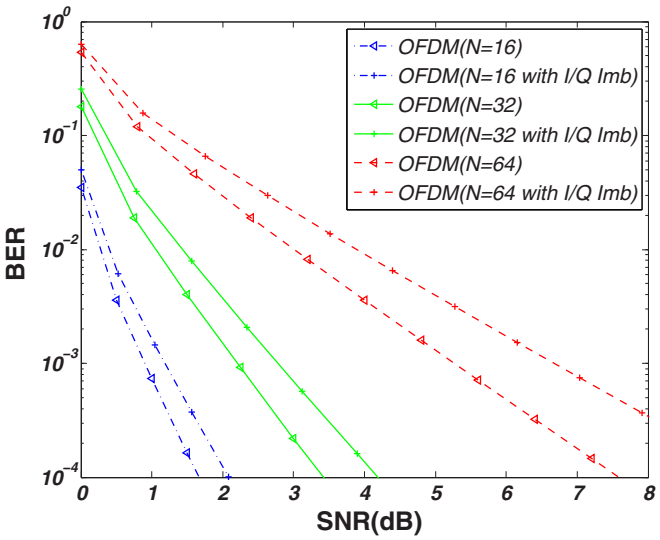

FIG. 4. BER performance in the OFDM-based CV-QKD scheme with I/Q imbalance present versus the SNR when subcarriers are 16, 32, and 64, respectively.

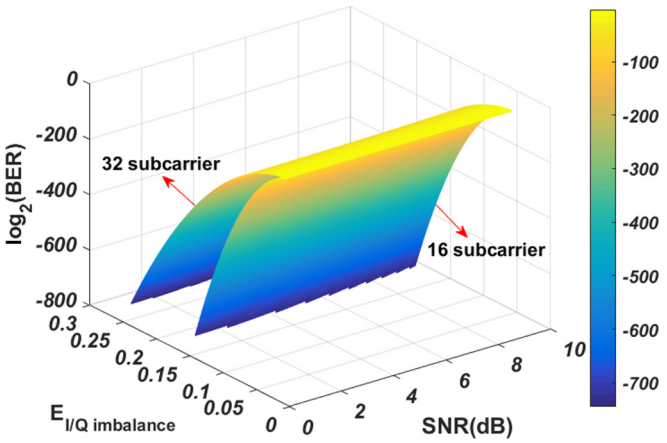

FIG. 5. BER performance as a function of the I/Q imbalance ($E_{I/Q\,\text{imbalance}}$) λ and the SNR. With the increase of the I/Q imbalance, the BER maintains positive behavior at the cost of the extra loss of the SNR, and 16 subcarriers in the scheme possess higher robustness than 32 subcarriers.

is calculated [36] as

$$\text{BER} = \frac{\sqrt{M}-1}{\sqrt{M}\log_2\sqrt{M}}\text{erfc}\left(\sqrt{\frac{2^{\sqrt{N}}-1}{2^{\sqrt{N}-1}}\frac{3\lambda\text{SNR}\log_2 M}{2(M-1)}}\right), \tag{20}$$

where

$$\text{erfc}(x) = \frac{2}{\sqrt{\pi}}\int_x^\infty e^{-t^2}dt, \tag{21}$$

M indicates the modulation level (our scheme employs 4-QAM), N is the number of orthogonal subcarriers, and the λ (quantificat parameter for I/Q imbalance) and SNR are satisfied by $\text{SNR}_{\text{Tol}} = \lambda\text{SNR}$ in which $\lambda = k\varepsilon\cos\theta$ and $k \in (0.8, 1)$ [37,38].

The expectation value of the FER for a data frame length of n bits with probability theory is denoted by

$$\text{FER} = 1 - (1 - \text{BER})^n, \tag{22}$$

which is analyzed in Eq. (15), and $n = 8$ bits (1 byte) is calculated as the data frame length. To measure the BER for 16-, 32-, and 64-subcarrier OFDM systems with and without the I/Q imbalance, a numerical simulation is implemented and is shown in Fig. 4. The required SNR for a BER of 10^{-3} are 1.1 and 1.5 dB for 16 subcarrier OFDM and I/Q imbalance OFDM system with 16 subcarriers, respectively. The OFDM with the impact of the I/Q imbalance can decrease the SNR by 0.4 dB compared with the ideal OFDM systems. By increasing the number of orthogonal subcarriers up to 32, The OFDM improves the SNR at a BER of 10^{-3} by 1.0 dB. The simulation results reveal that with the presence of the I/Q imbalance in the OFDM-based CV-QKD system, the SNR slightly decreases a little bit more than in the ideal OFDM system. The three-dimensional diagram of (SNR, λ, $\log_2$ BER) has been plotted, as shown in Fig. 5, which is of value for us to find the I/Q imbalance's different degrees of influence on the SNR and the BER.

