

Multichannel parallel continuous-variable quantum key distribution with Gaussian modulationJian Fang,^{*} Peng Huang,[†] and Guihua Zeng[‡]*State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Jiaotong University, Shanghai 200240, China*

(Received 9 October 2013; published 12 February 2014)

We propose a scheme for continuous-variable quantum key distribution (CV-QKD) using the subcarrier multiplexing technique which was employed in microwave photonics. This scheme allows distribution of N channels with independent Gaussian-modulated CV-QKD in parallel with one laser source and several phase modulators. We analyze the influence of nonlinear signal mixing and security in the asymptotic limit. Results indicate that by using this multiplexing technique, each channel will have a non-Gaussian extra source noise, resulting in slight shortening of the maximum transmission distance, while the total secret key rate can be considerably increased. This scheme could also be used for key distribution for multiple users, and combined with wavelength division multiplexing devices it has potential to be used for construction of a CV-QKD network.

DOI: [10.1103/PhysRevA.89.022315](https://doi.org/10.1103/PhysRevA.89.022315)

PACS number(s): 03.67.Dd, 03.67.Hk

I. INTRODUCTION

Quantum key distribution (QKD), a major practical application of quantum information, allows two distant parties to share a common secret key for cryptography in an untrusted environment [1–3]. Its security is guaranteed by the laws of quantum mechanics. Continuous-variable QKD, an alternative to single-photon-based discrete-variable quantum key distribution (DV-QKD), encodes information on the quadratures of a Gaussian state [4]. Any eavesdropping will introduce extra noise between two legal communication parties, who can realize Eve's existence by detecting the excess noise.

The Gaussian-modulated CV-QKD protocols, which have been experimentally demonstrated both in laboratory [5–8] and field [9] tests, are proven to be secure against collective attacks [10,11] and coherent attacks [12,13]. They use homodyne detectors instead of the single-photon counters employed in DV-QKD systems, and are more attractive from a practical point of view. By using multidimensional reverse reconciliation [14,15], the secure transmission distance can be extended to as long as 80 km [8].

Most of the existing CV-QKD systems are pulsed systems and the secret key bit rate R can be expressed as $R = f_{\text{rep}} K$, where f_{rep} denotes the pulse repetition rate and K is the secret key rate (bit per pulse). Compared with classical communication systems, the secret key bit rate of CV-QKD is still low, ranging from several bits/s to hundreds of kbits/s at the distance of more than 25 km [6–9]. There are three possible approaches to solve this problem. The first one is to improve the secret key rate K , which is a diminishing function of the transmission distance and sensitive to the excess noise, so at long transmission distance the secret key rate is much smaller than 10^{-3} bit per pulse. The second approach is to increase the frequency of pulse repetition rate, which requires faster data acquisition cards, wider bandwidth of quantum detectors, and higher postprocessing speed.

The third approach is to use the multiplexing technique, which allows delivery of N independent secret keys in a single

fiber. This method was initially realized by using wavelength division multiplexing (WDM) devices, which need N coherent laser sources with different central frequencies, and each channel needs individual amplitude and phase modulators. The WDM scheme can be deemed as just a combination of several independent QKD systems. Interestingly, the subcarrier multiplexing technique, which was employed in the field of microwave photonics and the radio-on-fiber (ROF) systems, has been proven useful in the BB84 protocol recently [16–18]. In their scheme, the sender Alice randomly encodes one of the discrete phases $\{0, \pi/2, \pi, 3\pi/2\}$ on several radio-frequency (rf) oscillators and the receiver Bob decodes them by using oscillators of frequencies identical to Alice's. This method requires a frequency-locking module between two distant parties, which may increase the complexity of the whole system.

Inspired by this method, we propose a scheme to employ the subcarrier multiplexing technique in the Gaussian-modulated CV-QKD protocol. Unlike in Ref. [18], each rf oscillator is modulated with continuous phase and amplitude information, while the system does not require frequency locking. In our proposal, the subcarrier frequencies are evenly separated. We consider the influence of nonlinear signal mixing and analyze the security against collective attacks. The results are attractive. The Gaussian modulation of each channel will introduce non-Gaussian extra noise, which is generated from the continuous information modulated on other channels. This extra noise is proportional to Alice's modulation variance and cannot be neglected.

We evaluate the secret key bit rate in the asymptotic limit for both each channel and the whole system. Results indicate that the extra source noise will slightly reduce of the maximum transmission distance, while the total secret key rate can be considerably increased. Also each channel could generate independent secret keys at the same time, meaning the key distribution in the multichannel system is parallel. This scheme could be used to distribute keys to multiple users. Combined with current WDM technique, the multichannel scheme has the potential to be used to construct a CV-QKD network.

This paper is structured as follows. In Sec. II, a brief review of the Gaussian protocol is given. In Sec. III, we describe the principle of the multichannel scheme. In Sec. IV, the effect of

^{*}aceofspades@sjtu.edu.cn[†]huang.peng@sjtu.edu.cn[‡]ghzeng@sjtu.edu.cn

nonlinear signal mixing is studied to derive the expression of the extra source noise due to intermodulation. We construct the entanglement-based scheme in Sec. V and use it to analyze the security under collective attacks. The results of numerical simulation are discussed in Sec. VI and conclusions are drawn in Sec. VIII.

II. BRIEF REVIEW OF THE GAUSSIAN PROTOCOL

The Gaussian CV-QKD protocols are based on the Gaussian modulation of a Gaussian state of light, which could be coherent state [4], squeezed state [19], or thermal state [20]. From a practical point of view, the most suitable protocol for experimental demonstration is the Gaussian-modulated coherent state (GMCS) quantum cryptography protocol, which was proposed by Grosshans and Grangier in 2002 [4]. The GMCS protocol requires two independent Gaussian-distributed modulations with the identical variance V_A on the x and p quadratures of a coherent state. Expressed in terms of phase and amplitude, the distribution corresponds to a uniform modulation of the phase in $[0, 2\pi]$ and a Rayleigh distribution of amplitude with the probability density function $\text{Ra}(\sigma = \sqrt{V_A})$, where

$$z \sim \text{Ra}(\sigma) = \frac{z}{\sigma^2} e^{-\frac{z^2}{2\sigma^2}}. \quad (1)$$

Alice’s modulated states are sent to Bob through the quantum channel. The quantum channel is described by the transmission efficiency T and excess noise ϵ , resulting in a noise variance of $1 + T\epsilon$ at Bob’s input. Unlike the DV-QKD

protocol, the GMCS protocol requires a strong local oscillator (LO). In order to ensure that the LO and signal light have identical modes, both the LO and signal light are generated by Alice using an unbalanced beam splitter (BS) from the same pulsed coherent laser. Then Alice applies time multiplexing and polarization multiplexing techniques to let the LO and signal propagate in the same fiber.

When Bob receives the states, he first uses the demultiplexing devices to separate the LO and quantum signal. Then he performs homodyne detection, randomly measuring the x or p quadrature. To measure the quadrature p , he dephases the local oscillator by $\pi/2$. Then Alice and Bob perform classical data processing, including reconciliation and privacy amplification, and finally share the common secret keys from the accumulated data.

