SCIENCE CHINA
Information Sciences

• **Supplementary File** •

Hybrid quantum key distribution network

Siyu Ren[1,2], Yu Wang[3] & Xiaolong Su[1,2*]

[1] *State Key Laboratory of Quantum Optics and Quantum Optics Devices, Institute of Opto-Electronics, Taiyuan* 030006*, China;*
[2] *Collaborative Innovation Center of Extreme Optics, Shanxi University, Taiyuan* 030006*, China;*
[3] *State Key Laboratory of Cryptology, Beijing* 100878*, China*

Appendix A Secret key rate of CV QKD system

In the continuous variable quantum key distribution (CV QKD), Alice prepares Gaussian modulated coherent states and sends them to Bob through a quantum channel, Bob performs homodyne measurements on the received states. It has been shown that QKD with coherent state is equivalent to the entanglement-based scheme, where one mode of an Einstein-Podolsky-Rosen (EPR) entangled state is measured by Alice with heterodyne detection system [1]. Generally, the entanglement-based QKD model is used to analyze the security of CV QKD, as shown in Figure A1. We evaluate the secure key rate of CV QKD according to the security analysis in Ref. [2] The EPR state at Alice's station is the entanglement source for the QKD. The EPR state at Bob's station is used to represent the electronic noise V_{el} introduced by Bob's detector [3].

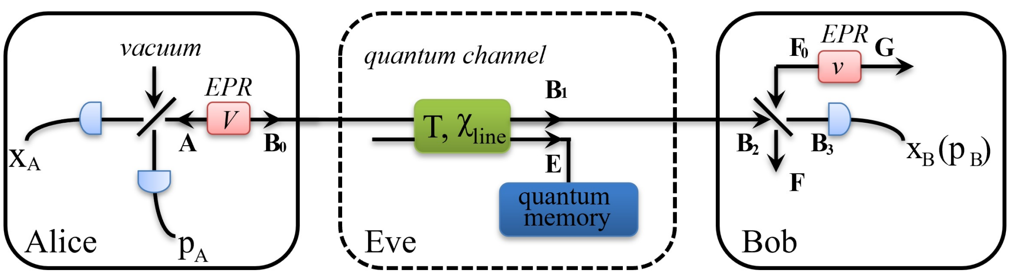

Figure A1 Entanglement-based scheme of a Gaussian coherent-state CVQKD protocol.

For each pulse, Alice randomly chooses two values for the amplitude quadrature $x_A = \hat{a} + \hat{a^{\dagger}}$ and the phase quadrature $p_A = (\hat{a} - \hat{a}^{\dagger})/i$ from a Gaussian distribution centred at zero and of variance $V_A N_0$, where $N_0 = 1$ is the shot noise variance. She prepares a coherent state centred at (x_A, p_A) and sends it to Bob through the quantum channel. The quantum channel features a transmission efficiency T and an excess noise ε. resulting in a noise variance at Bob's input of $(1 + T\epsilon)N_0$. The total channel-added noise referred to the channel input, expressed in shot noise units, is given by

$$\chi_{line} = (1 + T\epsilon)/T - 1 = 1/T - 1 + \epsilon \tag{A1}$$

When Bob receives the modulated coherent state, he measures either one of the two quadratures randomly by a homodyne detector. A practical detector is characterized by an efficiency η and a noise V_{el} due to detector electronics. For homodyne detection, a detection-added noise referred to Bob's input is defined and expressed in shot-noise units, which is given by

$$\chi_{\text{hom}} = [(1 - \eta) + V_{el})]/\eta \tag{A2}$$

The total noise referred to the channel input can then be expressed as

$$\chi_{tot} = \chi_{line} + \chi_{\text{hom}}/T \tag{A3}$$

The mutual information of Alice and Bob, I_{AB}, is given by

$$I_{AB}^{\text{hom}} = \frac{1}{2}\log_2 \frac{V_B}{V_{B|A}} = \frac{1}{2}\log_2 \frac{V + \chi_{tot}}{1 + \chi_{tot}} \tag{A4}$$

where V is the variance of amplitude and phase quadratures of one mode of the EPR state at Alice's station. $V_B = \eta T(V + \chi_{tot})$ and $V_{B|A} = \eta T(1 + \chi_{tot})$ are Bob's measured variance and the conditional variance, respectively.

