SCIENCE CHINA
Information Sciences

August 2023, Vol. 66 180507:1–180507:12
https://doi.org/10.1007/s11432-022-3712-3

• RESEARCH PAPER •
Special Topic: Quantum Information

Practical continuous-variable quantum key distribution with feasible optimization parameters

Li MA[1], Jie YANG[1,2], Tao ZHANG[1], Yun SHAO[1], Jinlu LIU[1], Yujie LUO[1], Heng WANG[1], Wei HUANG[1], Fan FAN[1], Chuang ZHOU[1], Liangliang ZHANG[1], Shuai ZHANG[1], Yichen ZHANG[2], Yang LI[1*] & Bingjie XU[1*]

[1]*Science and Technology on Communication Security Laboratory, Institute of Southwestern Communication, Chengdu* 610041, *China;*
[2]*State Key Laboratory of Information Photonics and Optical Communications, Beijing University of Posts and Telecommunications, Beijing* 100876, *China*

Received 7 September 2022/Revised 5 December 2022/Accepted 6 March 2023/Published online 26 June 2023

Abstract Continuous-variable quantum key distribution (CV-QKD) offers an approach to achieve a potential high secret key rate (SKR) in metropolitan areas. There are several challenges in developing a practical CV-QKD system from the laboratory to the real world. One of the most significant points is that it is really hard to adapt different practical optical fiber conditions for CV-QKD systems with unified hardware. Thus, how to improve the performance of practical CV-QKD systems in the field without modification of the hardware is very important. Here, a systematic optimization method, combining the modulation variance and error correction matrix optimization, is proposed to improve the performance of a practical CV-QKD system with a restricted capacity of postprocessing. The effect of restricted postprocessing capacity on the SKR is modeled as a nonlinear programming problem with modulation variance as an optimization parameter, and the selection of an optimal error correction matrix is studied under the same scheme. The results show that the SKR of a CV-QKD system can be improved by 24% and 200% compared with previous frequently used optimization methods theoretically with a transmission distance of 50 km. Furthermore, the experimental results verify the feasibility and robustness of the proposed method, where the achieved optimal SKR achieved practically deviates <1.6% from the theoretical optimal value. Our results pave the way to deploy high-performance CV-QKD in the real world.

Keywords continuous-variable, quantum key distribution, post-processing, optimization, secret key rate

Citation Ma L, Yang J, Zhang T, et al. Practical continuous-variable quantum key distribution with feasible optimization parameters. Sci China Inf Sci, 2023, 66(8): 180507, https://doi.org/10.1007/s11432-022-3712-3

1 Introduction

Quantum key distribution (QKD) can realize secure key distribution remotely with unsecured channels in real time based on the principle of quantum mechanics, which has made a series of progresses in recent years [1–9]. There are mainly two types of QKD protocols, which respectively encode information on discrete variables [10, 11] and continuous variables [12–14]. The continuous-variables QKD (CV-QKD) takes advantage of the use of standard telecommunication technologies [15–18] and obtains high key rates within metropolitan areas.

Recently, significant progress has also been made in the field of theory and experiments on CV-QKD. On the one hand, each core procedure of a CV-QKD system (e.g., quantum state preparation, measurement, and postprocessing) should be correctly and efficiently implemented experimentally, which provides a hardware basis for high-performance CV-QKD and has made significant progress in recent years [19–29]. On the other hand, to further enhance the performance of a CV-QKD system, many advanced theoretical methods have been proposed and demonstrated, including the excess noise modeling

* Corresponding author (email: yishuihanly@pku.edu.cn, xbjpku@pku.edu.cn)

and suppression [16, 30–32], system parameter optimization method (e.g., modulation variance V_A), advanced information reconciliation method [33–38], high-efficiency error correction matrix design [39, 40], rate-adaptive algorithm [41–46], postselection [47–49], and add noise method [50], which provides a software basis to improve the system performance. Based on a particular CV-QKD hardware setup with a predefined protocol, how to comprehensively optimize the secret key rate (SKR) based on the above theoretical methods are of great importance. However, the above methods are not independent of one another, and sometimes one needs to make a systematic optimization. For example, the optimal choice of V_A will significantly influence the SKR, which is closely related to the error correction matrix $\boldsymbol{H}$ design and choice. A global optimization method for a CV-QKD system in software is still incomplete, among which the systematic optimization of system parameters with error correction is of special importance with respect to the SKR. In contrast, there are several challenges in developing widely used practical CV-QKD systems. One of the most significant points is that it is really hard to adapt different practical optical fiber conditions for CV-QKD systems with unified hardware. Thus, how to improve the performance of practical CV-QKD systems in the field without modification of the hardware is very important.

In a practical CV-QKD system, V_A should be adjusted periodically with the variation in system parameters to optimize the system performance in real time. When the system environment is relatively stable in the short term, the system parameters channel transmittance T, excess noise ξ, detection electrical noise v_{el}, and detection efficiency η change slowly with time. In this condition, one can reasonably use the calculated optimal V_A based on the measured system parameters of a raw data block as the expected real optimal V_A for the next successive raw data block. Thus, practically, the signal-to-noise ratio (SNR) of the system is mainly determined by V_A, which directly decides the performance of the data reconciliation in postprocessing and significantly affects the SKR of the CV-QKD system. Although various schemes to optimize V_A have been proposed, it is usually assumed that the reconciliation efficiency β in data reconciliation and frame error rate (FER) in error correction are constant under a specific transmission distance [26, 34]. However, since the SNR is mainly determined by V_A under a specific transmission distance, to maintain β as a constant for different V_A, several different $\boldsymbol{H}$ with corresponding code rates should be designed for the data reconciliation, which is very difficult to fulfill in practice. Furthermore, the FER for a specific $\boldsymbol{H}$ should vary under different V_A [51], and various $\boldsymbol{H}$ are needed to keep the FER as a constant, which is difficult to fulfill. Actually, under typical transmission distances, it is only possible to switch between a few well-designed $\boldsymbol{H}$ with different code rates according to the SNRs [16]. The fluctuations of β and FER with V_A should be taken into consideration to achieve a systematic optimization.

