Passive state preparation in the Gaussian-modulated coherent-states quantum key distribution

Bing Qi,[1,2,*] Philip G. Evans,[1] and Warren P. Grice[1]

[1]*Quantum Information Science Group, Computational Sciences and Engineering Division,*
Oak Ridge National Laboratory, Oak Ridge, Tennessee 37831, USA
[2]*Department of Physics and Astronomy, The University of Tennessee, Knoxville, Tennessee 37996, USA*

In the Gaussian-modulated coherent-states (GMCS) quantum key distribution (QKD) protocol, Alice prepares quantum states *actively*: For each transmission, Alice generates a pair of Gaussian-distributed random numbers, encodes them on a weak coherent pulse using optical amplitude and phase modulators, and then transmits the Gaussian-modulated weak coherent pulse to Bob. Here we propose a *passive* state preparation scheme using a thermal source. In our scheme, Alice splits the output of a thermal source into two spatial modes using a beam splitter. She measures one mode locally using conjugate optical homodyne detectors, and transmits the other mode to Bob after applying appropriate optical attenuation. Under normal conditions, Alice's measurement results are correlated to Bob's, and they can work out a secure key, as in the active state preparation scheme. Given the initial thermal state generated by the source is strong enough, this scheme can tolerate high detector noise at Alice's side. Furthermore, the output of the source does not need to be single mode, since an optical homodyne detector can selectively measure a single mode determined by the local oscillator. Preliminary experimental results suggest that the proposed scheme could be implemented using an off-the-shelf amplified spontaneous emission source.

I. INTRODUCTION

Quantum key distribution (QKD) has drawn a lot of attention for its proven security against adversaries with unlimited computing power [1–6]. In QKD, two remote legitimate users (Alice and Bob) can establish a secure key by transmitting quantum states through an insecure channel controlled by the adversary (Eve). Any attacks by Eve will, with a high probability, disturb the transmitted quantum state, and thus can be detected.

Many practical QKD systems are based on the so-called prepare-and-measure scheme, where Alice prepares quantum states and transmits them to Bob, who in turn performs measurements. The quantum state preparation step is conventionally implemented in an *active* manner: Alice first generates truly random numbers using a quantum random number generator [7,8], which she uses to prepare a corresponding quantum state by performing modulations on the output of a single source, or switching among multiple sources. One well-known example is the decoy state BB84 QKD using phase randomized weak coherent sources [9–11], where for each transmission, Alice needs to randomly prepare one of the four BB84 states [1], randomly change the average photon number (to generate either the signal state or one of the decoy states), and (in certain implementations) randomize the global phase of the weak coherent state [12]. As the transmission rate in QKD has been growing dramatically over the years, it is becoming more and more challenging to prepare quantum state precisely at the corresponding speed.

More recently, *passive* state preparation schemes have been proposed in QKD as an alternative approach [13–25]. In this scheme, Alice explores intrinsic fluctuations of the source, or intentionally designs the source in a way such that certain parameters (for example, intensity) will present unpredictable fluctuations. Typically, two optical modes with correlated fluctuations are output from the source. By measuring one mode locally, Alice can determine the random noise carried by the other mode, which will be transmitted to Bob. This idea was initially proposed as a simple way to generate random intensity fluctuations in the decoy-state QKD protocols [13–15]. Later on, it was also applied in preparing the four BB84 states approximately [24].

So far the passive state preparation scheme has only been studied in discrete-variable (DV) QKD based on single photon detection. Here we propose a passive state preparation scheme in continuous-variable (CV) QKD based on coherent detection [26–28].

CV-QKD based on coherent detection could potentially be a cost-effective solution in practice, especially over a relatively short distance [29]. One of the most promising CV-QKD protocols is the Gaussian-modulated coherent-states (GMCS) QKD [28], which has been demonstrated over practical distances [28,30–35]. Similar to the case of DV QKD, in the GMCS QKD, quantum states are prepared actively: For each transmission, Alice first generates a pair of Gaussian-distributed random numbers, then encodes them on a weak coherent state using optical amplitude and phase modulators. Since the modulation format is relatively complicated and the tolerable modulation error is small, high extinction ratio modulators with good stability are required in the GMCS QKD [36].