The maximum information available to Eve on Bob's key is bounded by the Holevo quantity [4].

$$\chi_{BE}^{\text{hom}} = S(\rho_E) - \int dm_B p(m_B) S\rho_E^{m_B} \tag{A5}$$

* Corresponding author (email: Suxl@sxu.edu.cn)

where m_B represents the measurement of Bob, and it can take the form $m_B = x_B(dm_B = dx_B)$ for a homodyne detector. Also, $p(m_B)$ 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 ρ.

Using the fact that Eve's system purifies the system AB_1, Bob's measurement purifies the system AEFG, and $S(\rho_{AFG}^{m_B})$ is independent of m_B for Gaussian protocols, χ_{BE}^{hom} is given by [3]

$$\chi_{BE}^{\text{hom}} = S(\rho_{AB_1}) - S(\rho_{AFG}^{m_B}) \tag{A6}$$

Since it has been shown that Gaussian attacks are optimal for collective attacks [5,6], it is enough to consider Gaussian states, in which case the expressions for the entropies can be further simplified as follows:

$$\chi_{BE}^{\text{hom}} = \sum_{i=1}^{2} G(\frac{\lambda_i - 1}{2}) - \sum_{i=3}^{5} G(\frac{\lambda_i - 1}{2}) \tag{A7}$$

where

$$G(x) = (x+1)\log_2(x+1) - x\log_2 x \tag{A8}$$

$\lambda_{1,2}$ are the symplectic eigenvalues of the covariance matrix γ_{AB_1} characterizing the state ρ_{AB_1}, and $\lambda_{3,4,5}$ are the symplectic eigenvalues of the covariance matrix $\gamma_{AFG}^{m_B}$ characterizing the state $\rho_{AFG}^{m_B}$ after Bob's projective measurement.

The covariance matrix γ_{AB_1} only depends on the system including Alice and the quantum channel, therefore the matrix of the first part of χ_{BE}^{hom} is written as

$$\gamma_{AB_1} = \begin{bmatrix} \gamma_A & \sigma_{AB_1}^T \\ \sigma_{AB_1} & \gamma_{B_1} \end{bmatrix} \tag{A9}$$

$$= \begin{bmatrix} V \cdot I & \sqrt{T(V^2-1)} \cdot \sigma_z \\ \sqrt{T(V^2-1)} \cdot \sigma_z & T(V + \chi_{line}) \cdot I \end{bmatrix} \tag{A10}$$

where I is the 2×2 identity matrix and $\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$. The symplectic eigenvalues $\lambda_{1,2} \geqslant 1$ of the above matrix are given by

$$\lambda_{1,2}^2 = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}] \tag{A11}$$

with

$$A = V^2(1-2T) + 2T + T^2(V + \chi_{line})^2 \tag{A12}$$

$$B = T^2(V\chi_{line} + 1)^2 \tag{A13}$$

To calculate the second part of χ_{BE}, we need to find the symplectic eigenvalues of the covariance matrix $\gamma_{AFG}^{m_B}$, which can be written as

$$\gamma_{AFG}^{m_B} = \gamma_{AFG} - \sigma_{AFGB_3}^T H \sigma_{AFGB_3} \tag{A14}$$

In the above equation, H is the symplectic matrix that represents the homodyne measurement on mode B_3. In the former case, $H_{hom} = (X\gamma_{B_3}X)^{MP}$, where $X = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$ and MP stands for the Moore-Penrose pseudo-inverse of a matrix. The matrices γ_{B_3}, γ_{AFG}, and σ_{AFGB_3} can all be derived from the decomposition of the covariance matrix:

$$\gamma_{AFGB_3} = \begin{bmatrix} \gamma_{AFG} & \sigma_{AFGB_3}^T \\ \sigma_{AFGB_3} & \gamma_{B_3} \end{bmatrix} \tag{A15}$$

The above matrix can be derived with appropriate rearrangement of lines and columns from the matrix describing the system AB_3FG:

$$\gamma_{AB_3FG} = (Y^{BS})^T[\gamma_{AB_1} \oplus \gamma_{F_0G}]Y^{BS} \tag{A16}$$