In this paper, we propose and experimentally verify a feasible optimization method for a practical CV-QKD system with a restricted capacity of postprocessing. Different from the previously proposed method, in our work, for certain data reconciliation and error correction matrix $\boldsymbol{H}$, the influences of V_A on β and the FER are quantitatively analyzed and experimentally verified. This method can be easily applied in a practical CV-QKD system, and the actual achieved SKR deviates only $<1.6\%$ from the theoretical optimal value in our experiment. Moreover, the proposed method can be combined with various advanced postprocessing technologies to realize a global optimization method for the CV-QKD system in software without any hardware modification, such as rate-adaptive algorithm, postselection, and add noise method, to further improve the performance of CV-QKD.

The paper is organized as follows. In Section 2, we introduce the optimization method for the CV-QKD system with GG02 and no-switching protocol, respectively. In Section 3, we show the simulation and experimental performance of the method. Finally, in Section 4, we discuss and conclude this paper.

2 Feasible optimization method for a CV-QKD system

First, the influence of V_A on the SKR for GG02 [12] and no-switching CV-QKD protocol [13] is quantitatively analyzed, where the optimization of the SKR can be defined as a nonlinear programming problem. Second, an experimentally feasible operational process for the above optimization method is given, where the fitting curve of the FER on V_A is experimentally given.

2.1 Theoretical model for the optimal choice of V_A and the error correction matrix

In the GG02 protocol with homodyne detection, we suppose that x and y denote the raw keys of Alice and Bob after the sifting process. The SKR with composable finite-size security can be expressed as [52, 53]

$$K_{\text{finite}}^{\text{hom}} = \frac{np_{\text{ec}}}{N}\left(\beta^{\text{hom}} I^{\text{hom}}(x:y) - \chi^{\text{hom}}(y:E) - \frac{\Delta_{\text{aep}}}{\sqrt{n}} + \frac{\Theta}{\sqrt{n}}\right), \tag{1}$$

where N is the block size of the raw key, n ($m = N - n$) is the fraction for key distillation (parameter estimation), and the probability of successful error-correction is p_{ec} ($p_{\text{ec}} = 1 - \text{FER}$), $\text{FER} \in [0, 1]$, $\beta^{\text{hom}} \in [0, 1]$, $I^{\text{hom}}(x:y)$ is the Shannon mutual information between Alice and Bob, $\chi^{\text{hom}}(y:E)$ is the Holevo bound of Bob and Eve. The extra finite-size terms are given as

$$\Delta_{\text{aep}} = 4\log_2(\sqrt{d}+2)\sqrt{\log_2\left(\frac{18}{p_{\text{ec}}^2\varepsilon_s^4}\right)}, \tag{2}$$

$$\Theta = \log_2\left[p_{\text{ec}}\left(1 - \frac{\varepsilon_s^2}{3}\right)\right] + 2\log_2\sqrt{2}\varepsilon_h, \tag{3}$$

where d represents the size of the effective alphabet after analog-to-digital conversion of sender's and receiver's CVs (quadrature encodings and outcomes). ε_h is a hashing parameter and ε_s is a smoothing parameter with a value of 10^{-10}. Reverse reconciliation is employed here to beat the 3 dB limit in CV-QKD.

As shown in Appendix A, $I^{\text{hom}}(x:y)$ and $\chi^{\text{hom}}(y:E)$ can be analytically represented by T, ξ, η, v_{el}, and V_A. When the system environment is relatively stable, T, ξ, η, and v_{el} should change slowly which can be approximated as constants in two successive rounds of raw data. Thus $I^{\text{hom}}(x:y)$ and $\chi^{\text{hom}}(y:E)$ can be treated as a function of the V_A, where $I^{\text{hom}}(x:y) = f_{I^{\text{hom}}(x:y)}(V_A)$ and $\chi^{\text{hom}}(y:E) = f_{\chi^{\text{hom}}(y:E)}(V_A)$. $\beta^{\text{hom}} = R/I^{\text{hom}}(x:y)$, where R is the code rate of the practically used error correction matrix $\boldsymbol{H}$. Furthermore, the performance of the decoding in error correction is directly related to the SNR, which means $\text{FER} = f_{\text{FER}}(V_A)$ is decided by $\boldsymbol{H}$ and can be measured experimentally. Denote $Q = -\frac{\Delta_{\text{aep}}}{\sqrt{n}} + \frac{\Theta}{\sqrt{n}}$ in (1)–(3), and one can easily verify that Q is directly related to FER given fixed n, d, ε_h, and ε_s, which means $Q = f_Q(V_A)$.