Next, we calculate the secret key rate as a function of the transmission distance. First, the total secret key bit rate K_{Tol} can be derived as

$$K_{\text{Tol}} = f\sum_{i=1}^{n} K_i, \tag{23}$$

where f is the system repetition rate and K_i is the secret key bit per pulse.

The numerical simulation between the secret key bit rate K_{Tol} and the transmission distance for the OFDM-based CV-QKD protocol under the I/Q imbalance when selecting several numbers of subcarriers is shown in Fig. 6. Compared with the single-channel CV-QKD system [39], the total secret key bit rates of the OFDM-based CV-QKD system are considerably increased. Particularly, the greater the number of subcarriers is, the higher the total secret key bit rate is. It is a remarkable fact that the total secret key bit rate K_{Tol} is an increasing function in terms of the total subchannels N. Besides it can be seen clearly that with the impact of the I/Q imbalance the total secret key bit rate and the maximum transmission distance both decrease a little bit, which will degrade the performance in the communication between Alice and Bob. The performances of the OFDM system are limited by the presence of a multipath fading channel with I/Q imbalance. If the communication distance is a relatively long length (within 160 km), a greater number of subcarriers (64 subcarriers) should be chosen to enhance the performance in Alice and Bob's communication.

It can be noticed that the total secret key rate of the OFDM scheme is higher than the upper bound of the original CV-QKD within 170 km. Hence, we could draw a fair conclusion that, when the transmission distance is less than 170 km, the OFDM-based CV-QKD scheme has a better performance than the original scheme. However, we cannot determine which schemes will have the greater performance for a secret key capacity ranging from 170 to 190 km.

It is remarkable that the secret key bit rates of 16, 32, and 64 subcarriers decrease rapidly in a relatively mass range after the transmission distance gets to 150 km, where we can obtain the

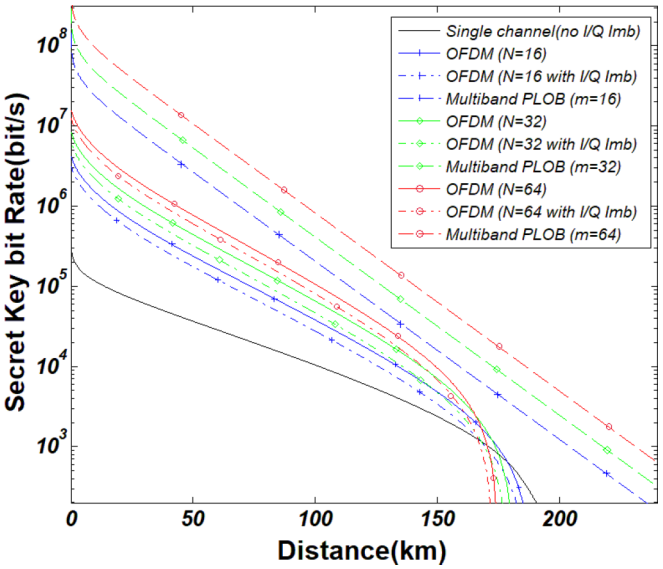

FIG. 6. The comparison between the total secret key bit rate K_{Tol} for the multiplexing OFDM CV-QKD protocol and the upper bound of the original CV-QKD protocol. The other comparison for our proposed protocol with the PLOB bound of the multiband scenario is shown as well, where the secret key bit rate can be calculated as $K_{\mathrm{Tol}}^{\mathrm{PLOB}} = -fm\log_2(1-\eta)$.

optimizing performance between the secret key rate and the transmission distance. The multiplexing technique combined with CV-QKD has a desirable improvement on the limitation of secret key bit rate, the numerical value of which can raise an order of magnitude.