In this paper, we propose a passive state preparation scheme using a thermal source. One observation is that in the GMCS QKD, from Eve's and Bob's points of view, the quantum states sent by Alice are thermal. So, instead of preparing a thermal state from a coherent state by preforming Gaussian

*qib1@ornl.gov

modulations, Alice can simply use a thermal source: Alice splits the output of the thermal source into two spatial modes using a beam splitter. She measures both the X and P quadratures of one mode using conjugate optical homodyne detectors, and transmits the other mode to Bob after applying appropriate optical attenuation. To estimate the quadrature values of the outgoing mode, Alice can scale down her measurement results by the attenuation applied on the outgoing beam. At Bob's end, he performs similar measurements to determine the quadrature values of the received state. Under normal conditions, Alice's measurement results will be correlated to Bob's, and they can further work out a secure key. Note in this scheme, the shared randomness originates from the intrinsic quadrature fluctuations of a thermal state. We remark that our propsoal is different from previous studies on CV-QKD using the noisy coherent state or thermal state [37–39], where the super-Poissonian photon statistics of the source is regarded as excess noise in CV-QKD based on active state preparation. It was first proposed in [37] that the above preparation noise could be suppressed by increasing the modulation variance and then applying strong attenuation.

One may wonder whether the vacuum noise introduced by Alice's conjugate optical homodyne detection will ultimately prevent her from acquiring a precise estimation of the quadrature values of the outgoing mode. As we will show in this paper, given the initial thermal state generated by the source is strong enough, the contribution of Alice's detector noise on the estimation error of the outgoing state can be reduced effectively by introducing high attenuation on the outgoing mode.

In practice, it may be difficult to prepare a *single mode* thermal state and match its spectral-temporal mode with that of the local oscillator (LO) used in homodyne detection. Fortunately, to implement our protocol, Alice's thermal source does not need to be single mode. The LO in homodyne detection acts as a mode "filter" and can selectively measure only one mode emitted by the source. By using a multimode (broadband) source, it is also easy to align the central wavelength of the LO within the spectrum of the thermal source.

This paper is organized as follows: In Sec. II, we present details of the GMCS QKD based on a passive state preparation scheme. In Sec. III, we conduct numerical simulations to estimate the potential secure key rates of the proposed scheme. In Sec. IV, we characterize the output of a practical amplified spontaneous emission (ASE) source. Preliminary results suggest that such a source could be employed to implement the passive state preparation scheme. Finally, we conclude this paper with a discussion in Sec. V.

II. PASSIVE STATE PREPARATION SCHEME

Presently, the GMCS QKD protocol is implemented based on the prepare-and-measure scheme: For each transmission, Alice draws two random numbers x_A and p_A, prepares a coherent state $|x_A + ip_A\rangle$ accordingly, and sends the prepared state to Bob through an insecure quantum channel. Here x_A and p_A are Gaussian random numbers with zero mean and a variance of $V_A N_0$, where V_A is the modulation variance chosen by Alice, and $N_0 = 1/4$ denotes the shot-noise variance. At Bob's end, he can either implement the homodyne protocol [28] by randomly measuring X or P quadrature for each
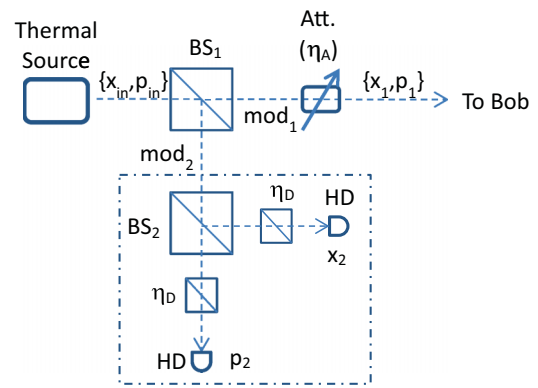

FIG. 1. The proposed passive state preparation scheme in the GMCS QKD. BS_1/BS_2, 50:50 beam splitter; Att., optical attenuator; HD, homodyne detector. The efficiency of the homodyne detector is modeled by a beam splitter with a transmittance of η_D. Note the combination of BS_1 and Att. could be replaced by an asymmetric beam splitter.

incoming pulse, or he can implement the heterodyne protocol [40] by first splitting the incoming pulse into two, and then measuring one in the X basis and the other in the P basis. After the above quantum transmission stage, Alice and Bob estimate the transmission efficiency and added noise of the channel. If the observed noise is below a certain threshold, they can work out a secure key by performing reconciliation and privacy amplification.