As a result, the SKR can be expressed as

$$K_{\text{finite}}^{\text{hom}}(V_A) = f(V_A)^{\text{hom}} = \frac{n}{N}(1 - f_{\text{FER}}(V_A))(R - f_{\chi^{\text{hom}}(y:E)}(V_A) + f_Q(V_A)). \tag{4}$$

In the no-switching protocol with heterodyne detection, the SKR with composable finite-size security can be expressed as [52, 53]

$$K_{\text{finite}}^{\text{het}} = \frac{np_{\text{ec}}}{N}\left(\beta^{\text{het}} I^{\text{het}}(x:y) - \chi^{\text{het}}(y:E) - \frac{\Delta_{\text{aep}}}{\sqrt{n}} + \frac{\Theta}{\sqrt{n}}\right). \tag{5}$$

Similarly, $I^{\text{het}}(x:y) = \log_2(1 + \text{SNR})$, $\beta^{\text{het}} I^{\text{het}}(x:y) = 2R$, and $\chi^{\text{het}}(y:E) = f_{\chi^{\text{het}}(y:E)}(V_A)$.

Thus, the SKR for the no-switching protocol can be expressed as

$$K_{\text{finite}}^{\text{het}}(V_A) = f(V_A)^{\text{het}} = \frac{n}{N}(1 - f_{\text{FER}}(V_A))(2R - f_{\chi^{\text{het}}(y:E)}(V_A) + f_Q(V_A)). \tag{6}$$

In both (4) and (6), the V_A can be regarded as the only variable when T, ξ, η, and v_{el} remain stable in two successive raw data block. Therefore, the optimization of the SKR for a given $\boldsymbol{H}$ is a constrained nonlinear programming problem as

$$\underset{V_A}{\text{Max}}\frac{n}{N}(1 - f_{\text{FER}}(V_A))(v_{\text{det}}R - f_{\chi^{\text{hom/het}}(y:E)}(V_A) + f_Q(V_A)), \tag{7}$$

where v_{det} is the quantum duty ("qu-duty") associated with detection: $v_{\text{det}} = 1$ for homodyne and $v_{\text{det}} = 2$ for heterodyne. Subject to $0 \leqslant \beta^{\text{hom/het}} \leqslant 1$, where $f_{\text{FER}}(V_A)$, $f_{\chi^{\text{hom/het}}(y:E)}(V_A)$, and $f_Q(V_A)$ are nonlinear functions of V_A. For a given $\boldsymbol{H}$, the optimization method therefore realizes a trade-off between the FER $f_{\text{FER}}(V_A)$ and the Holevo information $f_{\chi^{\text{hom/het}}(y:E)}(V_A)$.

Based on the above method, one can easily make a systematic optimal choice of V_A and $\boldsymbol{H}$ with different code rates under different transmission distances.

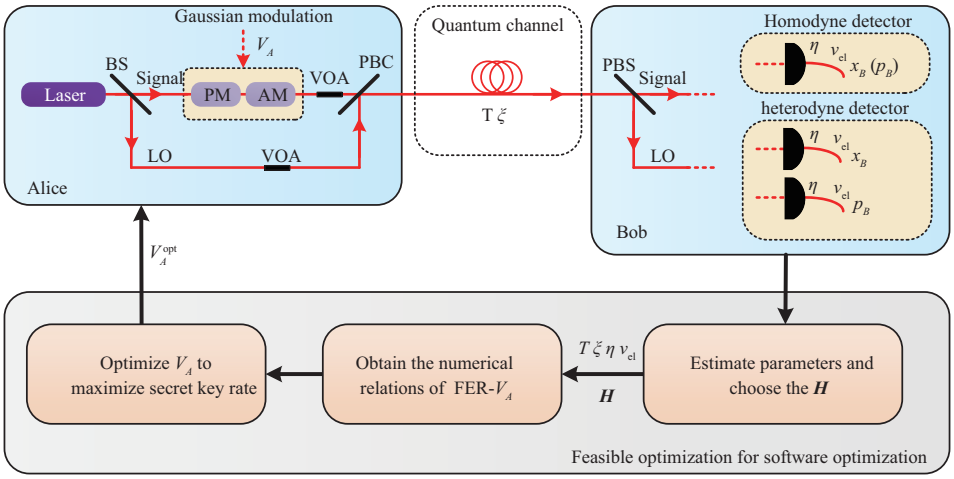

Figure 1 (Color online) Feasible optimization scheme for the proposed optimization method. For a heterodyne detector, Bob employs two identical balanced detectors for simplicity. BS: beam splitter; AM: amplitude modulator; PM: phase modulator; PBS/C: polarization beam splitter/coupler; LO: local oscillator; VOA: variable optical attenuator.

2.2 Feasible operational process for the proposed optimization method

The feasible optimization scheme for the proposed method in a CV-QKD system is shown in Figure 1. First, we obtained the system parameters $\{T, \xi, \eta, v_{\rm el}\}$ and chose an appropriate $\boldsymbol{H}$. Usually, we choose the range of V_A from 0 to 100 [36], and we expect β to be as large as possible, e.g., $\beta \in [0.8, 1]$. Thus, the SNR range can be roughly estimated, and the corresponding $\boldsymbol{H}$ can be preliminarily chosen. For a CV-QKD system with a relatively stable environment, T, ξ, η, $v_{\rm el}$ should change slowly in a period of time, which can be measured and updated in real time for each data block. Second, we obtained the numerical relation of FER-V_A via curve fitting for the chosen $\boldsymbol{H}$. Based on the specific performance of data reconciliation and error correction, $f_{\rm FER}(V_A)$ can be obtained experimentally. Finally, we substituted $f_{\rm FER}(V_A)$ into (4) and (6) to obtain the comprehensive function of SKR on V_A, based on which the optimal modulation variance $V_A^{\rm opt}$ can be accordingly estimated.