III. DESCRIPTION OF THE MULTICHANNEL SCHEME

The operation principle of the multichannel scheme is shown in Fig. 1. Alice uses a beam splitter (BS) to separate the coherent pulsed laser source centered at ω_0 into two beams: One is weaker and the other is stronger. The weaker beam is prepared for generating quantum signals while the stronger beams is used for local oscillators (LO). The optical field is assumed to be quasimonochromatic; i.e., the spectral width $\Delta\omega$ of the pulse spectrum is much smaller than its central frequency ω_0 . This assumption is always satisfied when the pulse width is larger than 0.4 ps [21]. The quantized single-mode electric field $\hat{E}(t)$ of the signal light before modulation can be expressed as

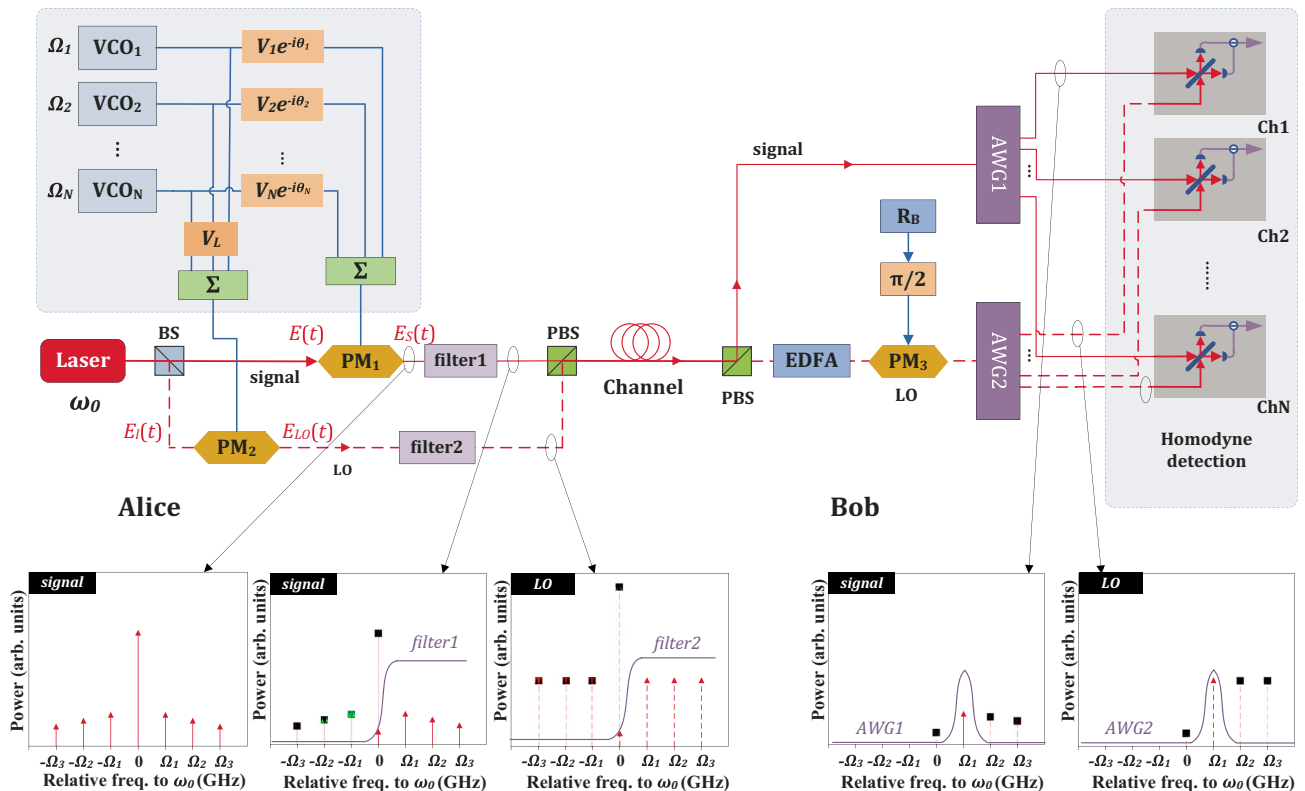


FIG. 1. (Color online) System layout of the multichannel parallel CV-QKD scheme. The signal light is in red (gray) solid line and the local oscillator light is in red (gray) dashed line.

$\hat{E}(t) = \hat{E}^+(t) + \hat{E}^-(t)$, where

$$\hat{E}^+(t) = i\sqrt{\frac{\hbar\omega_0}{2\epsilon_0 V_0}} \hat{a}(0)e^{-i\omega_0 t} \quad (2)$$

and $\hat{E}^-(t) = [\hat{E}^+(t)]^\dagger$. ϵ_0 is the dielectric permittivity and V_0 denotes the mode volume. i is the imaginary unit. $E^+(t)$ and $E^-(t)$ denote the positive-frequency and negative-frequency components of the quantized electric field, respectively. $\hat{a}(0)$ is the dimensionless complex amplitude operator, which can be decomposed by two quadratures as $\hat{a}(0) = \hat{X} + i\hat{P}$. Since $\hat{E}^+(t)$ and $\hat{E}^-(t)$ are conjugated, we need to consider only the positive-frequency component in following discussions, while the identical results could be obtained from the negative one by similar methods.

Signal light is externally modulated through a phase modulator (PM₁) by N radio-frequency (rf) subcarriers. Each subcarrier, which is generated from a voltage control oscillator (VCO) of frequency $\Omega_k, k \in \{1, 2, \dots, N\}$, is independently amplitude modulated by a Rayleigh distributed random number V_k and phase modulated by a uniform distributed random number $\phi_k \in [0, 2\pi]$. All the modulated rf signals are combined together with a bias voltage V_b . Then the voltage applied on PM₁ is expressed as

$$V_S(t) = -\sum_{k=1}^N V_k \cos(\Omega_k t + \phi_k) - V_b. \quad (3)$$

After Alice's phase modulation, the positive-frequency component turns to

$$\begin{aligned} \hat{E}_S^+(t) &= \hat{E}^+(t) \exp\left[-\frac{i\pi V(t)}{V_\pi}\right] \\ &= \hat{E}^+(t) e^{i\theta_b} \exp\left[i \sum_{k=1}^N m_k \cos(\Omega_k t + \phi_k)\right], \end{aligned} \quad (4)$$

where $m_k = V_k \pi / V_\pi$, $\theta_b = V_b \pi / V_\pi$. V_π is the half-wave voltage of the phase modulator. This equation can be written as Taylor expansion with following form:

$$\begin{aligned} \hat{E}_S^+(t) &= \hat{E}^+(t) e^{i\theta_b} \sum_{n=0}^{+\infty} \frac{i^n}{n!} \left[\sum_{k=1}^N m_k \cos(\Omega_k t + \phi_k) \right]^n \\ &\cong \hat{E}^+(t) e^{i\theta_b} \left[1 + \frac{i}{2} \sum_{\substack{k=-N \\ k \neq 0}}^N m_k e^{-i(\Omega_k t + \phi_k)} \right. \\ &\quad \left. + \frac{i^2}{8} \sum_{\substack{r,s=-N \\ r,s \neq 0}}^N m_r m_s e^{-i[(\Omega_r + \Omega_s)t + \phi_r + \phi_s]} \right], \end{aligned} \quad (5)$$

where we define $m_{-k} = m_k$, $\Omega_{-k} = -\Omega_k$ and $\phi_{-k} = -\phi_k$ for any integer $|k| \in \{1, \dots, N\}$. Here we use the second-order Taylor expansion because when m_k is small enough, e.g., $m_k \leq 0.02$, the effect of higher-order terms is negligible [17]. Then the signal field at frequency $\omega_0 + \Omega_k$ is

$$\hat{E}_S^+|_{\omega_0 + \Omega_k}(t) = \frac{1}{2} \hat{E}^+(t) e^{-i\Omega_k t + i\theta_b} C_k, \quad (6)$$

where

$$C_k = i m_k e^{-i\phi_k} + \frac{i^2}{4} \sum_{\substack{r,s=-N \\ r,s \neq 0 \\ \Omega_r + \Omega_s = \Omega_k}}^N m_r m_s e^{-i(\phi_r + \phi_s)}. \quad (7)$$