Note, from Eve and Bob's points of view, the state from Alice is a single-mode thermal state with an average photon number of $V_A/2$. In fact, the security of the GMCS QKD is commonly proved based on an equivalent entanglement-based protocol [41], where Alice performs conjugate homodyne detection on one mode of a two-mode squeezed vacuum state and sends the other mode to Bob. In this picture, the state from Alice is indeed thermal.

Here, we propose a passive state preparation scheme using a thermal source. While this protocol can be conveniently implemented with a multimode thermal source, for simplicity, in this section we assume the thermal source is single mode. The protocol is summarized as follows (see Fig. 1).

(1) Alice splits the output of a thermal source into two spatial modes (mod_1 and mod_2 in Fig. 1) using a 50:50 beam splitter. We assume the average output photon number of the source is n_0.

(2) Alice attenuates the average photon number of mod_1 down to $V_A/2$ by using an optical attenuator and transmits it to Bob. Here $V_A < n_0$ is the desired modulation variance.

(3) Alice measures both the X and P quadratures of mod_2 by performing conjugate homodyne detection. From her measurement results of $\{x_2, p_2\}$, Alice estimates the quadrature values of the outgoing mode as $x_A = \sqrt{\frac{2\eta_A}{\eta_D}} x_2$ and $p_A = \sqrt{\frac{2\eta_A}{\eta_D}} p_2$, where η_A is the transmittance of the optical attenuator and η_D is the efficiency of Alice's detector.

(4) Bob measures both the X and P quadratures of the received quantum state by performing conjugate homodyne detection. His measurement results are $\{x_B, p_B\}$.

(5) Alice and Bob repeat the above process many times.

(6) Alice and Bob perform reconciliation and privacy amplification on the raw data $\{x_A, p_A\}$ and $\{x_B, p_B\}$. Given the observed noise is below a certain threshold, they can work out a secure key. This step is the same as in the active state preparation scheme.

Note from Eve's point of view, the quantum state sent by Alice in this passive state preparation scheme is the same as the one in the conventional active state preparation scheme. So the well-established security proofs of the GMCS QKD can be applied directly in our scheme. To evaluate the secure key rate, we need to determine how much additional noise will be introduced by this passive state preparation scheme. As we will show below, given the thermal state generated by the source is bright enough, our scheme can tolerate high noise and low efficiency of Alice's detector. We remark that the combination of BS_1 and Att. in Fig. 1 could be replaced by an asymmetric beam splitter.

For simplicity, we only consider the X quadrature below. The P quadrature can be studied in a similar way. The X quadrature of the outgoing state is given by

$$x_1 = \sqrt{\frac{\eta_A}{2}} x_{in} + \sqrt{1 - \frac{\eta_A}{2}} x_{v1}, \qquad (1)$$

where x_{in} stands for the X quadrature of the output of the source, η_A is the transmittance of the optical attenuator, and x_{v1} represents vacuum noise introduced by the beam splitter and the attenuator.

Similarly, Alice's measurement result of the X quadrature is given by

$$x_2 = \sqrt{\frac{\eta_D}{4}} x_{in} + \sqrt{1 - \frac{\eta_D}{4}} x_{v2} + N_{el}, \qquad (2)$$

where η_D and N_{el} are the efficiency and noise of Alice's detector; x_{v2} represents vacuum noise due to the two 50:50 beam splitters and the loss of detector. We assume N_{el} is Gaussian noise with zero mean and a variance of υ_{el}. In this paper, all of the noise variances are defined in the shot-noise unit.

Alice can estimate x_1 from her measurement result x_2 using

$$x_A = \sqrt{\frac{2\eta_A}{\eta_D}} x_2. \qquad (3)$$

Using (1)–(3), Alice's uncertainty on x_1 is given by

$$\Delta = \langle (x_A - x_1)^2 \rangle = \frac{2\eta_A}{\eta_D}\left(1 + \upsilon_{el} - \frac{\eta_D}{2}\right) + 1. \qquad (4)$$

From (4), the excess noise (the noise above vacuum noise) due to the passive state preparation scheme is given by

$$\varepsilon_A = \Delta - 1 = \frac{2\eta_A}{\eta_D}\left(1 + \upsilon_{el} - \frac{\eta_D}{2}\right). \qquad (5)$$