In the following, we introduce in detail the method to obtain the numerical relation of $f_{\rm FER}(V_A)$. In homodyne detection, the same system parameters as in [34,54] are employed to numerically generate raw data. The transmission distance was set as $L = 50$ km, $\eta = 0.606$, $\xi = 0.005$, $v_{\rm el} = 0.041$, $T = 10^{-\alpha L/10}$ with $\alpha = 0.2$ dB/km. The degree distribution function with $R = 0.1$ as in [41] was chosen to generate the $\boldsymbol{H}$ using our own matrix generation method as in [55]. $f_{\rm FER}(V_A)$ was directly determined by the SNR and $\boldsymbol{H}$. Thus, with different $\boldsymbol{H}$, different results will be obtained.

To measure the function FER-V_A, we first generated raw data based on the above system parameters with $V_A \in (0, 100]$. Second, an eight-dimensional multidimensional reconciliation was performed on the raw data, and the chosen $\boldsymbol{H}$ was employed for error correction. Thus, the FERs in the error correction under different V_A can be measured experimentally, and the numerical relationship FER-V_A can be obtained for a practical CV-QKD system. The curve fitting result of FER-V_A to generate $\boldsymbol{H}$ is shown in Figure 2(a). When $0 < V_A < 2.7$, FER $= 1$, indicating that the error correction has all failed. When $V_A > 3$, FER $= 0$, indicating that the error correction has all succeeded. However, when $2.7 \leqslant V_A \leqslant 3$, FER decreases with the increase in V_A. Therefore, we mainly needed to perform the curve fitting in the range of $2.7 \leqslant V_A \leqslant 3$. By employing different fitting functions and comparing the corresponding fitting effects and computational complexities, finally, the fourth-order Gaussian function was chosen in this paper, as shown in

$$\begin{aligned}{\rm FER} &= f_{\rm FER}(V_A)\\ &= \begin{cases} 1, & 0 < V_A < 2.7,\\ 0.8310{\rm e}^{-(\frac{V_A-2.654}{0.08704})^2} + 0.6753{\rm e}^{-(\frac{V_A-2.113}{0.4542})^2} + 0 + 0.3437{\rm e}^{-(\frac{V_A-2.722}{0.03649})^2}, & 2.7 \leqslant V_A \leqslant 3,\\ 0, & V_A > 3. \end{cases}\end{aligned} \tag{8}$$

In the numerical simulation, the block size N is set as 2×10^8, 2×10^9, 2×10^{10}, and ∞, respectively, and n is set to be $N/2$. The curve of $f_{\chi^{\rm hom}(y:E)}(V_A)$ is shown in Figure 2(b), which is a monotonically increasing

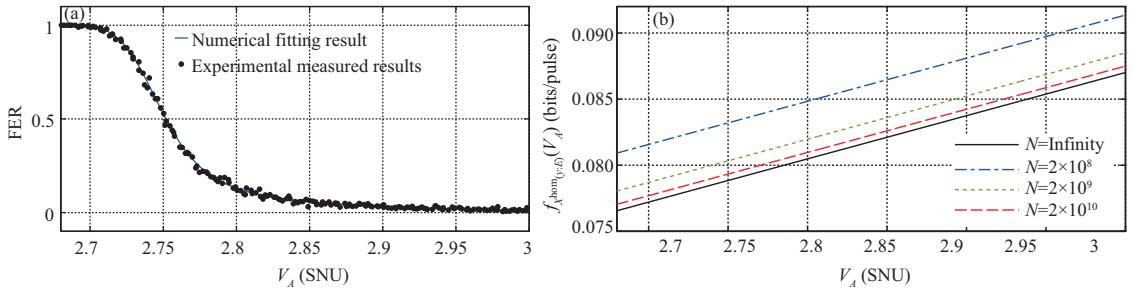

Figure 2 (Color online) (a) Experimentally measured results (black dots) and numerical fitting result (blue line) of FER-V_A with the GG02 protocol. (b) Simulation curves of the $f_{\chi^{\hom}(y:E)}(V_A)$ with the GG02 protocol. From top to bottom, the curves respectively show the results with a total block size of $N = 2 \times 10^8$, 2×10^9, 2×10^{10}, and ∞. The results show that both of them are proportional to V_A. The system parameters are set as follows: $L = 50$ km, $\eta = 0.606$, $\xi = 0.005$, $v_{\rm el} = 0.041$, $\alpha = 0.2$ dB/km, $T = 0.1$, and $R = 0.1$. SNU: shot noise units. The number of iterations is 60.

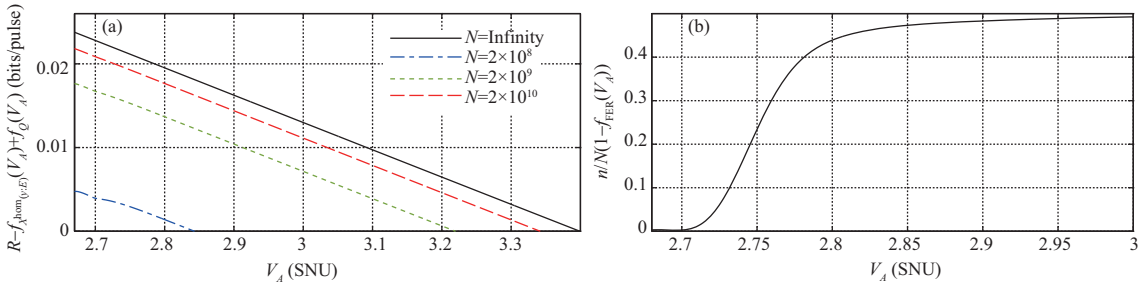

Figure 3 (Color online) (a) Simulation curves of the $R - f_{\chi^{\hom}(y:E)}(V_A) + f_Q(V_A)$ with respect to V_A under the GG02 protocol. From bottom to top, the curves respectively show the results with the total block size of $N = 2 \times 10^8$, 2×10^9, 2×10^{10}, and ∞. The results show that both of them are inversely proportional to V_A. (b) The curve is $\frac{n}{N}(1 - f_{\rm FER}(V_A))$ with respect to V_A. The system parameters are set as follows: $\frac{n}{N} = 0.5$, $L = 50$ km, $\eta = 0.606$, $\xi = 0.005$, $v_{\rm el} = 0.041$, $\alpha = 0.2$ dB/km, $T = 0.1$, and $R = 0.1$.