We can rewrite the expression of $\hat{E}_S^+|_{\omega_0 + \Omega_k}$ in a form similar to that of Eq. (2):

$$\hat{E}_S^+|_{\omega_0 + \Omega_k}(t) = \sqrt{\frac{\hbar(\omega_0 + \Omega_k)}{2\epsilon_0 V}} \hat{a}_k(0) e^{-i(\omega_0 + \Omega_k)t}, \quad (8)$$

where $\hat{a}_k(0) = X_{S(k)} + i P_{S(k)}$ is a new dimensionless complex amplitude operator of mode $\omega_0 + \Omega_k$ and can be expressed as

$$\hat{a}_k(0) = \frac{1}{2} \sqrt{\frac{\omega_0 + \Omega_k}{\omega_0}} C_k e^{i\theta_b} \hat{a}(0) \cong \frac{1}{2} C_k e^{-i\theta_b} \hat{a}(0). \quad (9)$$

If we adjust the bias phase θ_b to $-\arg[\hat{a}(0)] - \pi/2$, then the X quadrature of $\hat{a}_k(0)$ becomes

$$X_{S(k)} = \frac{\alpha_0}{2} m_k \cos(-\phi_k) + \frac{\alpha_0}{8} \sum_{\substack{r,s=-N \\ r,s \neq 0 \\ \Omega_r + \Omega_s = \Omega_k}}^N m_r m_s \sin(\phi_r + \phi_s), \quad (10)$$

where α_0 denotes the norm of $\hat{a}(0)$. The expression of $P_{S(k)}$ can be obtained by interchanging the $\sin(\cdot)$ and $\cos(\cdot)$ functions in Eq. (10). The compound signal then passes through an optical filter, which blocks all the subcarriers below the frequency ω_0 . This is because the subcarrier phase modulation in PM₁ encodes the same information (m_k and ϕ_k) on both the subcarriers centered at $\omega_0 + \Omega_k$ and $\omega_0 - \Omega_k$, while we use only the positive-frequency components for quantum key distribution.

The local oscillator (LO) light can also be generated in a way similar to the signal light. The difference is that the voltage applied on the LO's modulator does not contain randomly modulated information. Therefore the modulation voltage of LO can be written as

$$V_{LO}(t) = -V_L \sum_{k=1}^N \cos(\Omega_k t) - V'_b, \quad (11)$$

where V_L is the amplitude voltage of each RF component and V'_b is the bias voltage. Since LO is usually much larger (typically 10^6 – 10^8 times) than the quantum signal, it can be deemed as a classical optical field $E_l(t) = E_0 e^{-i\omega_0 t}$. So the LO light after modulator PM₂ is

$$\begin{aligned} E_{LO}(t) &\cong E_l(t) e^{i\psi_b} \left[1 + \frac{i m_L}{2} \sum_{\substack{k=-N \\ k \neq 0}}^N e^{-i\Omega_k t} \right. \\ &\quad \left. + \frac{i^2 m_L^2}{8} \sum_{\substack{r,s=-N \\ r,s \neq 0}}^N e^{-i(\Omega_r + \Omega_s)t} \right], \end{aligned} \quad (12)$$

where $m_L = V_L \pi / V_\pi$ and $\psi_b = V'_b \pi / V_\pi$. If bias phase ψ_b is adjust to $-\pi/2$, then the local oscillator light at frequency $\omega_0 + \Omega_k$ is

$$E_{\text{LO}}|_{\omega_0 + \Omega_k}(t) = \frac{1}{2} E_0 e^{-i(\omega_0 + \Omega_k)t} D_k, \quad (13)$$

in which the parameter D_k is

$$D_k = m_L + \frac{i}{4} M_2(N, k) m_L^2, \quad (14)$$

where $M_2(N, k)$ is the numbers of terms satisfying $\Omega_r + \Omega_s = \Omega_k, (|r|, |s| \in \{1, \dots, N\})$. The values of $M_2(N, k)$ can be calculated by enumeration method. We also derive the analytical expression of $M_2(N, k)$ as

$$M_2(N, k) = 2N - k - \frac{3}{2} - \frac{1}{2}(-1)^k. \quad (15)$$

For given total channel numbers N , $M_2(N, k)$ satisfies the following inequation:

$$N - 2 \leq M_2(N, k) \leq 2N - 2. \quad (16)$$

When $m_L \leq 0.01$ and $N \leq 40$, the impact introduced by nonlinear signal mixing on $|D_k|$ is less than 1.5%, which could be neglected. Therefore the LO field of each channel has the constant value $E_{\text{LO}}|_{\omega_0 + \Omega_k} = \frac{1}{2} E_0 m_L e^{-i(\omega_0 + \Omega_k)t}$ as shown in Fig. 1. In order to reduce the effect of scattering and nonlinearity in the fiber, the LO power should not be high enough. As the signal light, the LO is also filtered the subcarriers below ω_0 . Then the compound signal light and LO light are polarization multiplexed into the quantum channel and transmitted to Bob.

After receiving the states sent by Alice, Bob first separates the compound signal and LO by using a polarization beam splitter (PBS). Then he uses an erbium-doped optical fiber amplifier (EDFA) to amplify the LO to a considerable power and randomly phases the LO by $\{0, \pi/2\}$ to select the measurement basis. The random basis choosing procedure is determined by a binary random number generator, and Bob holds its result as R_B . He then uses two arrayed-waveguide gratings (AWG) to filter out each subcarrier and performs balanced homodyne detection on each pairs of signal and LO (both are centered at frequency $\omega_0 + \Omega_k$). Finally, Alice and Bob perform classical data processing, including reverse reconciliation and privacy amplification. After these stages, they share N channel-independent secret keys and the key distribution is completed.

In this paper, we consider three different frequency spacing plans: the low plan ($N = 5$) with evenly spaced (e.g., $\Omega_k = k\Omega_1$) channels from 5 to 25 GHz, the medium plan ($N = 15$) with evenly spaced channels from 2 to 30 GHz, and the high plan ($N = 40$) with evenly spaced channels from 1 to 40 GHz. From a practical point of view, 40-GHz phase modulators are currently commercially available and ultra-narrow-band AWG devices with 1-GHz channel spacing have been experimentally demonstrated [22]. So it is reasonable for us to consider these cases.