From (5), by increasing the attenuation on the outgoing mode (decreasing η_A), the excess noise ε_A can be effectively reduced. The maximum attenuation Alice can apply is constrained by the average photon number n_0 of the thermal state produced by the source and the desired modulation variance V_A. Using the relation $V_A = \eta_A n_0$, we can revise (5) as

$$\varepsilon_A = \frac{2V_A}{n_0 \eta_D}\left(1 + \upsilon_{el} - \frac{\eta_D}{2}\right). \qquad (6)$$

From (6), given a desired modulation variance V_A, the brighter the source, the smaller the excess noise introduced by Alice. A typical homodyne detector in the GMCS QKD can achieve $\eta_D = 0.5$ and $\upsilon_{el} = 0.1$. For a typical value of $V_A = 1$, to reduce the excess noise ε_A below 0.01, the required average photon number of the source is about 340 (per spatial-temporal mode), which can be satisfied by a practical ASE source, as shown in Sec. IV.

III. SIMULATION RESULTS

We conduct numerical simulations of the secure key rates of the passive state preparation scheme. The asymptotic secure key rate of the GMCS QKD, in the case of reverse reconciliation, is given by Refs. [30,42],

$$R = f I_{AB} - \chi_{BE}, \qquad (7)$$

where I_{AB} is the Shannon mutual information between Alice and Bob; f is the efficiency of the reconciliation algorithm; χ_{BE} is the Holevo bound between Eve and Bob. I_{AB} and χ_{BE} can be determined from the channel loss, observed noises, and other QKD system parameters.

We assume the quantum channel between Alice and Bob is telecom fiber with an attenuation coefficient of γ. The channel transmittance is given by

$$T = 10^{\frac{-\gamma L}{10}}, \qquad (8)$$

where L is the fiber length in kilometers.

In the case of conjugate homodyne detection, the noise added by Bob's detector (referred to Bob's input) is given by [42]

$$\chi_{het} = [1 + (1 - \eta_D) + 2\upsilon_{el}]/\eta_D, \qquad (9)$$

where we have assumed that Bob's detector has the same performance as Alice's.

The channel-added noise referred to the channel input is given by

$$\chi_{line} = \frac{1}{T} - 1 + \varepsilon_E, \qquad (10)$$

where ε_E is the excess noise due to Eve's attack. In practice any *untrusted* noise from the QKD system can be included into ε_E. Here, we separate ε_E into two terms,

$$\varepsilon_E = \varepsilon_A + \varepsilon_0, \qquad (11)$$

where ε_A is the excess noise due to the passive state preparation scheme as given in (6). ε_0 represents other sources of untrusted noise.

The overall noise referred to the channel input is given by

$$\chi_{tot} = \chi_{line} + \frac{\chi_{het}}{T}. \qquad (12)$$

Since both quadratures can be used to generate the secure key, the mutual information between Alice and Bob can be

determined by

$$I_{AB} = \log_2 \frac{V + \chi_{\text{tot}}}{1 + \chi_{\text{tot}}}, \tag{13}$$

where $V = V_A + 1$.

To estimate χ_{BE}, we adopt the realistic noise model where Eve cannot control the loss inside Bob's system, and the detector noise from Bob is assumed to be trusted [28]. This noise model has been widely used in CV-QKD experiments [28,30–33]. Under this model, the Holevo bound of the information between Eve and Bob is given by Ref. [30],

$$\chi_{BE} = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{14}$$

where $G(x) = (x + 1)\log_2(x + 1) - x\log_2 x$.

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}], \tag{15}$$

where

$$A = V^2(1 - 2T) + 2T + T^2(V + \chi_{\text{line}})^2, \tag{16}$$

$$B = T^2(V\chi_{\text{line}} + 1)^2, \tag{17}$$

$$\lambda_{3,4}^2 = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}], \tag{18}$$

where

$$C = \frac{1}{(T(V + \chi_{\text{tot}}))^2}[A\chi_{\text{het}}^2 + B + 1 + 2\chi_{\text{het}},$$
$$\times(V\sqrt{B} + T(V + \chi_{\text{line}})) + 2T(V^2 - 1)], \tag{19}$$

$$D = \left(\frac{V + \sqrt{B}\chi_{\text{het}}}{T(V + \chi_{\text{tot}})}\right)^2, \tag{20}$$

$$\lambda_5 = 1. \tag{21}$$

Simulation parameters are summarized as follows: $\gamma = 0.2$ dB/km, $\varepsilon_0 = 0.01$, $\upsilon_{el} = 0.1$, $\eta_D = 0.5$, and $f = 0.95$. The modulation variance V_A is numerically optimized at different fiber lengths.

