

Continuous-variable quantum key distribution based on continuous random basis choice

Weiqi Liu(刘维琪), Jinye Peng(彭进业), Peng Huang(黄鹏), Shiyu Wang(汪诗寓), Tao Wang(王涛), Guihua Zeng(曾贵华)
Citation: Chin. Phys. B . 2018, 27(7): 070305. **doi:** 10.1088/1674-1056/27/7/070305

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Practical security of continuous-variable quantum key distribution under finite-dimensional effect of multi-dimensional reconciliation

Yingming Zhou(周颖明), Xue-Qin Jiang(蒋学芹), Weiqi Liu(刘维琪), Tao Wang(王涛), Peng Huang(黄鹏), Guihua Zeng(曾贵华)
Chin. Phys. B . 2018, 27(5): 050301. **doi:** 10.1088/1674-1056/27/5/050301

Entangled-photons generation with quantum dots

Yuan Li(李远), Fei Ding(丁飞), Oliver G Schmidt
Chin. Phys. B . 2018, 27(2): 020307. **doi:** 10.1088/1674-1056/27/2/020307

Quantum light storage in rare-earth-ion-doped solids

Yi-Lin Hua(华怡林), Zong-Quan Zhou(周宗权), Chuan-Feng Li(李传锋), Guang-Can Guo(郭光灿)
Chin. Phys. B . 2018, 27(2): 020303. **doi:** 10.1088/1674-1056/27/2/020303

Cancelable remote quantum fingerprint templates protection scheme

Qin Liao(廖骏), Ying Guo(郭迎), Duan Huang(黄端)
Chin. Phys. B . 2017, 26(9): 090302. **doi:** 10.1088/1674-1056/26/9/090302

Spherical reconciliation for a continuous-variable quantum key distribution

Zhao Lu(卢钊), Jian-Hong Shi(史建红), Feng-Guang Li(李风光)
Chin. Phys. B . 2017, 26(4): 040304. **doi:** 10.1088/1674-1056/26/4/040304

Continuous-variable quantum key distribution based on continuous random basis choice*

Weiqi Liu(刘维琪)[1], Jinye Peng(彭进业)[1], Peng Huang(黄鹏)[2,†], Shiyu Wang(汪诗寓)[2], Tao Wang(王涛)[2], and Guihua Zeng(曾贵华)[1,2,‡]

[1] College of Information Science and Technology, Northwest University, Xi'an 710127, China

[2] State Key Laboratory of Advanced Optical Communication Systems and Networks, Shanghai Key Laboratory on Navigation and Location-based Service, and Center of Quantum Information Sensing and Processing (QSIP), Shanghai Jiao Tong University, Shanghai 200240, China

(Received 12 March 2018; revised manuscript received 8 April 2018; published online 25 June 2018)

Gaussian-modulated coherent state quantum key distribution is gradually moving towards practical application. Generally, the involved scheme is based on the binary random basis choice. To improve the performance and security, we present a scheme based on a continuous random basis choice. The results show that our scheme obviously improves the performance, such as the secure communication distance. Our scheme avoids comparing the measurement basis and discarding the key bits, and it can be easily implemented with current technology. Moreover, the imperfection of the basis choice can be well removed by the known phase compensation algorithm.

Keywords: continuous-variable quantum key distribution, basis choice

PACS: 03.67.Hk, 03.67.Dd, 03.67.–a **DOI:** 10.1088/1674-1056/27/7/070305

1. Introduction

Quantum key distribution (QKD) is an application of quantum information sciences, enabling two partners (Alice and Bob) to share a secret key, which in turn allows them to communicate securely. The security is guaranteed by Heisenberg's uncertainty principle and the no-clone theory. Since almost ten years ago, lots of interest has arisen in continuous-variable quantum key distribution (CVQKD), which provides various CVQKD protocols.[1–6] One of the most favorable protocols is the Gaussian-modulated coherent state (GMCS) protocol.[7–9] In this protocol, Alice performs Gaussian modulation to encode the key information, by modulating the quadratures X and P (using the amplitude and the phase modulators) of few-photon coherent states with a centered Gaussian distribution. These states are then sent along with a phase reference through the quantum channel to Bob, who randomly measures one of the two quadratures (X or P) using a homodyne detector, or both quadratures simultaneously with a heterodyne detector. So far, several experimental implementations have been carried out by several groups. Meanwhile, the unconditional security of the GMCS QKD against general collective and coherent eavesdropping attacks has been fully proved in some references.[10–14]