IV. EXTRA SOURCE NOISE DUE TO INTERMODULATION

According to Eq. (10), the expression of $X_{S(k)}$ can be written as two parts:

$$X_{S(k)} = X_{A(k)} + \Delta X_{(k)}, \quad (17)$$

where

$$X_{A(k)} = \frac{\alpha_0}{2} m_k \cos(-\phi_k), \quad (18)$$

$$\Delta X_{(k)} = \frac{\alpha_0}{8} \sum_{\substack{r, s = -N \\ r, s \neq 0 \\ \Omega_r + \Omega_s = \Omega_k}}^N m_r m_s \sin(\phi_r + \phi_s).$$

Since m_k follows a Rayleigh distribution $R(\sigma)$ and ϕ_k follows a uniform distribution in $[0, 2\pi]$, $X_{A(k)}$ follows the Gaussian distribution $\mathcal{N}(0, \sigma \alpha_0 / 2)$, which is identical to the modulation in Gaussian CV-QKD protocol. The second part, $\Delta X_{(k)}$, can be seen as a modulation noise. Notice that

$$m_r m_s \sin(\phi_r + \phi_s) = x_r p_s + p_r x_s, \quad (19)$$

where $x_r = m_r \cos \phi_r$, $p_r = m_r \sin \phi_r$, $x_s = m_s \cos \phi_s$, and $p_s = m_s \sin \phi_s$. For different r and s , the random variables x_r , p_r , x_s , and p_s are mutually independent and follow the same Gaussian distribution $\mathcal{N}(0, \sigma)$. Hence the probability density function of $x_r p_s$ (also for $x_s p_r$) is given by [23]

$$\begin{aligned} f(z) &= \int_{-\infty}^{+\infty} \int_{-\infty}^{+\infty} \frac{e^{-\frac{x^2}{2\sigma^2}}}{\sigma \sqrt{2\pi}} \frac{e^{-\frac{y^2}{2\sigma^2}}}{\sigma \sqrt{2\pi}} \delta(xy - z) dx dy \\ &= \frac{1}{\pi \sigma^2} K_0\left(\frac{|z|}{\sigma^2}\right), \end{aligned} \quad (20)$$

where $K_0(\cdot)$ is the zero-order modified Bessel function of the second kind and $\delta(\cdot)$ is the δ function. The mean values of the products are $\langle x_r p_s \rangle = \langle x_s p_r \rangle = 0$ while the variances are $\langle (x_r p_s)^2 \rangle = \langle (x_s p_r)^2 \rangle = \sigma^4$. So the variance of the term $m_r m_s \sin(\phi_r + \phi_s)$ is

$$\langle (m_r m_s \sin(\phi_r + \phi_s))^2 \rangle = \begin{cases} 2\sigma^2 & \text{for } r \neq s, \\ 4\sigma^2 & \text{for } r = s. \end{cases} \quad (21)$$

As shown in Sec. II, the total number of combinations satisfying $\Omega_s + \Omega_r = \Omega_k$ is $M_2(N, k)$. For an odd integer k , the combination $2\Omega_s = \Omega_k$ does not exist, so Ω_k can only be decomposed by the combinations of $\Omega_r + \Omega_s, r \neq s$. Since Ω_r and Ω_s are commutable, the term $m_r m_s \sin(\phi_r + \phi_s)$ exists twice. Therefore $\langle \Delta X_{(k)} \rangle = 0$ and the variance of ΔX can be expressed as

$$\langle \Delta X_{(k)}^2 \rangle = \frac{\alpha_0^2}{64} \left[\frac{M_2(N, k)}{2} \times 4 \times 2\sigma^4 \right] = \frac{\alpha_0^2}{16} M_2(N, k) \sigma^4. \quad (22)$$

When k is an even integer, there is one combination $2\Omega_s = \Omega_k$. So in this case $\langle \Delta X_{S(k)}^2 \rangle$ becomes

$$\begin{aligned} \langle \Delta X_{(k)}^2 \rangle &= \frac{\alpha_0^2}{64} \left[\frac{M_2(N, k) - 1}{2} \times 4 \times 2\sigma^4 + 4\sigma^4 \right] \\ &= \frac{\alpha_0^2}{16} M_2(N, k) \sigma^4, \end{aligned} \quad (23)$$

which is identical with the case of odd k . The variance of $\Delta P_{(k)}$ can be derived in a similar way. We assign the variance of $X_{A(k)}$ as $V_A = \alpha_0^2 \sigma^2 / 4$. Since $m_k \sim \text{Ra}(\sigma)$, the mean value of m_k should be $\bar{m}_k = \sigma \sqrt{\pi/2}$. Then the variance of $\Delta X_{(k)}$

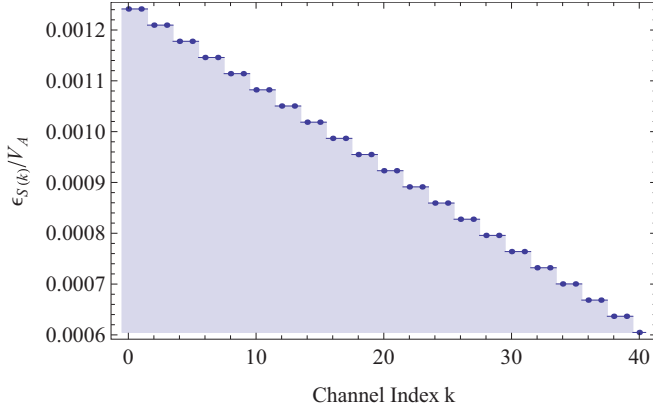


FIG. 2. (Color online) Source noise to modulation variance ratio $\epsilon_{S(k)}/V_A$ in terms of the channel index k . The total channel number is $N = 40$ and the mean value of m_k is 0.01.

and $\Delta P_{(k)}$ can be expressed in terms of \bar{m}_k and V_A as

$$\epsilon_{S(k)} \triangleq \langle \Delta X_{(k)}^2 \rangle = \langle \Delta P_{(k)}^2 \rangle = \frac{1}{2\pi} M_2(N, k) \bar{m}_k^2 V_A, \quad (24)$$

and finally we get

$$\langle X_{S(k)}^2 \rangle = \langle P_{S(k)}^2 \rangle = V_A + \epsilon_{S(k)}, \quad (25)$$

where $\epsilon_{S(k)}$ is the noise variance due to intermodulation defined in Eq. (24). From a physical point of view, the generation of $\epsilon_{S(k)}$ is the result of the nonlinear mixing between different modulated rf signals. As shown in Eqs. (3) and (4), although the rf voltages are combined linearly, phase modulation is not a linear process. Therefore the quadratures of a certain channel will be affected by the nonlinear mixing from other channels. In addition, since the modulated information of each channel is independent, the extra source noise is also independent of the Gaussian modulation of each channel. Hence it could be treated as a noise term in our analysis.

Figure 2 shows the ratio $\epsilon_{S(k)}/V_A$ in terms of the channel index k when $N = 40$. We find that the first channel ($k = 1$) has the maximum value of 0.001 24 while the last channel ($k = N$) has the minimum one of 0.0006. Other channels are placed between the first and last cases. When N is large, e.g., $N = 40$, the maximal value of $\epsilon_{S(k)}/V_A$ is approximately double that of the minimal one.

Notice that although each quadrature of V_A follows a Gaussian distribution, $\epsilon_{S(k)}$ is not a Gaussian noise. This situation is different from previous studies about the source noise, which was assuming to be Gaussian [24,25]. According to Eq. (24), since the extra source noise is proportional to V_A , it cannot be suppressed by increasing the variance of the modulation and then attenuating the state, so this noise must be taken into account in both theoretical analysis and actual experiments.