Moreover, we are interested in reviewing the PLOB upper bound in the case of a multiband quantum channel. For any direct transmission protocol over the pure-loss optical channel of transmissivity η, and assuming unlimited authenticated two-way public classical communication, it is shown that the key rate cannot exceed $-\log_2(1-\eta)$ bits per channel used [40]. The PLOB bound of the multiband quantum channel is analyzed in Appendix C.

Based on the discussion above, it is determined that the multiplexing technique of the OFDM-based CV-QKD protocol satisfies the condition. Inspired by this idea, the comparisons of the secret key rate for the OFDM-based CV-QKD and the multiband PLOB upper bound are depicted in Fig. 6. It can be noticed that the OFDM system with N subcarriers do not exceed the PLOB bound of the same channels. Moreover, with the increase of the subchannels, the secret key capacities of K_{OFDM} and K_{PLOB} are both enhanced. The maximum transmission distance of the OFDM-based CV-QKD protocol decreased when adding the sum of the subchannels, while the secret key capacity for the PLOB bound was improved with the greater number of subchannels.

We further illustrate the impact on the loss ratio of the secret key bit rate versus the transmission distance under the situation of I/Q imbalance [14,41]. The tendency of the loss ratio R_{loss} can be expressed as

$$R_{\mathrm{loss}} = \frac{\Delta K}{K_{\mathrm{OFDM}}} = \frac{K_{\mathrm{OFDM}} - K_{\mathrm{OFDM,IQimb}}}{K_{\mathrm{OFDM}}}, \qquad (24)$$

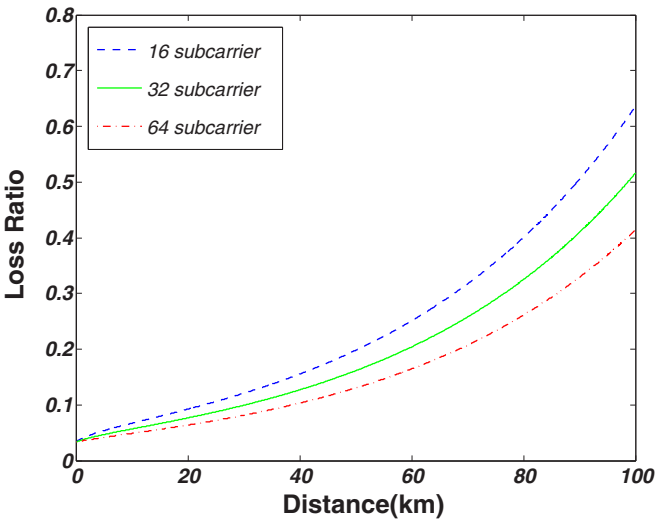

FIG. 7. The loss ratio R_{loss} for the OFDM-based CV-QKD protocol with I/Q imbalance against the transmission distance.

where K_{OFDM} and $K_{\mathrm{OFDM,IQimb}}$ represent the secret key bit rates of the OFDM-based CV-QKD scheme without and with the I/Q imbalance considered, as shown in Fig. 7. The simulation result shows that the loss ratio reaches a higher value when the transmission distance is over 70 km, which means the I/Q imbalance relatively has an even larger impact on the longer transmission distance.

V. CONCLUSION

In summary, we present a scheme for continuous-variable quantum key distribution using the orthogonal frequency division multiplexing technique, and we discuss how the modulation impairments affect OFDM-based CV-QKD systems. Then we find the mismatch brings the possibility of unwanted interference which produces an increase in the BER that is measured in each subcarrier multiplex channel. We also demonstrate the security of the OFDM-based CV-QKD scheme under the imperfect modulation and evaluate the secret key rate in the asymptotic region. Meanwhile, the secret key capacity is compared against the multiband PLOB bound. Our results show that by using the OFDM technique, the maximum transmission distance of each channel will be decreased slightly, while the total secret key rate could increase by roughly an order of magnitude. Furthermore, we notice that the I/Q imbalance increases the required SNR to maintain a certain level of the BER, which will degrade the transmission quality. In terms of the secret key bit rate, the modified scheme of the OFDM-based CV-QKD protocol with I/Q imbalance shows a considerable improvement compared with the original CV-QKD protocol.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 61379153 and No. 61572529).