Generally, the GMCS QKD protocol with homodyne detector requires a binary random basis choice, i.e., 0 or $\pi/2$, which makes Alice and Bob have to discard half of their data. Moreover, the devices and applications used in the practical system may be imperfect, which will incur loopholes to Eve in practical application. This points to the practical security which has been investigated widely, such as the laser source,[15–17] the beam splitter (BS),[18–21] the local oscillator,[22,23] the detector,[21,24] and the software or hardware for the phase compensation[25,26] and the basis choice. For the binary random basis choice, Bob randomly modulates 0 or $\pi/2$ on the phase modulator (PM) to measure either quadrature of the received quantum state. Maybe we can propose another alternative figuration of CVQKD system, so that the performance and practical security of the system may be improved.

In this paper, we present a GMCS QKD scheme based on the continuous random basis choice, in which Bob randomly measures the received states depending on the continuous random phase, then Alice reshapes her data. The security of this scheme is guaranteed by the no-cloning theorem and the uncertainty principle. To testify the performance and security of the scheme, we calculate the secret key rate under collective attacks when using reverse reconciliation and investigate the practical security under realistic quantum channel and detector. The simulation results show that the continuous random basis choice does improve the performance, such as the secure communication distance, and the imperfect basis choice can be well removed by the perfect phase compensation algorithm. Moreover, this scheme avoids comparing the measurement basis and discarding the key bits, and it can be implemented with current technology easily.

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61332019, 61671287, and 61631014), Northwest University Doctorate Dissertation of Excellence Funds, China (Grant No. YYB17022), and the National Key Research and Development Program, China (Grant No. 2016YFA0302600).

†Corresponding author. E-mail: huang.peng@sjtu.edu.cn

‡Corresponding author. E-mail: ghzeng@sjtu.edu.cn

© 2018 Chinese Physical Society and IOP Publishing Ltd

The paper is organized as follows. In Section 2, we introduce the GMCS QKD scheme based on the continuous random basis choice. In Section 3, the secret key rate of the scheme under collective attacks is calculated. In Section 4, we analyze the practical security induced by the imperfect basis choice. Conclusions are drawn in Section 5.

2. Scheme description

In the prepare-and-measurement (P&M) model of a standard GMCS QKD scheme, Alice randomly prepares an encoded quantum state and sends it to Bob for detection. Alice and Bob broadcast their measurement bases via an authenticated channel. They discard all polarization data sent and received in different bases and use the remaining data to generate a sifted key. Here we substitute the continuous random basis choice in our scheme, which avoids comparing the measurement basis and discarding the key data. The P&M model of our scheme is shown in Fig. 1. In detail, the quantum transmission procedure is described as follows.

(I) Alice generates two Gaussian random numbers $X_{\rm A}$ and $P_{\rm A}$ with mean values 0 and variances $V_{\rm A}$. Meanwhile, Bob generates a random bit b.

(II) Alice prepares the quantum coherent state. The initial quantum coherent state with shot noise $(\delta X_{\rm A}, \delta P_{\rm A})$ is modulated by the amplitude and the phase modulator to obtain the coherent state centered at $(X_{\rm A}, P_{\rm A})$. Then Alice sends the prepared states to Bob through the quantum channel, which features a transmission efficiency T and an excess noise ε. The total channel added noise referred to the channel input, expressed in shot noise units, is defined as $\chi_{\rm line} = 1/T - 1 + \varepsilon$.

(III) When Bob receives the modulated coherent state, he randomly measures the quadratures by a detector depending on the continuous random phase θ (from 0 to 2π). The continuous random basis choice is implemented by PM at Bob's side, which is based in the random bit b. The detection-added noise referred to Bob's input is defined and expressed in shot-noise units as $\chi_{\rm hom} = (1 - \eta + V_{\rm el})/\eta$, where η denotes the efficiency of the detector and $V_{\rm el}$ is the detector's electronic noise. The total noise referred to the channel input can then be expressed as $\chi_{\rm tot} = \chi_{\rm line} + \chi_{\rm hom}/T$.