In Fig. 2 we present the relations of the secure key rate and the fiber length for three different average photon numbers n_0. As shown in Fig. 2, a thermal source with an average output photon number above 100 can be employed to implement the passive CV QKD scheme efficiently.

IV. ASE SOURCE CHARACTERIZATION

Previous studies have shown that the ASE noise generated by a fiber amplifier is thermal [43,44]. In [45], we conducted conjugate homodyne detection and verified the photon statistics of a single-mode component (selected by the LO) of an ASE source follows a Bose-Einstein distribution, as expected from a single-mode thermal state. Nevertheless, the average photon number of the thermal state in the previous experiment [45] is relatively low (about 15). Here, we use a similar setup to characterize the output of a commercial ASE source operated at higher output power.

The experimental setup is shown in Fig. 3. A fiber amplifier (PriTel) with vacuum state input is employed as a broadband
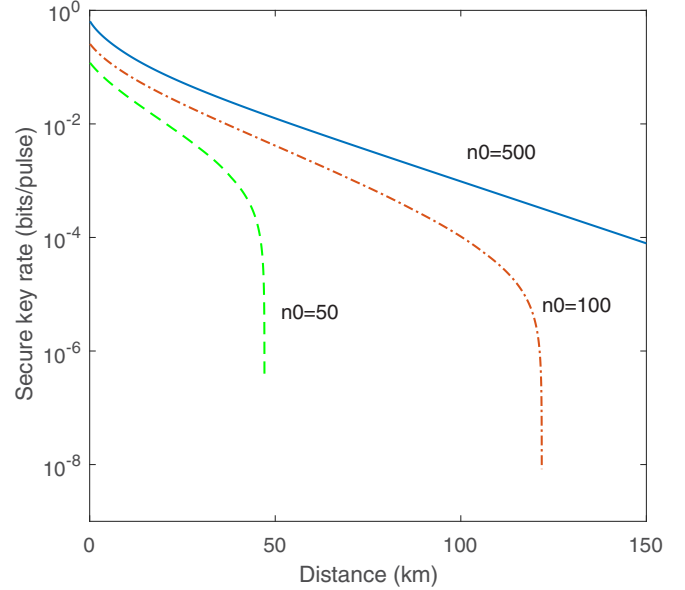

FIG. 2. Simulation results of the secure key rate for three different average photon numbers of the thermal state: $n_0 = 50, 100, 500$. Other simulation parameters are as follows: $\gamma = 0.2$ dB/km; $\varepsilon_0 = 0.01$; $\upsilon_{el} = 0.1$; $\eta_D = 0.5$; $f = 0.95$.

thermal source. A 0.8-nm optical bandpass filter centered at 1542 nm is placed after the ASE source (BP in Fig. 3) to reduce the power of unused light. To select out a single polarization mode, a fiber pigtailed polarizer is employed (Pol in Fig. 3). A continuous-wave (CW) laser source with a central wavelength of 1542 nm (Clarity-NLL-1542-HP from Wavelength Reference) is employed as the LO in coherent detection. Note it is not necessary to stabilize the laser wavelength, which can never drift out the above 0.8-nm range under normal operation. A variable optical attenuator (VOA in Fig. 3) is used to adjust the LO power, and a fiber polarization controller (PC in Fig. 3) is used to match the polarization of the LO with that of the thermal source. To perform conjugate optical homodyne detection, we use a commercial 90° optical hybrid (Optoplex) and two balanced amplified photodetectors (Thorlabs). The outputs of the two balanced photodetectors are sampled by a real time oscilloscope.

The noise of the two balanced detectors have been determined to be 0.37 and 0.35 in the shot-noise unit. The overall detection efficiency (taking into account the loss of the 90° optical hybrid and the quantum efficiency of the photodiode) is about 0.5. Figure 4 shows the distributions of the measurement
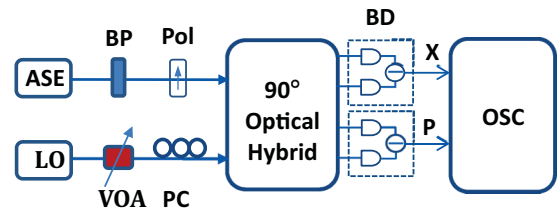