APPENDIX A: THE CALCULATION OF THE SECRET KEY RATE IN THE OFDM-BASED CV-QKD PROTOCOL

In the OFDM-based CV-QKD scheme, we consider reverse reconciliation and homodyne detection for calculation of the secret key rate. The continuous-variable quantum Fourier transform (CVQFT) transformed noise vector can be written as

$$F(\Delta) = [F(\Delta_1), \ldots, F(\Delta_n)]^T, \tag{A1}$$

where Δ is the Gaussian noise vector. Thus the Fourier-transformed transmittance of the ith subchannel N_i (resulting from the CVQFT operation at Bob) is denoted by $|F(T_{N_i})|^2$ [42].

At the transmitter, the modulated coherent state at Alice's ith subcarrier can be defined as $|x_i\rangle$. After an unsecure quantum channel, the received state at Bob's apparatus is $|x_i^{'}\rangle$, which could be influenced by the noise of the channel. Thus Alice's ith subcarrier $|x_i\rangle$ satisfies [42]

$$\langle x_i^2 \rangle = \sigma_{v_i}^2, \tag{A2}$$

and Bob's ith subcarrier $|x_i^{'}\rangle$ satisfies

$$\langle x_i^{'2} \rangle = |F(T_{N_i})|^2 \sigma_{v_i}^2 + \sigma_{N_i}^2, \tag{A3}$$

where $\sigma_{v_i}^2$ represents the modulation variance of the ith subcarrier. And the noise variance of each subchannel N_i is defined by

$$\sigma_{N_i}^2 = \sigma_{\varepsilon_i}^2 + \epsilon_i, \tag{A4}$$

where $\sigma_{\varepsilon_i}^2$ is the excess noise variance and ϵ_i represents the extra noise variance of intermodulation distortion for the ith subcarrier.

Before calculating Alice's conditional variance on Bob, we first manage to evaluate Alice's estimator $e_{\mathrm{A}_{(i)}}$ on Bob and Bob's estimator $e_{\mathrm{B}_{(i)}}$ on Alice, which can be respectively expressed as

$$e_{\mathrm{A}_{(i)}} = \frac{\langle x_i x_i^{'} \rangle}{\langle x_i^2 \rangle} x_i, \quad e_{\mathrm{B}_{(i)}} = \frac{\langle x_i^{'} x_i \rangle}{\langle x_i^{'2} \rangle} x_i^{'}. \tag{A5}$$

Based on the derivation above, Alice's conditional variance $V_{\mathrm{A|B}}$ of Bob's received state $|x_i^{'}\rangle$ could be given by

$$\begin{aligned} V_{\mathrm{A|B}} &= \langle e_{\mathrm{A}_{(i)}}^2 \rangle - \frac{|\langle x_i e_{\mathrm{A}_{(i)}} \rangle|^2}{\langle x_i^2 \rangle} \\ &= |F(T_{N_i})|^2 \sigma_{N_i}^2 V_N + |F(T_{N_i})|^2 \delta_i V_N, \end{aligned} \tag{A6}$$

where V_N is the shot-noise variance and δ_i is the excess noise of the ith subchannel N_i.

In the proposed OFDM-based CV-QKD protocol, we need to take imperfect modulation into account. Equations (9) and (10) show the relation about gain imbalance and phrase imbalance in the modulated OFDM system. We could evaluate and calculate the numeral impact on the CV-QKD scheme by the factor $g = \varepsilon \cos\theta$ which presents the imbalance degree of I/Q modulation [31]. When $(\varepsilon,\theta) = (1,0)$, i.e., $g = 1$, this implies that I/Q imbalance is not present in the system, which corresponds to Eqs. (2) and (8).

Assuming that Eve performs the optimal collective attacks, for the ith subcarrier, the information accessible to Eve is generally confined to the Holevo bound $S_{\mathrm{BE}_{(i)}}$. Therefore, the definition of the secret key rate in the case of reverse reconciliation under collective attacks can be expressed as

$$K_{(i)} = (1 - \mathrm{FER})(\beta I_{\mathrm{AB}_{(i)}} - S_{\mathrm{BE}_{(i)}}), \tag{A7}$$

where β is the reconciliation efficiency, $I_{\mathrm{AB}_{(i)}}$ is the mutual information of Alice and Bob, and $S_{\mathrm{BE}_{(i)}}$ is the Holevo bound.