V. SECURITY OF THE MULTICHANNEL SCHEME

A. Entanglement-based scheme

In the preparation and measurement scheme of the k th channel,

$$\begin{aligned} X_{(k)} &= X_{A(k)} + \Delta X_{(k)} + \delta X_{(k)}, \\ P_{(k)} &= P_{A(k)} + \Delta P_{(k)} + \delta P_{(k)}, \end{aligned} \quad (26)$$

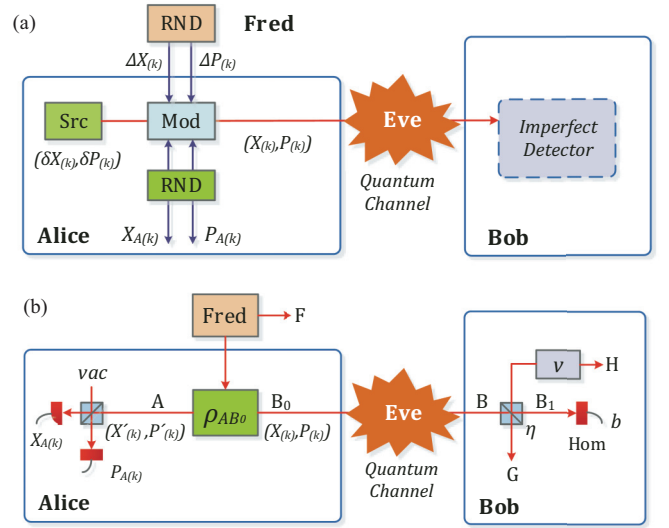


FIG. 3. (Color online) The entanglement-based scheme of the k th channel. Fred is assumed to be a neutral party and Eve cannot benefit from either Fred's information or the imperfections of Bob's homodyne detector.

where $\delta X_{(k)}$ and $\delta P_{(k)}$ originate from shot noise and satisfy the relation $\langle \delta X_{(k)}^2 \rangle = \langle \delta P_{(k)}^2 \rangle = 1$ (in shot noise unit). $X_{A(k)}$ and $P_{A(k)}$ are Alice's modulated random numbers and satisfy the Gaussian distribution that $\mathcal{N}(0, V_A)$. $\Delta X_{(k)}$ and $\Delta P_{(k)}$ are the added non-Gaussian noise with variance $\epsilon_{S(k)}$. The variances of $X_{(k)}$ and $P_{(k)}$ are

$$\langle X_{(k)}^2 \rangle = \langle P_{(k)}^2 \rangle = V_A + 1 + \epsilon_{S(k)}, \quad (27)$$

and the conditional variances $V_{X_{(k)}|X_{A(k)}}$ and $V_{P_{(k)}|P_{A(k)}}$ are [26]

$$\begin{aligned} V_{X_{(k)}|X_{A(k)}} &= \langle X_{(k)}^2 \rangle - \frac{\langle X_{(k)} X_{A(k)} \rangle^2}{\langle X_{A(k)}^2 \rangle} = 1 + \epsilon_{S(k)} \\ V_{P_{(k)}|P_{A(k)}} &= \langle P_{(k)}^2 \rangle - \frac{\langle P_{(k)} P_{A(k)} \rangle^2}{\langle P_{A(k)}^2 \rangle} = 1 + \epsilon_{S(k)}. \end{aligned} \quad (28)$$

In the equivalent entanglement-based scheme, which is shown in Fig. 3(b), Fred generates a pure three-mode entanglement state $|\Psi_{ABF(k)}\rangle$ satisfying $\text{tr}_F(|\Psi_{ABF(k)}\rangle\langle\Psi_{ABF(k)}|) = \rho_{AB_0(k)}$. The quadratures $(X_{(k)}, P_{(k)})$ denote the state sent to Bob, and $(X'_{(k)}, P'_{(k)})$ denote the state kept by Alice. Here we assume that $(X_{(k)}, P_{(k)})$ and $(X'_{(k)}, P'_{(k)})$ satisfy the following relations:

$$\langle X'^2_{(k)} \rangle = \langle P'^2_{(k)} \rangle = V, \quad \langle X^2_{(k)} \rangle = \langle P^2_{(k)} \rangle = V + \epsilon_{S(k)}, \quad (29)$$

where $V = V_A + 1$. According to the uncertainty relation [26], we have

$$|\langle X_{(k)} X'_{(k)} \rangle| \leq V(V + \epsilon_{S(k)}) - \frac{V}{V + \epsilon_{S(k)}}. \quad (30)$$

Since the three-party system Alice-Bob-Fred (ABF) may not be maximally entangled, the correlation between modes A and B_0 may not saturate the limit in Eq. (30), so it can be reasonably assumed that

$$\langle X_{(k)} X'_{(k)} \rangle = \sqrt{V^2 - 1}, \quad \langle P_{(k)} P'_{(k)} \rangle = -\sqrt{V^2 - 1}. \quad (31)$$

In the entanglement-based (E-B) scheme, when Alice takes a heterodyne detection on $X'_{(k)}$ and $P'_{(k)}$ simultaneously, the measurement values can be expressed as $X'_{A(k)} = X'_{(k)} - \delta X'_{A(k)}$ and $P'_{A(k)} = P'_{(k)} - \delta P'_{A(k)}$, where $\langle (\delta X'_{A(k)})^2 \rangle = \langle (\delta P'_{A(k)})^2 \rangle = 1$. Alice's best estimation of $(X'_{(k)}, P'_{(k)})$ is denoted by $(X_{A(k)}, P_{A(k)})$, which satisfies [26]

$$X_{A(k)} = \sqrt{\frac{V-1}{V+1}} X'_{A(k)}, \quad P_{A(k)} = -\sqrt{\frac{V-1}{V+1}} P'_{A(k)}, \quad (32)$$

and finally we have $\langle X_{A(k)}^2 \rangle = \langle P_{A(k)}^2 \rangle = V_A$ and $V_{X(k)|X_{A(k)}} = V_{P(k)|P_{A(k)}} = 1 + \epsilon_{S(k)}$, which has the identical results as in the prepare-and-measurement (P-M) scheme. If we hide the entanglement source and Alice's detection in a black box, the eavesdropper cannot distinguish which scheme is applied, so we can conclude that this E-B scheme is equivalent to the P-M scheme.

In the P-M scheme, Bob's imperfect detector is featured by a detection efficiency η and the electric noise variance v_{el} . We could define an added noise χ_h that refers to Bob's input as $\chi_h = (1 - \eta + v_{el})/\eta$. In the E-B scheme, it is modeled by a beam splitter with transmission of η coupled with an Einstein-Podolsky-Rosen (EPR) state of variance v . So in the E-B scheme, the added noise referred to as Bob's input is $(1 - \eta)v/\eta$. To make the detection-added noise equal, the variance v should be chosen as $v = (1 - \eta + v_{el})/(1 - \eta)$.

B. Security against collective attacks

In this section, we consider the security of the multichannel CV-QKD protocol with reverse reconciliation. According to the fact that coherent attacks are the most powerful eavesdropping attacks and are not more efficient than collective attacks [10,11], we will analyze the security against collective attacks.

Since the quadrature information of each channel is independent, we assume Eve's attacks of every channel are also independent of others. Fred is supposed to be a neutral party which can not be controlled by the eavesdropper [27]. This situation implies that both Alice and Eve cannot benefit from the information kept by Fred. Then the secret key rate (bit/pulse) of the k th channel is expressed as

$$K_{(k)} = \beta I_{AB} - S_{BE}, \quad (33)$$

where β is the efficiency of reverse reconciliation assumed to be constant for each channel. I_{AB} , which represents the Shannon mutual information between Alice and Bob, can be derived from Bob's measured variance V_{B_2} and the conditional variance $V_{B_2|A}$ as

$$I_{AB} = \frac{1}{2} \log_2 \frac{V_{B_2(k)}}{V_{B_2|A}} = \frac{1}{2} \log_2 \frac{V + \epsilon_{S(k)} + \chi_{\text{tot}}}{1 + \epsilon_{S(k)} + \chi_{\text{tot}}}, \quad (34)$$

where $\chi_{\text{tot}} = \chi_{\text{line}} + \chi_h/T$ and $\chi_{\text{line}} = 1/T - 1$. T is the transmission efficiency of the quantum channel and can be evaluated by the transmission distance L by $T = 10^{-0.02L}$. Eve's information on Bob's measurement is given by the Holevo bound [28]:

$$S_{BE} = S(\rho_E) - S(\rho_{E|B=b}), \quad (35)$$

where $S(\cdot)$ denotes the von Neumann entropy and b represents the measurement result of Bob. Here we consider Alice and