(IV) Bob informs Alice the phases θ that he selects in each time and keeps his measurement outcomes $m_{\rm B} = X_{\rm A}\cos\theta + P_{\rm A}\sin\theta$. Then Alice reshapes her data depending on θ.

(V) Finally, Alice and Bob apply reconciliation and privacy amplification algorithms to extract a private binary key string from the shared information. The reconciliation is direct when Alice's data are used as a reference for establishing the key and reverse when the reference is Bob's data.

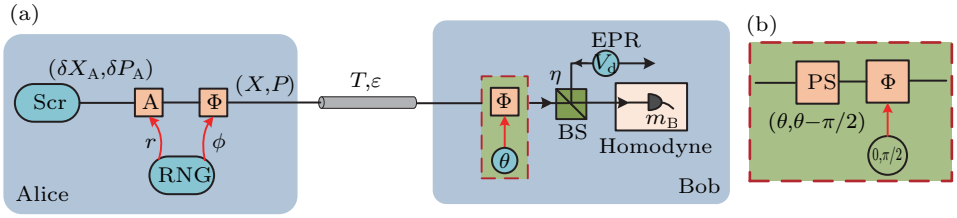


Fig. 1. (color online) The P&M model of the GMCS QKD scheme based on the continuous random basis choice. (a) The schematic model. A represents the amplitude modulator (AM), Φ represents the phase modulator, and RNG represents the random numbers generator. (b) The modulation module at Bob's side, which can be equivalent to the dotted box in (a). θ can be equal to the binary random basis choice 0 or $\pi/2$ with the phase shifts θ or $\theta - \pi/2$. PS means the phase shifts.

Actually, this scheme can be seen just as one specific case of the well-known GMCS model with special known phase shifts θ or $\theta - \pi/2$, as shown in Fig. 1(b). That is, the security against collective and coherent eavesdropping attacks will be the same as that of the general GMCS QKD protocol. The proposed scheme has several distinct features. We can implement this scheme with current technology easily and the scheme avoids comparing the measurement basis and discarding the key bits. The reconstruction of Alice's data may be implemented in the data post-processing procedure, which will reduce the complexity of the system. Specially, the proposed scheme does increase the performance of the CVQKD system and it is secure even when we apply the same angle θ to hundreds of frames. In the intercept-resend attack, Eve makes a heterodyne measurement ($X_{\rm A}$ and $P_{\rm A}$) of each incoming quantum state sent by Alice through the quantum channel, then prepares a coherent state according to her measurement results and sends it to Bob.[27] However, the uncertainty principle prevents her from doing so. The eavesdropper cannot accurately measure the $X_{\rm A}$ and $P_{\rm A}$ at the same time, so will not exactly know the sent quantum states and successfully attacks the system though the θ is published. In the proposed scheme, when Eve wants to intercept and measure the pulses sent by Alice, because the angle for the basis choice is from 0 to 2π, she cannot guess the angle correctly. Eve must simultaneously measure the quadratures, then she will inevitably induce at least two shot-noise units of excess noise[27] and obtain little information. It should be mentioned that it is insecure when we apply the same angle to hundreds of frames in the GMCS QKD protocol based on the binary random basis

choice. Because there are only two possibilities of angle for the basis choice, Eve can intercept the pulses sent by Alice and accurately measure the quadrature X_A (or P_A) by the homodyne detector. She can control the interception proportions to further decrease the excess noise to a normal level without being detected and then obtains the information sent by Alice.

3. Performance analysis

In the following, we derive the expression of the secret key rate of the proposed scheme for the case of collective attacks. It is well known that the P&M scheme is formally equivalent to the corresponding entanglement-based (E-B) scheme.[8] In the E-B scheme, the coherent state preparation is modeled by a heterodyne measurement of one half of a two-mode squeezed vacuum (EPR) state of variance $V = V_A + 1$. The other half of the EPR state is sent to Bob through the quantum channel. Bob's detector inefficiency is modeled by a BS with transmission η, while its electronic noise V_{el} is modeled by an EPR state of variance V_d, one half of which is entering the second input port of the BS, as shown in Fig. 2. The variance for the homodyne detector is $V_d = 1 + V_{el}/(1-\eta)$.[28] Finally, Alice and Bob proceed with classical data processing procedures, which include a reconciliation algorithm. Reverse reconciliation has been shown to offer a great advantage in the QKD system, therefore calculations in this paper have been performed for this case.