Here, γ_{F_0G} is the matrix that describes the EPR state of variance v used to model the detector's electronic's noise. It is written as

$$\gamma_{F_0G} = \begin{bmatrix} v \cdot I & \sqrt{(v^2-1)} \cdot \sigma_z \\ \sqrt{(v^2-1)} \cdot \sigma_z & v \cdot I \end{bmatrix} \tag{A17}$$

where $v = \eta\chi_{\text{hom}}/(1-\eta)$. Finally, the matrix Y^{BS} describes the beam splitter transformation that models the inefficiency of the detector and acts on modes B_2 and F_0. It is given by the expression:

$$Y^{BS} = I_A \oplus Y_{B_2F_0}^{BS} \oplus I_G \tag{A18}$$

with

$$Y_{B_2F_0}^{BS} = \begin{bmatrix} \sqrt{\eta} \cdot I & \sqrt{1-\eta} \cdot I \\ -\sqrt{1-\eta} \cdot I & \sqrt{\eta} \cdot I \end{bmatrix} \tag{A19}$$

We now have all the elements required to proceed to the calculation of the symplectic eigenvalues $\lambda_{3,4,5}$. We find that the eigenvalues $\lambda_{3,4} \geqslant 1$ are given by expressions of the form

$$\lambda_{3,4}^2 = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}] \tag{A20}$$

where

$$C = \frac{A\chi_{\text{hom}} + V\sqrt{B} + T(V + \chi_{line})}{T(V + \chi_{tot})} \tag{A21}$$

$$D = \sqrt{B}\frac{V + \sqrt{B}\chi_{\text{hom}}}{T(V + \chi_{tot})} \tag{A22}$$

The last symplectic eigenvalue is $\lambda_5 = 1$. Based on the equations above, we calculate the Holevo information bound χ_{BE}^{hom} and thus derive the Holevo secret key generation rate

$$\Delta I_{Holevo}^{\text{hom}} = I_{AB}^{\text{hom}} - \chi_{BE}^{\text{hom}} \tag{A23}$$

for homodyne detection.

Taking the finite-size effects into account, the maximum secret key rate bounded by collective attacks is given by [7]

$$R_{finite} = \frac{n}{N}[\beta I_{AB}^{\text{hom}} - \chi_{BE}^{\text{hom}} - \triangle(n)] \tag{A24}$$

where N and n denote the sampling length and the block length for final key estimation, respectively. We set $N = 10^{10}$ and $n = N/2$ according to the Ref. [7]. $\triangle(n) =$ is related to the security of the privacy amplification and its detailed calculation process will also be given in Ref. [7]. We set $T = 10^{-\alpha L/10}$, with $\alpha = 0.2$ dB/km the linear attenuation of a standard optical fibre and L the distance. The remaining parameters are $V = 4, \eta_{practical} = 60\%, \eta_{ideal} = 98\%, V_{el} = 0.01, \epsilon = 0.01$ and $\beta = 95.6\%$. Here, we ignore the repetition rate of CV QKD system just for the consistency with DV QKD.

Appendix B Secret key rate of decoy state DV QKD system

Decoy states is a useful method for substantially improving the performance of QKD, which allows an efficient way to distill secret key using weak coherent pulses. In the decoy state BB84 QKD, the secret key rate is given by [8]

$$R \geqslant q\left\{-Q_\mu f H_2\left(E_\mu\right) + Q_1\left[1 - H_2\left(e_1\right)\right]\right\} \tag{B1}$$

where q depends on the implementation of the protocol (for the Bennett-Brassard 1984 (BB84) protocol $q = 1/2$). The subscript μ denotes the intensity of signal states, Q_μ is the gain of signal states, E_μ is the overall quantum bit error rate (QBER), Q_1 is the gain of single-photon states, e_1 is the error rate of the single-photon states, f is the bidirectional error correction efficiency, $H_2(x)$ is the binary Shannon information function, which is given by

$$H_2(x) = -x\log_2(x) - (1 - x)\log_2(1 - x) \tag{B2}$$

Q_μ and E_μ can be measured directly from the experiment, while Q_1 and e_1 should be estimated.