Fred together as a larger state A' . Since the fact that Eve has the ability to purify the system $A'B$, we have $S(\rho_E) = S(\rho_{A'B})$. After Bob's measurement, the global pure state collapses to $\rho_{A'EGH|b}$, so $S(\rho_{E|b}) = S(\rho_{A'GH|b})$. Notice that the state $\rho_{A'GH|b}$ is determined by state $\rho_{A'B}$ [24]. According to the optimality of Gaussian attacks [10,11], S_{BE} reaches its maximum when the state $\rho_{A'B}$ (i.e. ρ_{FAB}) is Gaussian. Then the Eve's information can be bounded by

$$S_{BE} \leq S_{BE}^G = S(\rho_{FAB}^G) - S(\rho_{FAGH|b}^G), \quad (36)$$

where ρ_{FAB}^G is a Gaussian state with the covariance matrix [27]

$$\gamma_{FAB}^G = \begin{bmatrix} F_{11} & F_{12} & F_{13} \\ F_{21} & V\mathbb{I}_2 & \sqrt{T(V^2-1)}\sigma_z \\ F_{31} & \sqrt{T(V^2-1)}\sigma_z & T(V + \epsilon_{S(k)} + \chi_{\text{line}})\mathbb{I}_2 \end{bmatrix}, \quad (37)$$

which is identical to the covariance matrix of ρ_{FAB} . $\mathbb{I}_2 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. $F_{m,n}$ represents the unknown 2×2 matrix describing either F or its correlations with AB . Although the entropy of ρ_{FAB}^G can not be calculated directly, there exists another Gaussian state $\rho_{FAB}'^G$ with the covariance matrix $\gamma_{FAB}'^G$

$$\gamma_{FAB}'^G = \begin{bmatrix} \mathbb{I}_2 & 0 & 0 \\ 0 & V'\mathbb{I}_2 & \sqrt{T(V'^2-1)}\sigma_z \\ 0 & \sqrt{T(V'^2-1)}\sigma_z & T(V' + \chi_{\text{line}})\mathbb{I}_2 \end{bmatrix}, \quad (38)$$

where $V' = V + \epsilon_{S(k)}$. The reduced state $\rho_B'^G = \text{tr}_{FA}(\rho_{FAB}'^G)$ is identical to the reduced state $\rho_B^G = \text{tr}_{FA}(\rho_{FAB}^G)$; therefore ρ_{FAB}^G can be changed to $\rho_{FAB}'^G$ through a unitary transformation U_{FA} [29]. Then we have $S(\rho_{FAB}'^G) = S(\rho_{FAB}^G)$. Similarly, the conditional state $\rho_{FAGH|b}^G$ can be transformed into the $\rho_{FAGH|b}'^G$ through U_{FA} , then $S(\rho_{FAGH|b}'^G) = S(\rho_{FAGH|b}^G)$. Therefore we have

$$S_{BE} \leq S_{BE}^G = S(\rho_{FAB}'^G) - S(\rho_{FAGH|b}'^G), \quad (39)$$

and the lower bound $\tilde{K}_{(k)}$ of the secret key rate can be expressed as

$$\begin{aligned} \tilde{K}_{(k)} &= \beta I_{AB} - S_{BE}^G, \\ &= \beta I_{AB} - \sum_{j=1}^3 G\left(\frac{\lambda_j - 1}{2}\right) + \sum_{j=4}^7 G\left(\frac{\lambda_j - 1}{2}\right), \end{aligned} \quad (40)$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$. The first three symplectic eigenvalues $\lambda_{1,2,3} \geq 1$, which are derived from the covariance matrix $\gamma_{FAB}'^G$, can be expressed as

$$\lambda_{1,2} = \frac{1}{2}(A \pm \sqrt{A^2 - 4B}), \quad \lambda_3 = 1, \quad (41)$$

where

$$\begin{aligned} A &= (V + \epsilon_{S(k)})^2 - 2T[(V + \epsilon_{S(k)})^2 - 1] \\ &\quad + T^2(V + \epsilon_{S(k)} + \chi_{\text{line}})^2 \\ B &= T^2[1 + (V + \epsilon_{S(k)})\chi_{\text{line}}]^2. \end{aligned} \quad (42)$$

The symplectic eigenvalues $\lambda_{4,5,6,7} \geq 1$ can be obtained from the covariance matrix $\gamma_{FAGH|b}^G$ and have the following form:

$$\lambda_{4,5}^2 = \frac{1}{2}(C \pm \sqrt{C^2 - 4D}), \quad \lambda_{6,7} = 1, \quad (43)$$

where

$$C = \frac{A\chi_h + (V + \epsilon_{S(k)})\sqrt{B} + T(V + \epsilon_{S(k)} + \chi_{\text{line}})}{T(V + \epsilon_{S(k)} + \chi_{\text{line}}) + \chi_h} \quad (44)$$

$$D = \frac{\sqrt{B}(V + \epsilon_{S(k)}) + B\chi_h}{T(V + \epsilon_{S(k)} + \chi_{\text{line}}) + \chi_h},$$

where A and B are given in Eq. (42). Based on Eqs. (41), (42), (43), and (44), we can calculate the asymptotic lower bound of the secret key rate in Eq. (40) against collective attacks.

VI. SIMULATION AND DISCUSSION

For a given total channel number N , the bit rate of the secret key of the k th channel is given as

$$R_{(k)} = f_{\text{rep}} \tilde{K}_{(k)}, \quad (45)$$

where $\tilde{K}_{(k)}$ is the secret key bit per pulse and can be evaluated using Eq. (33). We assume the system repetition rate f_{rep} , quantum efficiency η , and the electronic noise of homodyne detector v_{el} as $f_{\text{rep}} = 1$ MHz, $\eta = 0.552$, and $v_{el} = 0.015$, corresponding to the typical experimental parameters [8]. The excess noise ϵ is assumed to be $\epsilon = 0.02$, which is a conservative value [6]. The reverse reconciliation is set to $\beta = 0.93$, which is an achievable value with existing techniques [15]. We choose $V_A = 10$ as the modulation variance at Alice's side.

According Fig. 2, since the first and last channels have the maximal and minimal extra source noise, we need to evaluate only the secret key of these two channels while the other channels are placed between them. Figure 4 shows the secret key bit rate for the first ($k = 1$) and last ($k = N$) channels in cases of $N = 5, 15$, and 40 . For each case, the $k = N$ channel always performs best among all the channels in both secret key

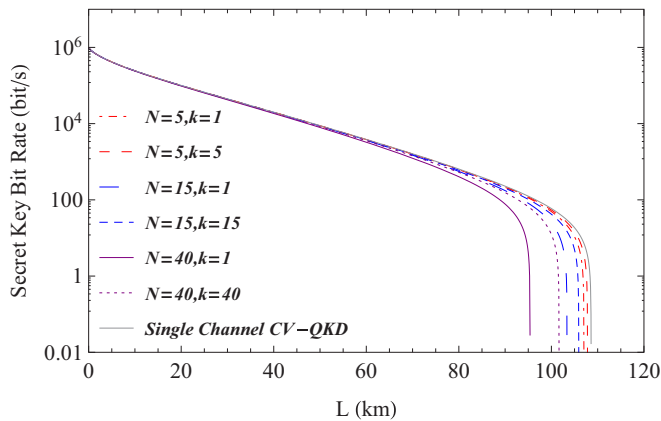


FIG. 4. (Color online) The secret key bit rate $R_{(k)}$ as a function of transmission distance L of the first and last channels. Curves from left to right are $(N, k) = (40, 1), (40, 40), (15, 1), (15, 15), (5, 1), (5, 5)$, and the single-channel case.