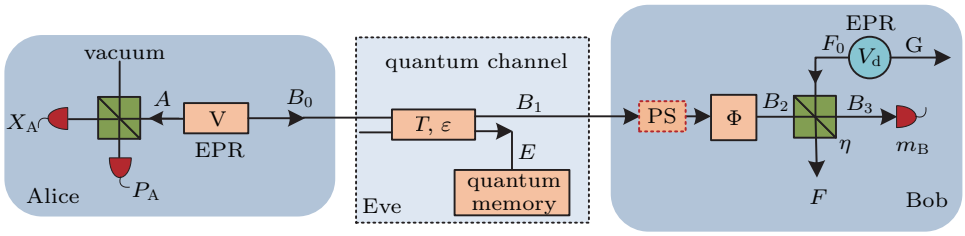


Fig. 2. (color online) The E–B model of the GMCS QKD based on the continuous random basis choice.

In the case of collective attacks, Eve interacts individually with each pulse but is allowed to wait for the entire classical procedure to end before performing the best possible collective measurement on her ensemble of stored ancillae. The maximum information of Bob's key available to Eve is limited by the Holevo bound

$$\chi_{BE} = S(\rho_E) - \int \mathrm{d}m_B p(m_B) S(\rho_E^{m_B}), \tag{1}$$

where m_B represents the measurement of Bob, $p(m_B)$ is the probability density of the measurement, $\rho_E^{m_B}$ is the eavesdropper's state conditional on Bob's measurement result, and S is the Von Neumann entropy of the quantum state. Due to the fact that Eve can purify the system AB_1, and that Bob's measurement purifies the system AEFG (see Fig. 2), χ_{BE} becomes

$$\chi_{BE} = S(\rho_{AB_1}) - S(\rho_{AFG}^{m_B}). \tag{2}$$

For collective attacks, the Gaussian attacks are optimal. Thus it is enough to consider the Gaussian states and for one n-mode Gaussian state, the entropy can be expressed as

$$S(\rho) = \sum_i G\left(\frac{\lambda_i - 1}{2}\right), \tag{3}$$

where λ_i are the symplectic eigenvalues of the corresponding covariance matrix γ characterizing the state, and $G(x) = (x+1)\log_2(x+1) - x\log_2 x$.

Therefore, the covariance matrix γ_{AB_1}, which depends on the system including Alice and the quantum channel, can be written as

$$\gamma_{AB_1} = \begin{bmatrix} V \cdot \mathbf{1}_2 & \sqrt{T(V^2-1)} \cdot \sigma_z \\ \sqrt{T(V^2-1)} \cdot \sigma_z & T(V + \chi_{\text{line}}) \cdot \mathbf{1}_2 \end{bmatrix}, \tag{4}$$

where the matrices $\mathbf{1}_2 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$, and $\sigma_z = \left[\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right]$. Then we need to calculate the symplectic eigenvalues of the covariance matrix $\gamma_{AFG}^{m_B}$, which can be written as

$$\gamma_{AFG}^{m_B} = \gamma_{AFG} - \boldsymbol{\sigma}_{AFG;B_3}^{\mathrm{T}} \boldsymbol{H} \boldsymbol{\sigma}_{AFG;B_3}. \tag{5}$$

In the above equation, $H = [\boldsymbol{X}(\theta)\gamma_{B_3}\boldsymbol{X}(\theta)]^{\mathrm{MP}}$, where MP stands for the Moore–Penrose pseudo-inverse of a matrix and we have[29,30]

$$\boldsymbol{X} = \begin{bmatrix} \cos\theta & 0 \\ 0 & \sin\theta \end{bmatrix}. \tag{6}$$