Considering the effect of imperfect modulation in the OFDM-based CV-QKD system, the Shannon mutual information between Alice and Bob, $I_{\mathrm{AB}_{(i)}}$, for homodyne detection can be evaluated from Bob's measured variance $V_{\mathrm{A}_{(i)}}$ and the conditional variance $V_{\mathrm{A|B}}$ as

$$\begin{aligned} I_{\mathrm{AB}_{(i)}} &= \frac{1}{2} \log_2 \frac{(V_{\mathrm{A}_{(i)}} + 1)g}{V_{\mathrm{A|B}} + 1} \\ &= \frac{1}{2} \log_2 \frac{\varepsilon \cos\theta \left(\langle e_{\mathrm{A}_{(i)}}^2 \rangle + 1\right)}{|F(T_{N_i})|^2 \left(\sigma_{N_i}^2 + \delta_i\right) V_N + 1}. \end{aligned} \tag{A8}$$

Accordingly, based on Eve's estimator $e_{\mathrm{E}_{(i)}}^A$ on Alice, and Eve's estimator $e_{\mathrm{E}_{(i)}}^B$ on Bob, the conditional variance can be derived as

$$V_{\mathrm{B|E}} = \frac{V_N}{|F(T_{N_i})|^2 \left(\sigma_{N_i}^2 + \delta_i + \sigma_{v_i}^{-2}\right)}. \tag{A9}$$

And Eve's information on Bob's measurement $S_{\mathrm{BE}_{(i)}}$ is given by the Holevo bound:

$$\begin{aligned} S_{\mathrm{BE}_{(i)}} &= \frac{1}{2} \log_2 \frac{g V_{\mathrm{B}_{(i)}}}{V_{B|E}} \\ &= \frac{1}{2} \log_2 \frac{\varepsilon \cos\theta \langle e_{\mathrm{B}_{(i)}}^2 \rangle |F(T_{N_i})|^2 \left(\sigma_{N_i}^2 + \delta_i + \sigma_{v_i}^{-2}\right)}{V_N}. \end{aligned} \tag{A10}$$

APPENDIX B: THE UPPER BOUND OF SECRET KEY RATE IN ORIGINAL CV-QKD PROTOCOL

For a fair comparison, we consider reverse reconciliation and homodyne detection for data postprocessing in this section. We could obtain the reverse secret key capacities of a memoryless quantum channel as the optimal rates which are explicitly shown in the continuous-variable framework by considering arbitrary one-mode Gaussian channels [43,44].

For a quantum memoryless channel $\mathcal{N}$, transforming the input state $\rho_{\mathrm{A}'}$ of a sender (Alice) into the output state $\rho_{\mathrm{B}'}$ of a receiver (Bob), the channel which features a transmission efficiency T and an excess noise ε can always be followed by a trace with the eavesdropper (Eve). Eve is authorized to interact with each coherent state pulse sent by Alice and perform measurements on them after sifting, but before the reconciliation phase. The maximum information on Bob's key available to Eve is limited by the Shannon bound $I(\mathrm{B} : \mathrm{E})$.

The mutual information of Alice and Bob, $I(\mathrm{A} : \mathrm{B})$, is derived from Bob's measured variance $V_{\mathrm{B}} = \eta T(V + \chi_{\mathrm{tot}})$ and the conditional variance $V_{\mathrm{B|A}} = \eta T(1 + \chi_{\mathrm{tot}})$ using Shannon's equation,

$$I_{(\mathrm{A:B})}^{\mathrm{hom}} = \frac{1}{2} \log_2 \frac{V_{\mathrm{B}}}{V_{\mathrm{B|A}}} = \frac{1}{2} \log_2 \frac{V + \chi_{\mathrm{tot}}}{1 + \chi_{\mathrm{tot}}}, \tag{B1}$$

where χ_{tot} represents the total noise referred to the channel input and $V = V_{\text{A}} + 1$ is the variance of quadratures for modes A and B.

Accordingly, Eve's information on Bob's measured quadrature, $I(\text{B} : \text{E})$, is also derived using Shannon's equation in the case of homodyne detection:

$$I_{(\text{B:E})}^{\text{hom}} = \frac{1}{2}\log_2 \frac{V_{\text{B}}}{V_{\text{B|E}}} = \frac{1}{2}\log_2 \frac{T^2(V + \chi_{\text{tot}})(1/V + \chi_{\text{line}})}{1 + T\chi_{\text{hom}}(1/V + \chi_{\text{line}})}, \tag{B2}$$

where the total channel-added noise referred to the channel input is defined as χ_{line} and the detection-added noise referred to Bob's input can be expressed as χ_{hom}.