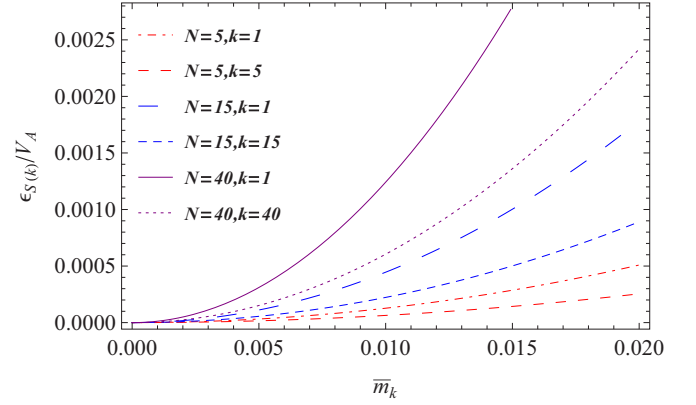


FIG. 5. (Color online) Source noise to modulation variance ratio $\epsilon_{S(k)}/V_A$ in terms of \bar{m}_k of the first channel ($k = 1$) and the last channel ($k = N$). Curves from top to bottom represent $(N, k) = (40, 1), (40, 40), (15, 1), (15, 15), (5, 1),$ and $(5, 5)$, respectively.

rate and the maximum transmission distance while the $k = 1$ channel performs the worst. This is because the extra source noise introduced by intermodulation is a decreasing function of the channel index k as shown in Fig. 2 and an increasing function of the total channel number N as shown in Fig. 5. Due to the extra source noise, the maximum transmission distance and the secret key rate of the subcarrier channels are smaller than single-channel CV-QKD.

The total secret key bit rate can be defined as a sum of key rate of each channel

$$R_{\text{tot}} = \sum_{k=1}^N R_{(k)}. \quad (46)$$

R_{tot} as a function of transmission distance L is demonstrated in Fig. 6. The total secret key bit rate is considerably increased with the channel numbers N from 0 to 80 km. Interestingly, the maximum transmission distance is a decreasing function in terms of N . We also find that the high-count channel system (e.g., $N = 40$) may perform worse than the midcount and low-count channel systems in certain distance ranges

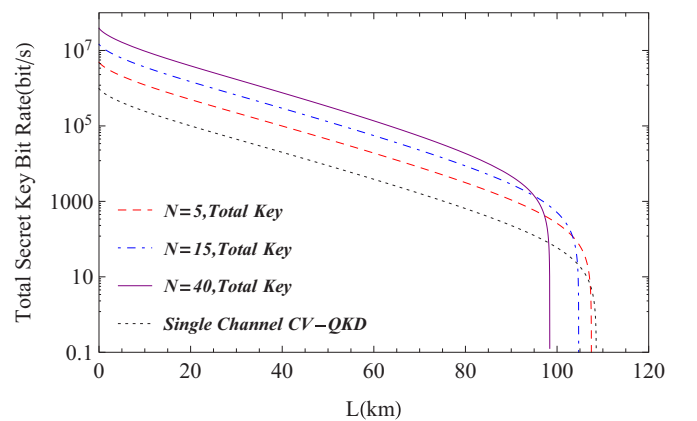


FIG. 6. (Color online) The total secret key bit rate R_{tot} as a function of transmission distance L in cases of different channel plans. From top to bottom: $N = 40, 15, 5$, and the single channel case.

(90–110 km). This is mainly due to the fact that R_{tot} of the high-count system starts to go down and falls to zero rapidly, while at this distance the low-count system still has a positive key rate. With the increase of total channel numbers, the effect of nonlinear signal mixing between channels becomes more salient. As a result, more extra source noise will be introduced when channel number N grows. In the security analysis model, since the states Alice sent turn noisy, the maximum secure distance of each channel will be reduced. Therefore, the performance of both each channel and total secret bit rate will turn down at longer distance.

In order to estimate the increment on the secret key bit rate of multichannel protocol, we define the multichannel gain as

$$G_M = \frac{R_{\text{tot}}}{R_{sc}} = \frac{1}{R_{sc}} \sum_{k=1}^N R_{(k)}, \quad (47)$$

where R_{sc} represents the secret key bit rate of a single-channel CV-QKD with the identical parameters as those in the multichannel scheme. Figure 7(a) shows the evolution of G_M as a function of the mean value of m_k at the distance of $L = 50$ km. For $\bar{m}_k \leq 0.005$, the effect of nonlinear signal mixing can be neglected and the multichannel gain is almost identical

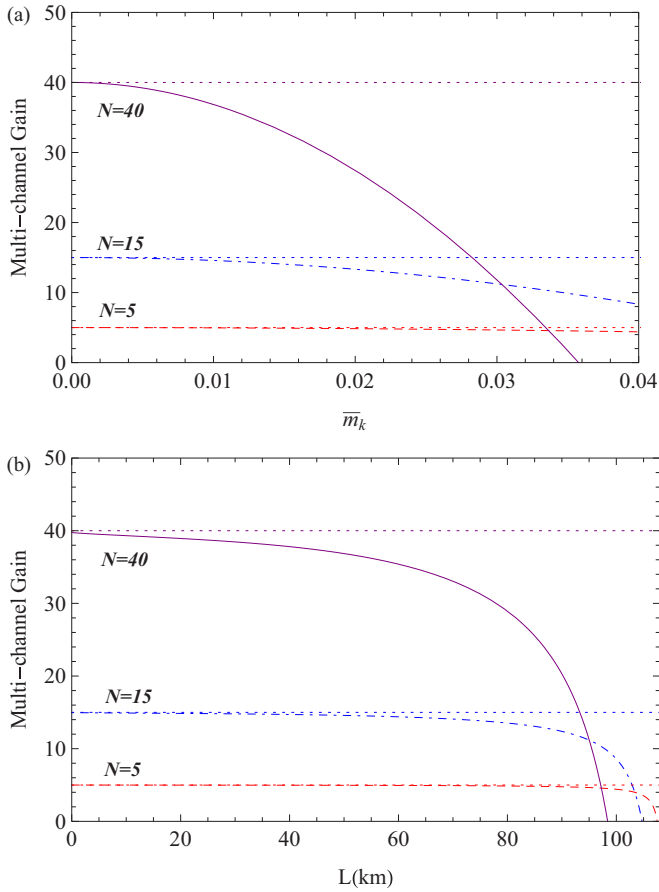


FIG. 7. (Color online) The multichannel gain of the system. Panel (a) is the function of \bar{m}_k at the distance of $L = 50$ km. Panel (b) is the function of transmission distance when $\bar{m}_k = 0.01$. Curves from top to bottom are $N = 40, 15$, and 5 . Dotted lines act as a reference. Other parameters: $\beta = 0.93$, $\epsilon = 0.02$, $\eta = 0.552$, $v_{el} = 0.015$, and $V_A = 10$.

to the number of channels (N). With the increase of \bar{m}_k , G_M is reduced, so $G_M \leq N$. Figure 7(b) demonstrates the relation between G_M and the transmission distance L with $\bar{m}_k = 0.01$. G_M descends rapidly with the increment of L and finally falls to zero when R_{tot} reaches its maximum transmission distance. In short distance ranges (e.g., $L \leq 30$ km), the multichannel system greatly improves the total secret key bit rate with a gain of about N times.