function of V_A. Furthermore, the simulation curves of $R - f_{\chi^{\hom}(y:E)}(V_A) + f_Q(V_A)$ and $\frac{n}{N}(1 - f_{\rm FER}(V_A))$ with respect to V_A for GG02 protocol is shown in Figure 3, where $R - f_{\chi^{\hom}(y:E)}(V_A) + f_Q(V_A)$ is a monotonically decreasing function of V_A, and $\frac{n}{N}(1 - f_{\rm FER}(V_A))$ is a monotonically increasing function of V_A. Therefore, the optimal value of V_A to obtain the maximum SKR can be found.

Finally, we substitute (8) into (4) to obtain $K^{\rm hom}_{\rm finite}(V_A) = f(V_A)^{\rm hom}$.

Likewise, for CV-QKD system with heterodyne detection, the system parameters [21] are set as $L = 25$ km, $\eta = 0.56$, $\xi = 0.022$, $v_{\rm el} = 0.042$, $\alpha = 0.2$ dB/km, $T = 0.3162$, and $R = 0.1$. The numerical relation of FER-V_A can be obtained in the same way. The curve fitting result of FER-V_A obtained with the fourth-order Gaussian function is shown in (9) and the corresponding fitting curve is shown in Figure 4(a). The curve of $f_{\chi^{\rm het}(y:E)}(V_A)$, $2R - f_{\chi^{\rm het}(y:E)}(V_A) + f_Q(V_A)$, and $\frac{n}{N}(1 - f_{\rm FER}(V_A))$ for no-switching protocol are shown in Figure 4(b) and Figure 5.

$$\begin{aligned} {\rm FER} &= f_{\rm FER}(V_A) \\ &= \begin{cases} 1, & 0 < V_A < 1.84, \\ -0.1987{\rm e}^{-(\frac{V_A-1.851}{0.01752})^2} - 0.8834{\rm e}^{-(\frac{V_A-1.854}{0.03432})^2} + 0 + 8727{\rm e}^{-(\frac{V_A-0.5462}{0.4082})^2}, & 1.84 \leqslant V_A \leqslant 2.02, \\ 0, & V_A > 2.02. \end{cases} \end{aligned} \tag{9}$$

Finally, we substitute (9) into (6) to obtain $K^{\rm het}_{\rm finite}(V_A) = f(V_A)^{\rm het}$.

2.3 Feasibility of the method

To calculate the optimal V_A, two kinds of information are needed: system parameters (T, ξ, η, and $v_{\rm el}$) and $f_{\rm FER}(V_A)$. The system parameters can be efficiently estimated in real time in the parameter estimation process. Although $f_{\rm FER}(V_A)$ is fitted numerically without analytic solutions, $f_{\rm FER}({\rm SNR})$ is only determined by the error correction matrix $\boldsymbol{H}$ and decoding method. After a specifically optimal $\boldsymbol{H}$ and the decoding method is chosen for a CV-QKD system under a certain transmission distance,

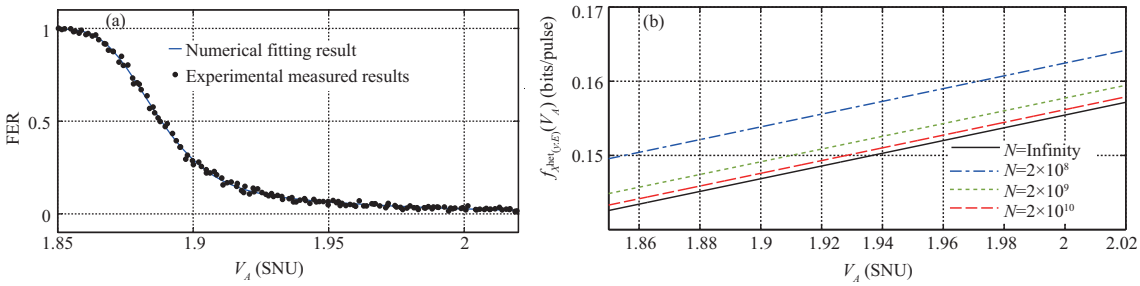

Figure 4 (Color online) (a) Experimental measurement results (black dots) and numerical fitting results (blue line) of FER-V_A with the no-switching protocol. (b) Simulation curves of $f_{\chi^{\rm het}(y:E)}(V_A)$ with the no-switching protocol. From top to bottom, the curves respectively show the results with the total block size of $N = 2 \times 10^8$, 2×10^9, 2×10^{10}, and ∞. The results show that both of them are proportional to V_A. The system parameters are set as follows: $L = 25$ km, $\eta = 0.56$, $\xi = 0.022$, $v_{\rm el} = 0.042$, $\alpha = 0.2$ dB/km, $T = 0.3162$, and $R = 0.1$. The number of iterations is 60.