The matrices γ_{B_3}, γ_{AFG}, and $\boldsymbol{\sigma}_{AFG;B_3}$ can be derived from the following covariance matrix:

$$\gamma_{AFG;B_3} = \begin{bmatrix} \gamma_{AFG} & \boldsymbol{\sigma}_{AFG;B_3}^{\mathrm{T}} \\ \boldsymbol{\sigma}_{AFG;B_3} & \gamma_{B_3} \end{bmatrix}, \tag{7}$$

where $\gamma_{AFG;B_3} = (\boldsymbol{Y}^{\mathrm{BS}})^{\mathrm{T}}[\gamma_{AB_1} \oplus \gamma_{F_0G}]\boldsymbol{Y}^{\mathrm{BS}}$, here γ_{F_0G} is written as

$$\gamma_{F_0G} = \begin{bmatrix} V_d \cdot \mathbf{1}_2 & \sqrt{(V_d^2-1)} \cdot \sigma_z \\ \sqrt{(V_d^2-1)} \cdot \sigma_z & V_d \cdot \mathbf{1}_2 \end{bmatrix}, \tag{8}$$

and $\boldsymbol{Y}^{\mathrm{BS}}$ is calculated as

$$\boldsymbol{Y}^{\mathrm{BS}} = \begin{bmatrix} \mathbf{1}_2 & 0 & 0 & 0 \\ 0 & \sqrt{\eta} \cdot \mathbf{1}_2 & \sqrt{1-\eta} \cdot \mathbf{1}_2 & 0 \\ 0 & -\sqrt{1-\eta} \cdot \mathbf{1}_2 & \sqrt{\eta} \cdot \mathbf{1}_2 & 0 \\ 0 & 0 & 0 & \mathbf{1}_2 \end{bmatrix}. \tag{9}$$

Finally, the above matrices are calculated as

$$\gamma_{B_3} = \begin{bmatrix} \eta T(V+\chi_{\text{line}})+V_{\text{d}}(1-\eta) & 0 \\ 0 & \eta T(V+\chi_{\text{line}})+V_{\text{d}}(1-\eta) \end{bmatrix}, \tag{10}$$

$$\boldsymbol{\sigma}^{\text{T}}_{AFG;B_3} = \begin{bmatrix} \sqrt{\eta T(V^2-1)} & 0 \\ 0 & -\sqrt{\eta T(V^2-1)} \\ A & 0 \\ 0 & A \\ -\sqrt{(1-\eta)(V_{\text{d}}^2-1)} & 0 \\ 0 & \sqrt{(1-\eta)(V_{\text{d}}^2-1)} \end{bmatrix}, \tag{11}$$

$$\gamma_{AFG} = \begin{bmatrix} V & 0 & B & 0 & 0 & 0 \\ 0 & V & 0 & -B & \sqrt{(V_{\text{d}}^2-1)\eta} & 0 \\ B & 0 & C & 0 & 0 & -\sqrt{(V_{\text{d}}^2-1)\eta} \\ 0 & -B & 0 & C & V_{\text{d}} & 0 \\ 0 & \sqrt{(V_{\text{d}}^2-1)\eta} & 0 & 0 & 0 & V_{\text{d}} \\ 0 & 0 & -\sqrt{(V_{\text{d}}^2-1)\eta} & 0 & 0 & 0 \end{bmatrix}, \tag{12}$$

with

$$A = \sqrt{\eta(1-\eta)}(V+\chi_{\text{line}})T - V_{\text{d}}\sqrt{\eta(1-\eta)}, \quad B = \sqrt{T(V^2-1)(1-\eta)}, \quad C = (1-\eta)(V+\chi_{\text{line}})T + V_{\text{d}}.$$

Here we assume that the distribution of θ is symmetric and uniform, and define $k = E[\cos^2\theta]$, where $E[X]$ denotes the expectation of the random variable X. The parameter k is related to the chosen distribution of the continuous random phase. Because θ can be any angle from 0 to 2π and γ_{B_3} is not associated with θ, finally the matrix $\boldsymbol{X}\gamma_{B_3}\boldsymbol{X}$ is given as

$$\boldsymbol{X}\gamma_{B_3}\boldsymbol{X} = \begin{bmatrix} [\eta T(V+\chi_{\text{line}})+V_{\text{d}}(1-\eta)]k & 0 \\ 0 & [\eta T(V+\chi_{\text{line}})+V_{\text{d}}(1-\eta)](1-k) \end{bmatrix}. \tag{13}$$