VII. PRACTICAL CONSIDERATIONS

Now we turn to consider the practical limitations implemented on the ideal scheme. In the previous discussions, we use ideal arrayed-waveguide gratings (AWGs) as the optical filters in our theoretical analysis. In practice, the implementation of our scheme depends on both the bandwidth of modulator and the resolution of AWG device. Now, 40-GHz phase modulators are commercially available. The state of the art in AWGs could have 32 outputs, with 10-GHz channel spacing, more than -30 dB extinction ratio and -3 dB attenuation for the central channels [30]. Spacing between channels could be reduced to 5 GHz by spectral interleaving of two devices with extra -3 dB attenuation. Ultranarrow AWG with 1-GHz spacing has been available since 2002 [22] but has not been commercialized yet. In principle, no fundamental limitation exists on the attainable channel separation. Thus future development on AWG technologies would improve its performance, including narrower spacing, higher extinction ratio, and lower insert loss.

In this paper, our target is to estimate the best improvement by applying our multichannel scheme, and the improvement could be seen as the upper bound. However, implementation imperfections may reduce the improvement, depending on how defective the devices are. We reconsider the impact on the total secret key bit rate with the typical imperfective values (e.g., -3 dB AWG attenuation and -10 dB extinction ratio). Results show that although these implementation imperfections will make the total key rate decreased, our scheme still has positive improvement. Future improved AWG devices will make the performance much closer to the ideal estimation, which has been evaluated in our theoretical analysis.

Besides the optical filters, it is also assumed that the modules, such as the light source, amplifier, and VCO, are ideal devices. In practice, as the channel spacing we use in our scheme becomes narrower, the requirements we need for these modules become greater. For example, when the channels are 1 GHz apart, both the lasers and amplifiers need to have KHz linewidth, as well as very stable VCOs. Ultranarrow-bandwidth lasers and EDFAs, centered at 1550 nm with KHz linewidth, are both commercially available. VCO stable at 40 GHz has also been demonstrated, with a wide locking range of 10.6 GHz and low phase noise of -108.65 dBc/Hz at 1-MHz offset [31], meaning that very stable output could be ensured. So these current technologies are sufficient to be applied in our scheme.

VIII. CONCLUSIONS

In summary, we present a scheme for continuous variable quantum key distribution using the subcarrier multiplexing

technique in microwave photonics. We study the generation of both the subcarrier signal and the local oscillator light. We also analyze the influence of nonlinear signal mixing and the extra source noise due to intermodulation. We find the extra source noise is non-Gaussian distributed and proportional to the modulation variance V_A . Then we investigate the security against collective attacks and evaluate the lower bound for the secret key rate. Our results show that by using this multiplexing technique, the maximum transmission distance of each channel will decreased slightly, while the total secret key rate could have a considerable improvement.

We also notice that our scheme could be used for key distribution for multiple users. As shown in Sec. IV, each channel generates an independent secret key at the same time, meaning the key distribution in the multichannel system is parallel. This scheme could be used for one Alice to distribute keys to several Bobs. Limited by the electro-optic modulators,

the bandwidth occupied by the multichannel scheme is under 100 GHz, which is smaller than the interval of WDM devices, so several multichannel CV-QKD systems with different central frequencies could be combined with WDM devices, resulting in a potential CV-QKD network.

Future work will be the experiments of generating the multichannel signals and the demonstration of the multichannel CV-QKD system.

ACKNOWLEDGMENTS

This work was supported by the National Natural Science Foundation of China (Grants No. 61170228 and No. 61332019), China Postdoctoral Science Foundation (Grant No. 2013M540365), and Shanghai Jiao Tong University Postdoctoral Research Foundation (No. AE606203).

-
- [1] N. Gisin, G. Ribordy, W. Tittle, and H. Zbinden, *Rev. Mod. Phys.* **74**, 145 (2002).
 - [2] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dusek, N. Lutkütkenhaus, and M. Peev, *Rev. Mod. Phys.* **81**, 1301 (2009).
 - [3] 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).
 - [4] F. Grosshans and P. Grangier, *Phys. Rev. Lett.* **88**, 057902 (2002).
 - [5] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, *Nature (London)* **421**, 238 (2003).
 - [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] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, *Phys. Rev. A* **76**, 052323 (2007).
 - [8] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, *Nat Photon.* **7**, 378 (2013).
 - [9] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, *New J. Phys.* **11**, 045023 (2009).
 - [10] R. García-Patrón and N. J. Cerf, *Phys. Rev. Lett.* **97**, 190503 (2006).
 - [11] M. Navascués, F. Grosshans, and A. Acín, *Phys. Rev. Lett.* **97**, 190502 (2006).
 - [12] R. Renner and J. I. Cirac, *Phys. Rev. Lett.* **102**, 110504 (2009).
 - [13] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. B. Scholz, M. Tomamichel, and R. F. Werner, *Phys. Rev. Lett.* **109**, 100502 (2012).
 - [14] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, *Phys. Rev. A* **77**, 042325 (2008).
 - [15] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, *Phys. Rev. A* **84**, 062317 (2011).
 - [16] A. Ortigosa-Blanch and J. Capmany, *Phys. Rev. A* **73**, 024305 (2006).
 - [17] J. Capmany, A. Ortigosa-Blanch, J. Mora, A. Ruiz-Alba, W. Amaya, and A. Martinez, *IEEE J. Sel. Top. Quantum Electron.* **15**, 1607 (2009).
 - [18] A. Ruiz-Alba, J. Mora, W. Amaya, A. Martínez, V. García-Muñoz, D. Calvo, and J. Capmany, *IEEE Phot. J.* **4**, 931 (2012).
 - [19] N. J. Cerf, M. Levy, and G. Van Assche, *Phys. Rev. A* **63**, 052311 (2001).
 - [20] C. Weedbrook, S. Pirandola, and T. C. Ralph, *Phys. Rev. A* **86**, 022318 (2012).
 - [21] G. P. Agrawal, *Nonlinear Fiber Optics* (Academic Press, New York, 2001).
 - [22] K. Takada, M. Abe, T. Shibata, and K. Okamoto, *J. Lightwave Technol.* **20**, 850 (2002).
 - [23] E. Weisstein, *Normal Product Distribution*, <http://mathworld.wolfram.com/NormalProductDistribution.html>.
 - [24] Y. Shen, H. Zou, L. Tian, P. Chen, and J. Yuan, *Phys. Rev. A* **82**, 022317 (2010).
 - [25] Y. Shen, X. Peng, J. Yang, and H. Guo, *Phys. Rev. A* **83**, 052304 (2011).
 - [26] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, *Quantum Inf. Comput.* **3**, 535 (2003).
 - [27] P. Huang, G. He, and G. Zeng, *Int. J. Theor. Phys.* **52**, 1572 (2013).
 - [28] A. S. Holevo, *Probl. Peredachi Inf.* **9**, 3 (1973).
 - [29] M. A. Nielson and I. L. Chuang, *Quantum Computation and Quantum information* (Cambridge University Press, Cambridge, 2000).
 - [30] C. R. Doerr and K. Okamoto, in *Optical Fiber Telecommunications* (Academic, San Diego, CA, 2008).
 - [31] J.-C. Chien and L.-H. Lu, in *Proceedings of the International Solid-State Circuits Conference (ISSCC 2007)*, San Francisco, CA, USA, Feb. 2007 (IEEE Press, Piscataway, NJ, 2007), pp. 544–621.