The highest secret key rate which can be achieved by reverse protocols over a quantum channel $\mathcal{N}$ is called the reverse secret key capacity $K_{\mathcal{N}}$. Based on the analysis of the Shannon mutual information above, we can obtain the upper bound [43]:

$$K_{\mathcal{N}} = I_{(\text{A:B})}^{\text{hom}} - I_{(\text{B:E})}^{\text{hom}}. \tag{B3}$$

It should be noticed that one can never extract the exact amount of mutual information $I(\text{A} : \text{B})$ between Alice and Bob with a finite error-correcting code. Thus the reconciliation efficiency β is introduced in the upper bound secret key rate:

$$K_{\mathcal{N}} = \beta I_{(\text{A:B})}^{\text{hom}} - I_{(\text{B:E})}^{\text{hom}}. \tag{B4}$$

APPENDIX C: THE PLOB BOUND OF A MULTIBAND QUANTUM CHANNEL

For any direct transmission protocol over a pure-loss optical channel, Pirandola-Laurenza-Ottaviani-Banchi (PLOB) have recently proven that the secret key capacity K of the lossy channel is the maximum rate achievable by any optical implementation of QKD [40]. The PLOB upper bound of the secret key rate K_{PLOB} can be expressed as

$$K_{\text{PLOB}} = -\log_2(1 - \eta), \tag{C1}$$

where the parameter η is transmissivity. In general, the transmissivity η and the quantum channel transmission distance d are linked with the expression $\eta = 10^{-ad/10}$, where $a = 0.2$ dB/km is the loss coefficient of the optical fibers.

Moreover, the optimal rate-loss scaling of $K_{\text{PLOB}} \simeq 1.44\eta$ secret bits per channel use has been calculated, which would be a fundamental bound that only quantum repeaters may surpass.

The conclusion above can be used to calculate the PLOB bound secret key rate over a multiband quantum channel ε_{mb} which is represented by a set of m independent channels or bands [40]. The generic two-way capacity of the multiband channel is satisfied by

$$\mathcal{C}(\varepsilon_{\text{mb}}) \geqslant \sum_{i=1}^{m} \mathcal{C}(\varepsilon_i), \tag{C2}$$

where ε_i represents the two-way capacity of the ith subchannel. The condition for equality is that the bands are distillable (detailed in Ref. [40]).

For a distillable parallel multiband channel, the m subchannels are supposed to be independent. The secret key capacity of a multiband channel is considered to be additive. We assume the transmissivity η values of m multibands are equivalent for calculation. Thus the PLOB bound of a multiband quantum channel can be expressed as

$$K_{\text{PLOB}}^{\text{tot}} = \sum_{i=1}^{m} K_{\text{PLOB}}^{(i)} = -m\log_2(1 - \eta). \tag{C3}$$

[1] L. B. Samuel and V. L. Peter, Rev. Mod. Phys. **77**, 513 (2005).
[2] L. S. Madsen, V. C. Usenko, M. Lassen, R. Filip, and U. L. Andersen, Nat. Commun. **3**, 1083 (2012).
[3] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[4] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
[5] H. W. Li, Y. B. Zhao, Z. Q. Yin, S. Wang, Z. F. Han, W. S. Bao, and G. C. Guo, Opt. Commun. **282**, 4162 (2009).
[6] J. Lodewyck, M. Bloch, R. García-Patrón, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).
[7] S. Pirandola, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **101**, 200504 (2008).
[8] A. Leverrier, Phys. Rev. Lett. **114**, 070501 (2015).
[9] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[10] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Phys. Rev. A **86**, 032309 (2012).
[11] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[12] J. Fang, P. Huang, and G. H. Zeng, Phys. Rev. A **89**, 022315 (2014).
[13] D. Huang, P. Huang, D. K. Lin, and G. H. Zeng, Sci. Rep. **6**, 19201 (2016).
[14] D. Huang, D. K. Lin, C. Wang, W. Liu, S. Fang, J. Peng, P. Huang, and G. H. Zeng, Opt. Express **23**, 17511 (2015).
[15] M. Anandan, S. Choudhary, and P. K. Kumar, in *Proceedings of the International Conference on Fibre Optics and Photonics* (IEEE, New York, 2012), p. 1.
[16] S. Amiralizadeh, A. T. Nguyen, and L. A. Rusch, Opt. Express **23**, 26192 (2015).
[17] T. Jaemkarnjanaloha, R. Maneekut, and P. Kaewplung, in *Proceedings of the 13th International Joint Conference on e-Business and Telecommunications, ICETE 2016* (ACM, New York, 2016), Vol. 3, p. 43.
[18] Z. Wang, K. S. Kravtsov, Y. K. Huang, and P. R. Prucnal, Opt. Express **19**, 4501 (2011).
[19] A. G. Helmy, M. D. Renzo, and N. Al-Dhahir, IEEE Commun. Lett. **21**, 1485 (2017).
[20] S. Shimizu, G. Cincotti, and N. Wada, Opt. Express **20**, 525 (2012).
[21] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).