We now have all the elements required to proceed to the calculation of the symplectic eigenvalues. In addition, the mutual information of Alice and Bob, I_{AB}, is derived from Bob's measured variance V_{B} and the conditional variance $V_{\text{B|A}}$,

$$I_{\text{AB}} = \frac{1}{2}\log_2\frac{V_{\text{B}}}{V_{\text{B|A}}} = \frac{1}{2}\log_2\frac{V+\chi_{\text{tot}}}{1+\chi_{\text{tot}}}. \tag{14}$$

Given the parameters V_{A}, T, ε, V_{el}, β, and η, Alice and Bob can obtain the shared information, as well as the maximal bound on the information available to Eve. Finally, they will derive the secret key rate of the proposed scheme based on $R = \beta I_{\text{AB}} - \chi_{\text{BE}}$, where β is the efficiency of the reverse reconciliation. The secret key rate of the proposed scheme against the collective attacks is plotted in Fig. 3. As a comparison, we also plot the secret key rate of the conventional GMCS QKD system with the same parameters. The results show that the use of the continuous random basis choice does improve the performance of the system, such as the secure communication distance. Moreover, we study the secret key rate of the proposed scheme under different expectations of the uniform distribution and find that the performance is obviously different when we choose the different expectations of the distribution of the continuous random phase. Meanwhile, the performance of the proposed scheme is best when the expectation $k = 0.5$.

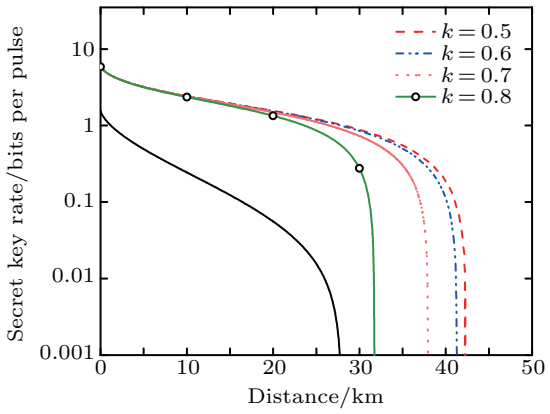


Fig. 3. (color online) The secret key rate of the scheme against the collective attacks. The curve at the left-most position represents the secret key rate of the GMCS QKD based on the binary random basis choice. Then from left to right, the curves represent the secret key rates of our proposed scheme with the parameters $k = 0.8$, 0.7, 0.6, and 0.5, respectively. Meanwhile, other parameters of the simulation are $V_{\text{A}} = 30$, $\varepsilon = 0.01$, $\eta = 0.6$, $V_{\text{el}} = 0.01$, and $\beta = 0.9$.

4. Practical security analysis

For any practical CVQKD system, the security includes not only the theoretical security, but also the practical security induced by the devices and applications. In our proposed scheme, the continuous random phase θ is needed for the basis choice. However, because of the imperfections of the digital to analog convertor (DAC) and PM, the real phase values ap-

plied to the system θ' may be not equal to the expected phase values θ, which will increase the excess noise of the system and induce a loophole.

Considering a practical basis choice with the imperfect DAC and PM, the output mode can be denoted as

$$m'_{\mathrm{B}} = X_{\mathrm{A}} \cos\theta' + P_{\mathrm{A}} \sin\theta'. \tag{15}$$

When defining $\delta\theta = |\theta - \theta'|$, this imperfection will be equivalent to adding an extra phase shift operation $U(\delta\theta) = \exp(\mathrm{i}\delta\theta a^{+}a)$ on Bob's signal states. $\delta\theta$ denotes the phase drifting after the imperfect basis choice, which follows a probability of $p(\delta\theta)$. We assume that the distribution $\delta\theta$ is symmetric and $\kappa = (E[\cos\delta\theta])^2$. If Alice and Bob are not aware of the imperfection of the basis choice, the transmission efficiency and the excess noise used in the evaluation of the secret key rate become[25]

$$T^{\kappa} = \kappa T, \tag{16}$$

$$\varepsilon^{\kappa} = [\varepsilon + (1-\kappa)(V-1)]/\kappa. \tag{17}$$

When Eve performs collective attacks, then the secret key rate under the reverse reconciliation is derived as

$$R^{\kappa} = \beta I^{\kappa}_{\mathrm{AB}} - \chi^{\kappa}_{\mathrm{BE}}, \tag{18}$$

where I^{κ}_{AB} is the mutual information between Alice and Bob with the imperfect basis choice procedure, and $\chi^{\kappa}_{\mathrm{BE}}$ is the Holevo bound on the information between Bob and Eve with the imperfection. The total noise and the total channel added noise will be denoted as $\chi^{\kappa}_{\mathrm{tot}} = \chi^{\kappa}_{\mathrm{line}} + \chi^{\kappa}_{\mathrm{hom}}/T^{\kappa}$ and $\chi^{\kappa}_{\mathrm{line}} = 1/T^{\kappa} - 1 + \varepsilon^{\kappa}$, respectively.