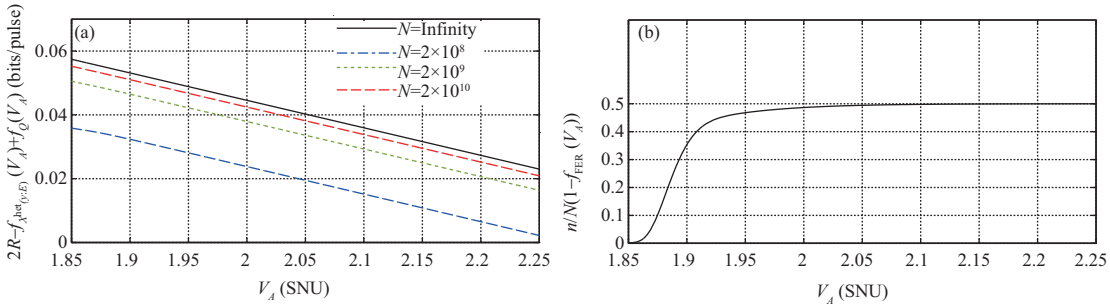

Figure 5 (Color online) (a) Simulation curves of $2R - f_{\chi^{\rm het}(y:E)}(V_A) + f_Q(V_A)$ with respect to V_A under the no-switching protocol. From bottom to top, the curves respectively show the results with the total block size of $N = 2 \times 10^8$, 2×10^9, 2×10^{10}, and ∞. The results show that both of them are inversely proportional to V_A. (b) The curve is $\frac{n}{N}(1 - f_{\rm FER}(V_A))$ with respect to V_A. The system parameters are set as follows: $\frac{n}{N} = 0.5$, $L = 25$ km, $\eta = 0.56$, $\xi = 0.022$, $v_{\rm el} = 0.042$, $\alpha = 0.2$ dB/km, $T = 0.3162$, and $R = 0.1$.

$f_{\rm FER}(\rm SNR)$ is only needs to be fitted numerically once, where collecting fitting curves with respect to all possible parameters is unnecessary. In a real CV-QKD experiment, $f_{\rm FER}(V_A)$ can be easily calculated in real time through the function $f_{\rm FER}(\rm SNR)$ and parameters (T, ξ, η, $v_{\rm el}$), where $\rm SNR = \frac{V_A \eta T}{\eta T \xi + v_{\rm det} + v_{\rm det} v_{\rm el}}$. Therefore, the proposed method can deal with the time-varying parameters, which can be effectively applied in a practical CV-QKD system.

3 Performance of the proposed optimization method

In the following, the performance of the optimization method is verified through a numerical simulation and experimental test, where a CV-QKD system with the GG02 protocol is implemented to present the optimization results experimentally.

3.1 Numerical simulation

In the numerical simulation, the block size N was set as 2×10^8, 2×10^9, 2×10^{10}, and ∞, and n was set to $N/2$. Then, by calculating the SKR under different V_A, the optimal $V_A^{\rm opt}$ under homodyne detection can be estimated, as shown in Figure 6. For the block sizes of 2×10^8, 2×10^9, 2×10^{10}, and ∞, $V_A^{\rm opt}$ was set as 2.7670, 2.8070, 2.8140, and 2.8165, and the corresponding optimal SKRs were 0.0007, 0.0060, 0.0078, and 0.0087 bits/pulse, respectively. The results show that $V_A^{\rm opt}$ gradually enhanced with the increase in N, but the change is almost negligible. Similarly, the simulation results under heterodyne detection are shown in Figure 7.

Taking $N = \infty$ as an example, the performance of our optimization method was compared with that of two frequently used optimization methods presented in [26, 33, 34, 36, 54]. In the first method, to adapt the code rates of various error correction matrices $\boldsymbol{H}$ under different transmission distances, V_A was accordingly adjusted to guarantee several fixed SNRs, which is referred to as the first method. In the second method, β and FER are assumed to be constant, and then V_A was optimized by maximizing

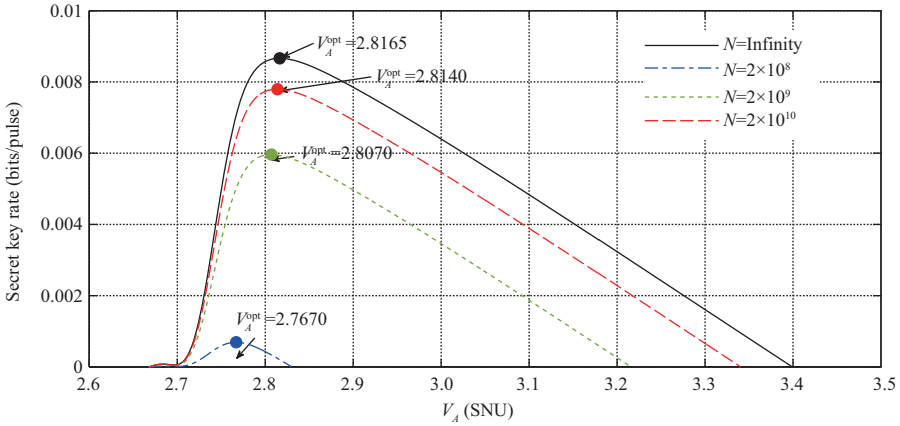

Figure 6 (Color online) Simulation curves of the SKR varying with V_A under the GG02 protocol. From bottom to top, the curves respectively show the results with the total block size of $N = 2 \times 10^8$, 2×10^9, 2×10^{10}, and ∞. V_A^{opt} are 2.7670, 2.8070, 2.8140, and 2.8165. The system parameters are set as follows: $L = 50$ km, $\eta = 0.606$, $\xi = 0.005$, $v_{\text{el}} = 0.041$, $\alpha = 0.2$ dB/km, $T = 0.1$, and $R = 0.1$.