[22] I. Derkach, V. C. Usenko, and R. Filip, Phys. Rev. A **96**, 062309 (2017).
[23] T. Q. Mao, Z. C. Wang, Q. Wang, and L. L. Dai, Opt. Commun. **360**, 1 (2016).
[24] F. H. Xu, B. Qi, and H. K. Lo, New J. Phys. **12**, 113026 (2010).
[25] W. Shieh, Q. Yang, and Y. Ma, Opt. Express **16**, 6378 (2008).
[26] T. H. Nguyen, P. Scalart, M. Gay, L. Bramerie, and C. Peucheret, in *Proceedings of the International Conference on Communication* (IEEE, New York, 2016), p. 1.
[27] A. Amari, P. Ciblat, and Y. Jaouen, in *Proceedings of the Tyrrhenian International Workshop on Digital Communications* (IEEE, New York, 2015), p. 17.
[28] H. Kai, L. F. D. Rosal, S. Weide, C. Kottke, M. Koepp, and V. Jungnickel, in *Proceedings of the 17th ITG-Symposium Photonic Networks* (IEEE, Leipzig, 2016), pp. 1–4.
[29] X. R. Ma, K. Li, and Y. Bai, IEEE Photon. Technol. Lett. **25**, 2047 (2013).
[30] W. Y. Liu, X. Y. Wang, N. Wang, S. N. Du, and Y. M. Li, Phys. Rev. A **96**, 042312 (2017).
[31] H. S. Chung, S. H. Chang, and K. Kim, IEEE Photon. Technol. Lett. **22**, 308 (2010).
[32] D. B. S. Soh, C. Brif, P. J. Coles, N. Lutkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5**, 041010 (2015).
[33] X. Y. Wang, Y. C. Zhang, Z. Y. Li, B. J. Xu, S. Yu, and H. Guo, Quantum Inf. & Comput. **17**, 1123 (2017).
[34] M. Milicevic, C. Feng, L. M. Zhang, and P. G. Gulak, Quantum Inf. **4**, 21 (2018).
[35] P. Jouguet and S. Kunz-Jacques, Quantum Inf. & Comput. **14**, 329 (2014).
[36] H. Chen, M. Chen, and S. Xie, J. Lightwave Technol. **27**, 4848 (2009).
[37] P. Kumar and A. Prabhakar, Opt. Commun. **282**, 3827 (2009).
[38] S. Bahrani, M. Razavi, and J. A. Salehi, J. Lightwave Technol. **33**, 4687 (2015).
[39] P. Huang, J. Fang, and G. H. Zeng, Phys. Rev. A **89**, 042330 (2014).
[40] S. Pirandola, R. Laurenza, C. Ottaviani, and L. Banchi, Nat. Commun. **8**, 15043 (2017).
[41] H. Oka, C. J. Ahn, T. Omori, and K. Y. Hashimoto, in *Proceedings of the International Symposium on Intelligent Signal Processing and Communication Systems* (IEEE, New York, 2015), p. 17.
[42] L. Gyongyosi and S. Imre, Proc. SPIE **9123**, 912307 (2014).
[43] S. Pirandola, R. Garcia-Patron, S. L. Braunstein, and S. Lloyd, Phys. Rev. Lett. **102**, 050503 (2009).
[44] C. Ottaviani, R. Laurenza, T. P. W. Cope, G. Spedalieri, S. L. Braunstein, and S. Pirandola, Quantum Inf. Sci. Technol. II **9996**, 999609 (2016).