The secret key rate R^{κ} is plotted in Fig. 4. The noise of the imperfect basis choice is weighted by the parameter κ, thus we plot the secret key rate with different parameters κ. The results show that the secret key rate is affected by the imperfection, since it affects the mutual information between Alice and Bob, and increases the information eavesdropped by Eve on the final key. Actually, this issue also exists in the GMCS QKD protocol involving the basis choice procedure, but can be well solved by the phase compensation algorithm.[25,31]

In the CVQKD system, the phase shift between the local and signal pulses is inevitable due to the variation of temperature and vibrations in the environment. The phase shift may affect the stability and the final key rate of the system. To overcome this issue, the phase compensation is a necessary procedure in practical applications of the CVQKD system. We introduce some brighter and randomly labeled stabilization pulses that are not used for generating a raw key, which can therefore be used for the calculation of the phase shifts. The stabilization pulses are sent in known phase states and placed at random positions within the weak quantum signals. When Bob receives the data, he firstly extracts the stabilization pulses and calculates the values of the phase shifts. Then Alice reconstructs the quantum data and Bob performs a linear operation on the received data.[31] In order to effectively compensate the phase shifts, the phase variation of the phase shifts should be less than the inaccuracy of the phase compensation algorithm. We test our algorithm in practice, the precision can reach 0.1° for each frame. Considering the angles of each pulse are the same, then 0.1° represents $\kappa \doteq 1$.[25] Meanwhile, according to the above analysis, $\kappa = 0.99$ represents $\delta\theta = 1.8^{\circ}$. Therefore, the precision of our phase compensation algorithm can meet the requirement of eliminating the imperfections of the basis choice. To demonstrate the effect of elimination, we simulate and plot the red marked curve in Fig. 4. The result shows that the red marked curve and the curve with the perfect basis choice are roughly coincident. In other words, the phase compensation algorithm can well solve the imperfections induced by the basis choice.

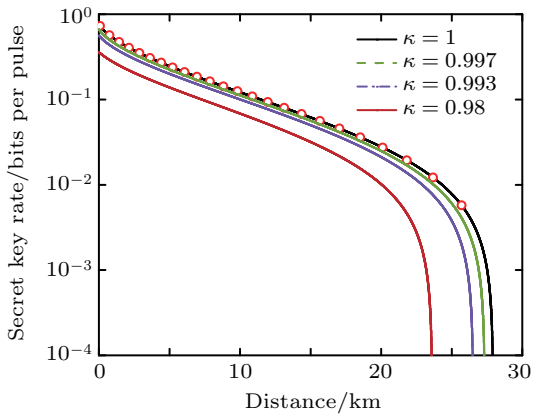


Fig. 4. (color online) The secret key rate as a function of the transmission distance of optical fiber with loss coeffiency 0.2 dB/km for different degrees of imperfection of continuous random basis choice (perfect basis choice corresponds to $\kappa = 1$). The curves without the marked points from right to left represent the secret key rates for $\kappa = 1$, 0.997, 0.993, and 0.98, respectively. The red marked curve represents the result of eliminating the imperfections by our phase compensation algorithm.

5. Conclusion

We have explored the possibility of enabling the GMCS QKD with the continuous random basis choice. The secret key rate of the proposed scheme under collective attacks has been calculated and the result shows that the use of the continuous random basis choice does improve the performance of the system, such as the secure communication distance. Moreover, the devices and applications may be imperfect in the practical system and we investigate the practical security of the scheme with the imperfect basis choice procedure. The results show that this imperfection will decrease the secret key rate and thus incur insecurity of the system. Fortunately, this issue can be well solved by the perfect phase compensation algorithm.