For the real single-photon source, The key generation rate of QKD (R_1) is:

$$R_1 = qY_1\left(-fH_2\left(e_1\right) + 1 - H_2\left(e_1\right)\right) \tag{B3}$$

The yield of an i-photon state, Y_i, comes from background (Y_0) and real signal. The yield of real single-photon signal equals to the overall transmission and detection efficiency, η_i, between Alice and Bob.

$$Y_i = Y_0 + \eta_i - Y_0\eta_i \tag{B4}$$

The error rate of the i-photon state, is given by

$$e_i = \frac{e_0 Y_0 e_d \eta_i}{Y_i} \tag{B5}$$

where e_d is the probability that a photon hit the wrong detector.

We calculate the key generation rate of QKD with infinite number of decoy states by using Eq. [27], where Q_μ, E_μ and Q_1 can be expressed as follow respectively.

$$Q_\mu = Y_0 + 1 - e^{-\eta\mu} \tag{B6}$$

$$E_\mu = \frac{1}{Q_\mu}\left(e_0 Y_0 + e_d\left(1 - e^{-\eta\mu}\right)\right) \tag{B7}$$

$$Q_1 = Y_1\mu e^{-\mu} \tag{B8}$$

We use the experimental parameters from a particular QKD experiment [9]. Although in recent years the device has some improvement, but the key generation rate has no essential change by using InGaAs/InP single-photon avalanche diodes.The parameters are $\mu = 0.48$, $f = 1.22$, $e_0 = 1/2$, $e_d = 0.033$, $Y_0 = 1.7 \times 10^{-6}$, $\eta = \eta_{Bob}t_{ab}$, t_{ab} is the channel transmittance, $\eta_{Bob} = 66\%$ for practical decoy-state DV QKD with advanced superconducting nanowire single photon detector operating at 2.05 K [10]. $\eta_{Bob} = 93\%$ for decoy-state DV QKD with advanced superconducting nanowire single photon detector, which operate below 2 K in a cryogenic system.

Appendix C Secret key rate of CV MDI QKD system

To evaluate the secure key rate of CV-MDI-QKD we follow the Supplementary Information of Ref. [11]. When the finite-size effects are taken into account, the secret key rate is evaluated by

$$R_{CV} = \frac{n}{N}[\beta I_{AB} - I_E] \tag{C1}$$

where $N = 10^{10}$ and $n = N/2$ denote the sampling length and the block length for final key estimation respectively, β is the reconciliation efficiency of the error correction code, and I_{AB} and I_E denote, respectively, Alice and Bob's mutual information and Eve's stolen information on Alice's key.

To derive an explicit formula for the secret key rate given above, Pirandola et al. consider a "realistic Gaussian attack against the two links" [11], which definitively provides an upper bound on the secure key rate. Here, we assume the most favorable situation for CV-MDI-QKD by considering that such realistic Gaussian attack is indeed optimal and the resulting key rate is achievable. In doing so, we have that the quantity I_{AB} can be expressed as [11]

$$I_{AB} = \log_2\left(\frac{V+1}{\chi}\right) \tag{C2}$$

where V is the modulation variance in shot-noise units and χ represents the so-called equivalent noise.

Moreover, for simplicity, we consider the key rate in the limit of large modulation ($V \geqslant 1$). In this scenario, and considering first the asymmetric case $\eta_A \neq \eta_B$, we have that I_E is given by

$$I_E = h(\beta) + \log_2(\gamma) - h(\delta) \tag{C3}$$

where the parameters β, γ, δ have the form

$$\beta = \frac{\eta_A\eta_B\chi - (\eta_A+\eta_B)^2}{|\ \eta_{A-}\eta_B\ |\ (\eta_A+\eta_B)} \tag{C4}$$

$$\gamma = \frac{e\ |\ \eta_{A-}\eta_B\ |\ (\phi+1)}{2(\eta_A+\eta_B)} \tag{C5}$$

$$\delta = \frac{\eta_A\chi - (\eta_A+\eta_B)}{\eta_A+\eta_B} \tag{C6}$$

Here, the term e denotes Euler's number, and the equivalent noise χ is given by

$$\chi = \frac{2(\eta_A+\eta_B)}{\eta_A\eta_B\eta_d} + \epsilon \tag{C7}$$

with ϵ being the excess noise. Finally, the function $h(x)$ has the form

$$h(x) = (\frac{x+1}{2})\log_2\left(\frac{x+1}{2}\right) - (\frac{x-1}{2})\log_2\left(\frac{x-1}{2}\right) \tag{C8}$$

In the symmetric case where $\eta_{A=}\eta_{B=}\eta$, we have that I_E is given by [11]

$$I_E = \log_2\left(\frac{e^2(\chi-4)(V+1)}{16}\right) - h(\frac{\chi-1}{2}) \tag{C9}$$

where the equivalent noise χ has now the form

$$\chi = \frac{4}{\eta\eta_d} + \epsilon \tag{C10}$$

The parameters are $\eta = 97\%$ [17], $\epsilon = 0.01$, V =10 and $\beta = 97\%$.