FIG. 3. Experimental setup. ASE, broadband thermal source; LO, narrow-band laser source; BP, optical band pass filter; Pol, fiber polarizer; VOA, variable optical attenuator; PC, polarization controller; BD, balanced photodetector; OSC, oscilloscope.
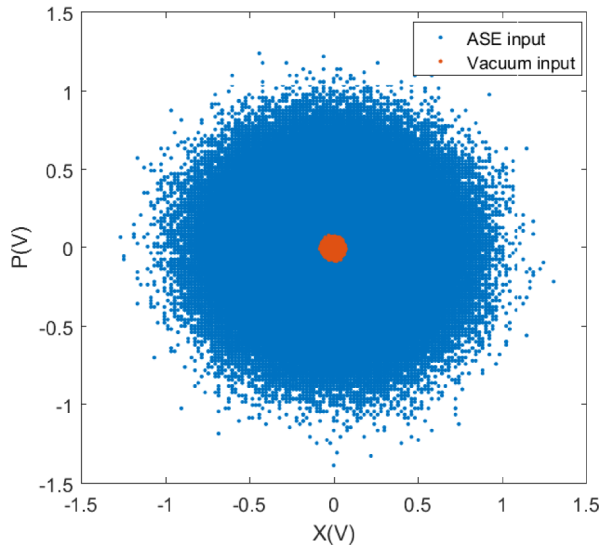
FIG. 4. Experimental results shown in phase space. The measurement results with both a vacuum input and a thermal state input are presented.

results with either a vacuum input or a thermal input. By normalizing the quadrature variances of the thermal state to the vacuum noise, the average photon number (per mode) of the thermal state has been determined to be about 800. As discussed in Sec. II, such a thermal source is bright enough to implement the passive CV-QKD scheme. Figure 5 shows the two-dimensional histogram of the measured data when the input is a thermal state. The small deviation from a perfect two-dimensional Gaussian distribution is most likely due to the nonuniform bin size of the 8-bit analog-to-digital converter of the oscilloscope.

The single-time second-order correlation function $g^{(2)}(0)$ is an important parameter to characterize a photon source [46]. In [45], we have shown that $g^{(2)}(0)$ can be conveniently calculated from the statistics of the conjugate homodyne measurement using

$$g^{(2)}(0) = \frac{\langle Z^2 \rangle - 4 \langle Z \rangle + 2}{(\langle Z \rangle - 1)^2}, \qquad (22)$$
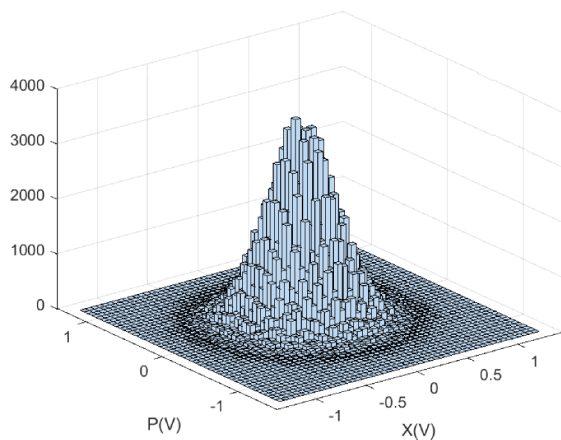
where $Z = X^2 + P^2$.

FIG. 5. The histogram of the experimental results with a thermal state input.

From the experimental data, the $g^{(2)}(0)$ of the ASE source has been determined to be 2.012, which is reasonably close to the theoretical value of 2 for a perfect thermal source.

V. DISCUSSION

Quantum state preparation is a crucial step in QKD. In the GMCS QKD, this step is implemented using a random number generator, a weak coherent source, and high performance optical modulators. In this paper, we propose a passive state preparation scheme where Alice and Bob generate shared randomness by measuring correlated thermal states split from a common thermal source. This scheme may significantly simplify the implementation of CV-QKD and make it more practical. Note this scheme is different from the entanglement-based QKD where each of Alice and Bob measures a subsystem of an entangled state. In the former, the trustworthiness of the source is required, while in the latter, the entanglement source may be controlled by Eve without compromising the security.

A few more words about imperfections at Alice's side. There are two types of imperfections to be addressed. One is associated with the thermal source itself, and the other is associated with Alice's detector.