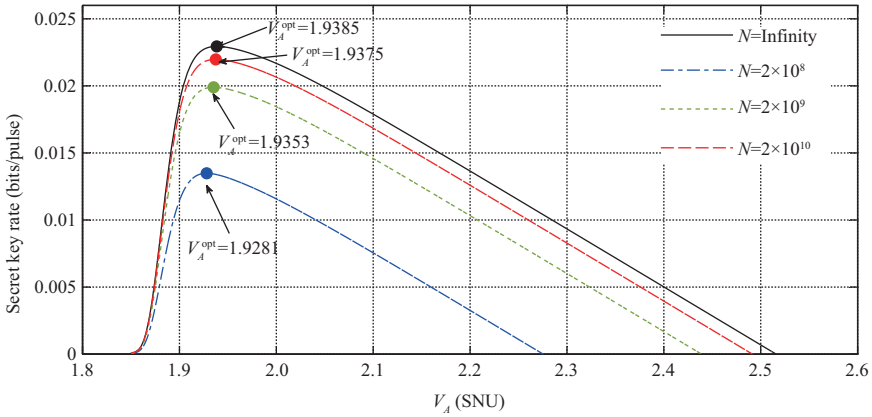

Figure 7 (Color online) Simulation curves of the SKR varying with V_A under the no-switching protocol. From bottom to top, the curves respectively show the results with the total block size of $N = 2 \times 10^8$, 2×10^9, 2×10^{10}, and ∞. V_A^{opt} are 1.9281, 1.9353, 1.9375, and 1.9385. The system parameters are set as follows: $L = 25$ km, $\eta = 0.56$, $\xi = 0.022$, $v_{\text{el}} = 0.042$, $\alpha = 0.2$ dB/km, $T = 0.3162$, and $R = 0.1$.

SKR, which is referred to as the second method. In the numerical simulation, for comparison, the same data reconciliation and error correction method were employed, and the simulation parameters were set as $L = 50$ km, $\eta = 0.606$, $\xi = 0.005$, $v_{\text{el}} = 0.041$, $\alpha = 0.2$ dB/km, $T = 0.1$, and $R = 0.1$. The simulation results are shown in Table 1. For the first method, the SNR was fixed as 0.161 with $\beta = 92.85\%$ and $V_A = 2.7665$. The experimentally verified result of the FER with our $\boldsymbol{H}$ in this case is 0.3192, and the SKR is 0.0070 bits/pulse. For the second method, β_0 and FER_0 were assumed to be 92% and 0.1, respectively. However, the optimization for V_A was performed without comprehensively considering the performance of the postprocessing. Consequently, the expected theoretical values of β and FER cannot be practically achieved. V_A^{opt} was 3.2193, the corresponding SNR was 0.1874, and the experimentally verified β was 80.71%, resulting in an SKR of 0.0029 bits/pulse. Finally, for the method proposed in this work, the SKR was 0.0087 bits/pulse while comprehensively considering the influence of V_A on the FER and β. Accordingly, an improvement of 24.29% and 200% compared with the first and second methods, respectively, was achieved. By calculating the PLOB bound [56], the SKR optimization result of our method achieved an improvement of 0.9443 and 4.7713 dB compared with the first and second methods, respectively.

We further analyzed the fluctuation of V_A^{opt} with different ξ, v_{el}, and R. The simulation results in Figure 8(a) show that V_A^{opt} and the corresponding maximized SKR decrease as ξ increases. Within the fluctuation range of ξ, the change in V_A^{opt} is very small. The simulation results in Figure 8(b) show that the V_A^{opt} increases as v_{el} increases and the corresponding SKR decreases. Within the fluctuation range

Table 1 Comparison of SKR optimization results with different methods[a)]

	R	V_A	β (%)	SNR	FER	SKR (bit/pulse)	Improvement (%)
Method 1 [33, 34]	0.1	2.7665	92.85	0.1610	0.3192	0.0070	24.29
Method 2 [26, 36, 54]	0.1	3.2193	80.71	0.1874	0.0000	0.0029	200
Our work	0.1	2.8165	91.34	0.1639	0.0872	0.0087	–

a) For method one, the SNR is fixed in 0.161 with $\beta = 92.85\%$. For method two, the β_0 and FER_0 are expected value of β and FER, which are assumed to be 92% and 0.1, respectively. R: code rate. The system parameters are set as: $L = 50$ km, $\eta = 0.606$, $\xi = 0.005$, $v_{\mathrm{el}} = 0.041$, $\alpha = 0.2$ dB/km, $T = 0.1$, and $R = 0.1$.