Appendix D Secret key rate of DV MDI QKD system

The secure key rate of decoy-state DV-MDI-QKD in the asymptotic limit of an infinitely long key is given by [12]

$$R_{DV} = P_{11}^Z Y_{11}^Z[1 - H_2(e_{11}^X)] - Q^Z f H_2(E^Z) \tag{D1}$$

where $P_{11}^Z = \mu_A\mu_B e^{-(\mu_A+\mu_B)}$ denotes the joint probability that both Alice and Bob generate a single-photon pulse, and with μ_A and μ_B being, respectively, the intensity of Alice and Bob's signal states; the parameters Y_{11}^Z and e_{11}^X are, respectively, the yield in the rectilinear(Z) basis and the error rate in the diagonal(X) basis, given that both Alice and Bob send single-photon states; $H_2(x) = -xlog_2(x) - (1-x)log_2(1-x)$ is the binary Shannon entropy function; the terms Q^Z and E^Z denote, respectively, the overall gain and quantum bit error rate (QBER) in the Z basis when both Alice and Bob emit a signal state; and $f \geqslant 1$ is the error correction inefficiency function.

The quantities Q^Z and E^Z are directly measured in the experiment, while Y_{11}^Z and e_{11}^X can be estimated using the decoy-state method [13]. Importantly, it has been shown that the use of two decoy states is already enough to obtain a tight estimation for Y_{11}^Z and e_{11}^X [14].

To model experimental errors, we employ the method proposed in Ref. [13] for polarisation encoding DV-MDI-QKD [15, 16]. In particular, we use two unitary operators, located at the input arms of the beam splitter within the relay to simulate the intrinsic error rate, denoted as e_d, due to the misalignment and instability of the optical system. In addition, we consider threshold single-photon detectors (SPDs) with detection efficiency η_d and dark count rate Y_0. Furthermore, for simplicity, we consider the asymptotic case where Alice and Bob use an infinite number of decoy states. As already mentioned, the practical situation with a finite number of decoy settings provides similar results [14]. In this scenario, we have that the parameters Y_{11}^Z and e_{11}^X have the form [13]

$$\begin{aligned} Y_{11}^Z &= (1-Y_0)^2[4Y_0^2(1-\eta_A\eta_d)(1-\eta_B\eta_d) \\ &+2Y_0(\eta_A\eta_d+\eta_B\eta_d-\frac{3}{2}\eta_A\eta_B\eta_d^2) \\ &+\frac{1}{2}\eta_A\eta_B\eta_d^2] \end{aligned} \tag{D2}$$

$$e_{11}^X = \frac{1}{2} - \frac{(1-Y_0)^2\eta_A\eta_B\eta_d^2(1-ed)^2}{4Y_{11}^X} \tag{D3}$$

where $\eta_A(\eta_B)$ denotes the channel transmittance from Alice (Bob) to the relay. That is $\eta_A = 10^{-\alpha l_A/10}$, where α is the loss coefficient of the channel that connects Alice with the relay measured in dB/km, and l_A is the length of this channel measured in km. The definition of η_B is analogous. Moreover, we have that $Y_{11}^X = Y_{11}^Z$.

For completeness, we include the mathematical expressions below. In particular,

$$Q^Z = \frac{1}{2}(\Omega_1+\Omega_2) \tag{D4}$$

$$E^Z = \frac{\Omega_1}{\Omega_1+\Omega_2} \tag{D5}$$

where the parameters Ω_1 and Ω_2 are given by

$$\begin{aligned} \Omega_1 &= 2e^{-\frac{\gamma}{2}}(1-Y_0)^2[I_0(\beta)+I_0(\beta-2\beta e_d) \\ &+2(1-Y_0)^2e^{-\frac{\gamma}{2}}-2(1-Y_0)e^{-\frac{\gamma(1-ed)}{2}}I_0(e_d\beta) \\ &-2(1-Y_0)e^{-\frac{\gamma ed)}{2}}I_0(\beta-e_d\beta)] \end{aligned} \tag{D6}$$