To deal with the imperfection of the thermal source itself, precise quantum state tomography can be performed to quantify the deviation of the output of the source from a perfect thermal state. This is especially important when a multimode thermal source is employed. We need to make sure there is no correlation between quadrature values of different modes. Otherwise, Eve may gain information without introducing noise by measuring modes not detected by Alice and Bob. Once the imperfection of the source has been quantified, it should be taken into account in the secure proof and key rate calculation. The output of a practical light source may drift with time, which implies that the above state tomography process may need to be repeated time by time. Of course, in the conventional active state preparation scheme, both the laser source and the modulators need to be calibrated over time for similar reasons. It seems reasonable to believe that a thermal source operated in CW mode will show better stability than optical modulators operated at high speed. How to deal with the source imperfections in CV-QKD has drawn much attention [36,38,47–50]. We leave this as a future research topic.

To deal with the imperfections of Alice's detector, in this paper we have made a conservative assumption that Alice's detector noise is untrusted and thus the corresponding excess noise is attributed to Eve's attack. In practice Eve cannot access Alice's system, so one could assume that the above noise is trusted, just like the noise from Bob's detector. Under reverse reconciliation, the trusted noise from Alice's detector will reduce the mutual information I_{AB} but will not change Eve's information χ_{BE}. This trusted noise model can tolerate higher detector noise and work with a lower photon number of the source. We remark that to justify the trusted noise model in practice, a specially designed monitoring system may be required to prevent Eve from manipulating the detector performance.

Note in our scheme, the randomness is generated from a thermal source. Can we trust this randomness? As has been discussed in [51], while quantum randomness is ultimately

connected to quantum superposition states, in the trusted device scenario, the state received by the detector does not need to be a pure state. For example, trusted randomness can be generated by measuring only one photon from an entangled photon pair, given Eve cannot access the other photon. In our scheme, photons from the thermal source are generated through spontaneous emission processes and are entangled with the atoms inside the source. Given the source itself is protected from Eve, true randomness can be generated.

While our theoretical discussions are based on a single-mode thermal state, in practice, the proposed scheme can be implemented using a broadband source operated in CW mode (a multimode source), thanks to the mode-selective feature of coherent detection. Since the randomness carried by different modes of the source are independent of each other, to generate shared randomness it is crucial that Alice's and Bob's detectors measure the same mode of the source. Furthermore, Alice and Bob need a scheme to establish a phase reference between their homodyne detection. Two schemes have been developed in CV QKD based on active state preparation, and both of them can be adopted in the passive state preparation protocol. In the first scheme, Alice generates two strong LOs from the same laser, uses one of them in her local measurement, and sends the second one to Bob to be used as a LO in his measurement. In the second scheme [52,53], both Alice and Bob generate LOs from their own local lasers. The phase relation between their measurement bases can be determined by sending relatively weak phase reference pulses from Alice to Bob.

Note added in proof. Recently, we noticed a related work by Newton *et al.* [54].

[1] C. H. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (IEEE Press, New York, 1984), pp. 175–179.

[2] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).

[3] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[4] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[5] H.-K. Lo, M. Curty, and K. Tamaki, Nat. Photon. **8**, 595 (2014).

[6] E. Diamanti, H.-K. Lo, B. Qi, and Z. Yuan, npj Quantum Info. **2**, 16025 (2016).

[7] X. Ma, X. Yuan, Z. Cao, B. Qi, and Z. Zhang, npj Quantum Info. **2**, 16021 (2016).

[8] M. Herrero-Collantes and J. C. Garcia-Escartin, Rev. Mod. Phys. **89**, 015004 (2017).

[9] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[10] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[11] X.-B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[12] Y. Zhao, B. Qi, and H.-K. Lo, Appl. Phys. Lett. **90**, 044106 (2007).

[13] W. Mauerer and C. Silberhorn, Phys. Rev. A **75**, 050305(R) (2007).

[14] Y. Adachi, T. Yamamoto, M. Koashi, and N. Imoto, Phys. Rev. Lett. **99**, 180503 (2007).

[15] X. F. Ma and H. K. Lo, New J. Phys. **10**, 073018 (2008).

[16] M. Curty, T. Moroder, X. F. Ma, and N. Lütkenhaus, Opt. Lett. **34**, 3238 (2009).

[17] M. Curty, X. F. Ma, B. Qi, and T. Moroder, Phys. Rev. A **81**, 022310 (2010).

[18] M. Curty, X. F. Ma, H. K. Lo, and N. Lütkenhaus, Phys. Rev. A **82**, 052325 (2010).