References

[1] Weedbrook C, Pirandola S, García-Patrón R, Cerf N J, Ralph T C, Shapiro J H and Lloyd S 2012 *Rev. Mod. Phys.* **84** 621
[2] Grosshans F and Grangier P 2002 *Phys. Rev. Lett.* **88** 057902
[3] Weedbrook C, Lance A M, Bowen W P, Symul T, Ralph T C and Lam P K 2004 *Phys. Rev. Lett.* **93** 170504
[4] Lance A M, Symul T, Sharma V, Weedbrook C, Ralph T C and Lam P K 2005 *Phys. Rev. Lett.* **95** 180503
[5] Gong L H, Song H C, He C S, Liu Y and Zhou N R 2014 *Physica Scripta* **95** 035101
[6] Song H C, Gong L H and Zhou N R 2012 *Acta Phys. Sin.* **61** 154206 (in Chinese)
[7] Grosshans F, Assche G V, Wenger J, Brouri R, Cerf N J and Grangier P 2003 *Nature* **421** 238
[8] Lodewyck J, Bloch M, García-Patrón R, Fossier S, Karpov E, Diamanti E, Debuisschert T, Cerf N J, Tualle-Brouri R, McLaughlin S W and Grangier P 2007 *Phys. Rev. A* **76** 042305
[9] Qi B, Huang L L, Qian L and Lo H K 2007 *Phys. Rev. A* **76** 052323
[10] García-Patrón R and Cerf N J 2006 *Phys. Rev. Lett.* **97** 190503
[11] Navascués M, Grosshans F and Acín A 2006 *Phys. Rev. Lett.* **97** 190502
[12] Renner R and Cirac J I 2009 *Phys. Rev. Lett.* **102** 110504
[13] Furrer F, Franz T, Berta M, Leverrier A, Scholz V B, Tomamichel M and Werner R F 2012 *Phys. Rev. Lett.* **109** 100502
[14] Leverrier A 2017 *Phys. Rev. Lett.* **118** 200501
[15] Gisin N, Fasel S, Kraus B, Zbinden H and Ribordy G 2006 *Phys. Rev. A* **73** 022320
[16] Jain N, Stiller B, Khan I, Makarov V, Marquardt C and Leuchs G 2014 *IEEE Journal of Selected Topics in Quantum Electronics* **21** 3
[17] Jain N, Anisimova E, Khan I, Makarov V, Marquardt C and Leuchs G 2014 *New J. Phys.* **16** 123030
[18] Huang J Z, Weedbrook C, Yin Z Q, Wang S, Li H W, Chen W, Guo G C and Han Z F 2013 *Phys. Rev. A* **87** 062329
[19] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev. A* **87** 052309
[20] Huang J Z, Kunz-Jacques S, Jouguet P, Weedbrook C, Yin Z Q, Wang S, Chen W, Guo G C and Han Z F 2014 *Phys. Rev. A* **89** 032304
[21] Kunz-Jacque S and Jouguet P 2015 *Phys. Rev. A* **91** 022307
[22] Jouguet P, Kunz-Jacques S and Diamanti E 2013 *Phys. Rev. A* **87** 062313
[23] Ma X C, Sun S H, Jiang M S and Liang L M 2013 *Phys. Rev. A* **88** 022339
[24] Qin H, Kumar R and Alléaume R 2013 *Proc. SPIE* 8899
[25] Huang P, Lin D K, Huang D and Zeng G H 2015 *International Journal of Theoretical Physics* **54** 2613
[26] Zhou Y M, Jiang X J, Liu W Q, Wang T, Huang P and Zeng G H (Acceptted by Chinese Physics B).
[27] Lodewyck J, Debuisschert T, García-Patrón R, Tualle-Brouri R, Cerf N J and Grangier P 2007 *Phys. Rev. Lett.* **98** 030503
[28] Fossier S, Diamanti E, Debuisschert T, Tualle-Brouri R and Grangier P 2009 *Journal of Physics B: Atomic, Molecular and Optical Physics* **42** 114014
[29] García-Patrón R and Cerf N J 2007 *Quantum Information with Optical Continuous Variables: from Bell Tests to Key Distribution*
[30] Eisert J and Plenio M 2003 arXiv:quant-ph/0312071
[31] Huang D, Huang P, Lin D K and Zeng G H 2016 *Scientific Reports* **6** 19201