$$\begin{aligned} \Omega_2 &= 2e^{-\frac{\gamma}{2}}(1-Y_0)^2[1+I_0(2\lambda)+2(1-Y_0)^2e^{-\frac{\gamma}{2}} \\ &-2(1-Y_0)e^{-\frac{\omega}{2}}I_0(\lambda)-2(1-Y_0)e^{-\frac{\gamma-\omega}{2}}I_0(\lambda)] \end{aligned} \tag{D7}$$

with $I_0(x)$ being the modified Bessel function, and where

$$\gamma = (\mu_A\eta_A+\mu_B\eta_B)\eta_d \tag{D8}$$

$$\beta = \eta_d\sqrt{\mu_A\eta_A\mu_B\eta_B} \tag{D9}$$

$$\lambda = \beta\sqrt{e_d(1-e_d)} \tag{D10}$$

$$\omega = \mu_A\eta_A\eta_d + e_d(\mu_B\eta_{B-}\mu_A\eta_A)\eta_d \tag{D11}$$

The parameters are $e_d = 0.1\%$, $Y_0 = 10^{-6}$, $f = 1.16$, $\eta_d = 66\%$ and $\eta_d = 93\%$ for DV-MDI-QKD with with advanced superconducting nanowire single photon detectors.

References

1 Grosshans F, Cerf N J. Virtual entanglement and reconciliation protocols for quantum cryptography with continuous variables. Quantum Inf Comput, 2003, 3: 535-552.

2 Fossier S, Diamanti E, Debuisschert T, et al. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. J Phys B, 2009, 42: 114014.

3 Lodewyck J, Bloch M, Garía-Patrón R, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. Phys Rev A, 2007, 76: 042305.

4 R. Renner. Security of quantum key distribution. Dissertation for the Doctoral Degree. Switzerland: ETH, 2005.

5 Navascués M, Grosshans F and Acín A. Optimality of Gaussian attacks in continuous-variable quantum cryptography. Phys Rev Lett, 2006, 97: 190502.

6 García-Patrón R and Cerf N J. Unconditional optimality of Gaussian attacks against continuous-variable quantum key distribution. Phys Rev Lett, 2006, 97: 190503.

7 Leverrier A, Grosshans F, and Grangier P. Finite-size analysis of a continuous-variable quantum key distribution. Phys Rev A, 2010, 81: 062343.

8 Lo H-K, Ma X F, and Chen K. Decoy state quantum key distribution. Phys Rev Lett, 2005, 94: 230504.

9 Gobby C, Yuan Z L and Shields A J. Quantum key distribution over 122 km of standard telecom fiber. Appl Phys Lett, 2004, 84: 3762.

10 Yin H L, Chen T Y, Yu Z W, et al. Measurement-device-independent quantum key distribution over a 404 km optical fiber. Phys Rev Lett, 2016, 117: 190501.

11 Pirandola S, Ottaviani C, Spedalier G, et al. High-rate measurement-device-independent quantum cryptography. Nature photon, 2015, 9: 397-402.

12 Lo H K, Curty M and Qi B. Measurement-device independent quantum key distribution. Phys Rev Lett, 2012, 108: 130503.

13 Xu F H, Curty M, Qi B, et al. Practical aspects of measurement-device-independent quantum key distribution. New J Phys, 2013, 15: 113007.

14 Xu F H, Xu H, and Lo H K. Protocol choice and parameter optimization in decoy-state measurement-device-independent quantum key distribution. Phys Rev A, 2014, 89: 052333.
15 Ferreira da Silva T, Vitoreti D, Xavier G B, et al. Proof-of-principle demonstration of measurement-device-independent quantum key distribution using polarization qubits. Phys Rev A, 2013, 88: 052303.
16 Tang Z Y, Liao Z F, Xu F H, et al. Experimental demonstration of polarization encoding measurement-device-independent quantum key distribution. Phys Rev Lett, 2014, 112: 190503.
17 Tian Y, Wang P, Liu J Q, et al. Experimental demonstration of continuous-variable measurement-device-independent quantum key distribution over optical fiber. Optica, 2022, 9: 492.