[19] Y. Zhang, W. Chen, S. Wang, Z.-Q. Yin, F.-X. Xu, X.-W. Wu, C.-H. Dong, H.-W. Li, G.-C. Guo, and Z.-F. Han, Opt. Lett. **35**, 3393 (2010).

[20] Y. Zhang, S. Wang, Z.-Q. Yin, W. Chen, W.-Y. Liang, H.-W. Li, G.-C. Guo, and Z.-F. Han, Chin. Phys. B **21**, 100307 (2012).

[21] Q.-C. Sun, W.-L. Wang, Y. Liu, F. Zhou, J. S. Pelc, M. M. Fejer, C.-Z. Peng, X.-F. Chen, X.-F. Ma, Q. Zhang, and J.-W. Pan, Laser Phys. Lett. **11**, 085202 (2014).

[22] Y. Li, W. S. Bao, H. W. Li, C. Zhou, and Y. Wang, Phys. Rev. A **89**, 032329 (2014).

[23] C. Zhou, W.-S. Bao, H.-W. Li, Y. Wang, Y. Li, Z.-Q. Yin, W. Chen, and Z.-F. Han, Phys. Rev. A **89**, 052328 (2014).

[24] M. Curty, M. Jofre, V. Pruneri, and M. W. Mitchell, Entropy **17**, 4064 (2015).

[25] S.-H. Sun, G.-Z. Tang, C.-Y. Li, and L.-M. Liang, Phys. Rev. A **94**, 032324 (2016).

[26] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999).

[27] M. Hillery, Phys. Rev. A **61**, 022309 (2000).

[28] F. Grosshans, G. V. Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[29] E. Diamanti and A. Leverrier, Entropy **17**, 6072 (2015).

[30] 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).

[31] B. Qi, L.-L. Huang, L. Qian, and H.-K. Lo, Phys. Rev. A **76**, 052323 (2007).

[32] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, Nat. Photon. **7**, 378 (2013).

[33] R. Kumar, H. Qin, and R. Alléaume, New J. Phys. **17**, 043027 (2015).

[34] D. Huang, P. Huang, D. Lin, and G. Zeng, Sci. Rep. **6**, 19201 (2016).

[35] Y.-C. Zhang *et al.*, arXiv:1709.04618.

[36] P. Jouguet, S. Kunz-Jacques, E. Diamanti, and A. Leverrier, Phys. Rev. A **86**, 032309 (2012).

[37] R. Filip, Phys. Rev. A **77**, 022310 (2008).

[38] V. C. Usenko and R. Filip, Phys. Rev. A **81**, 022318 (2010).

[39] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).

[40] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).

[41] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Info. Comput. **3**, 535 (2003).

[42] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle Brouri, and P. Grangier, J. Phys. B **42**, 114014 (2009).

[43] W. S. Wong, H. A. Haus, L. A. Jiang, P. B. Hansen, and M. Margalit, Opt. Lett. **23**, 1832 (1998).

[44] P. Voss, M. Vasilyev, D. Levandovsky, T.-G. Noh, and P. Kumar, IEEE Photon. Technol. Lett. **12**, 1340 (2000).

[45] B. Qi, P. Lougovski, and B. P. Williams, arXiv:1702.02558.

[46] R. J. Glauber, Phys. Rev. **130**, 2529 (1963).

[47] Y. Shen, X. Peng, J. Yang, and H. Guo, Phys. Rev. A **83**, 052304 (2011).

[48] J. Yang, B. Xu, and H. Guo, Phys. Rev. A **86**, 042314 (2012).

[49] V. C. Usenko and R. Filip, Entropy **18**, 20 (2016).

[50] I. Derkach, V. C. Usenko, and R. Filip, Phys. Rev. A **96**, 062309 (2017).

[51] B. Qi, Rev. Sci. Instrum. **88**, 113101 (2017).

[52] B. Qi, P. Lougovski, R. Pooser, W. Grice, and M. Bobrek, Phys. Rev. X **5**, 041009 (2015).

[53] D. B. S. Soh, C. Brif, P. J. Coles, N. Lütkenhaus, R. M. Camacho, J. Urayama, and M. Sarovar, Phys. Rev. X **5**, 041010 (2015).

[54] E. Newton, A. Ghesquière, F. L. Wilson, B. T. H. Varcoe, and M. Moseley, arXiv:1711.06592.

[55] http://www.energy.gov/downloads/doe-public-access-plan.