Table 2 The degree distribution functions of three error correction matrices with different R

R	Degree distribution function	Threshold
0.05	$v = 0.04r_1x_1^2x_2^{34} + 0.03r_1x_1^3x_2^{34} + 0.93r_1x_3$ $u = 0.01x_1^8 + 0.01x_1^9 + 0.41x_2^2x_3 + 0.52x_2^3x_3$	3.674
0.1	$v = 0.0775r_1x_1^2x_2^{20} + 0.0475r_1x_1^3x_2^{22} + 0.875r_1x_3$ $u = 0.0025x_1^{11} + 0.0225x_1^{12} + 0.03x_2^2x_3 + 0.845x_2^3x_3$	2.541
0.15	$v = 0.0858r_1x_1^2x_2^{12} + 0.0996r_1x_1^3x_2^{14} + 0.8146r_1x_3$ $u = 0.0160x_1^{10} + 0.0194x_1^{16} + 0.0198x_2^2x_3 + 0.7948x_2^3x_3$	2.038

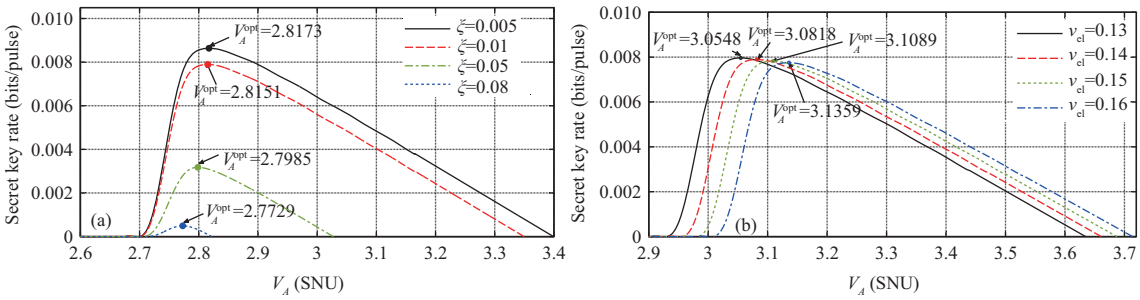

Figure 8 (Color online) Simulation results of the SKR with respect to V_A optimization in homodyne detection: $\eta = 0.606$, $\alpha = 0.2$ dB/km, $R = 0.1$, $L = 50$ km. (a) $v_{\mathrm{el}} = 0.041$, $\xi = 0.005$, 0.01, 0.05, 0.08 from top to bottom. The results of V_A^{opt} are 2.8173, 2.8151, 2.7985, and 2.7729. (b) $\xi = 0.005$, $v_{\mathrm{el}} = 0.13$, 0.14, 0.15, 0.16 from left to right. The results of V_A^{opt} are 3.0548, 3.0818, 3.1089, and 3.1359.

of v_{el}, the change in the SKR is also very small. The above results indicate that our method is robust even if the system parameters fluctuate slightly in real time.

The optimal choice of $\boldsymbol{H}$ is a complex problem. To verify the systematic optimization method between V_A and $\boldsymbol{H}$ choice, the density evolution method [57] was chosen to generate the degree distribution function for $R = 0.05$, 0.1, 0.15, as shown in Table 2. Then, the progressive-edge-growth algorithm [58] was chosen to generate the matrix $\boldsymbol{H}$ according to the degree distribution functions, whose FERs were experimentally measured and fitted with a nonlinear function similar to the results in (8) and (9). The SKR of a CV-QKD system with different $\boldsymbol{H}$ at a transmission distance of 50 km is shown in Figure 9, where the number of iterations is 60. Based on the above simulation results, to gain the maximum SKR, the matrices with $R = 0.1$ are the best choice. However, for a practical CV-QKD system, the optimal V_A influences not only the SKR but also the difficulty in quantum state preparation, measurement, and postprocessing. Accordingly, the proposed method in this paper provides a tool to calculate the cost quantitatively if the matrices with the maximum SKR are not chosen.

3.2 Experimental verification

We built a CV-QKD system with the GG02 protocol to verify the proposed methods experimentally, as shown in Figure 10. At Alice's side, a pulse light was separated into LO light and signal light by an asymmetrical Mach-Zehnder interferometer (AMZI), where the x and p quadratures of the signal light are modulated with a Gaussian distribution by an AM and phase modulator A (PM-A). Based on polarization-multiplexing and time-multiplexing methods, the signal light was cotransmitted with LO light to Bob through a fiber channel. At Bob's side, the time and polarization de-multiplexing between LO and signal light was realized by a DPC, PBS, and matched AMZI. Then, Bob randomly measured either x or p quadrature of signal light by a shot-noise-limited homodyne detector. The output signal of

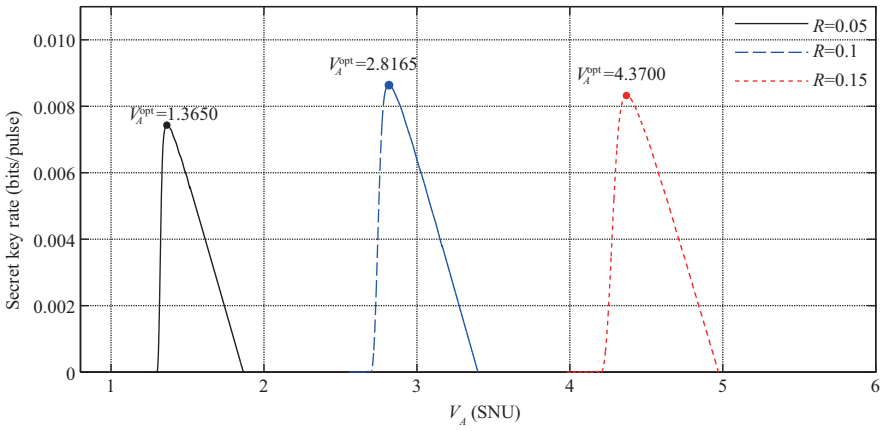

Figure 9 (Color online) SKR with respect to V_A optimization under different code rate error corrections in homodyne detection: $v_{el} = 0.041$, $\eta = 0.606$, $\alpha = 0.2$ dB/km, $L = 50$ km, $\xi = 0.005$, and $R = 0.05$, 0.1, 0.15 from left to right. The results of V_A^{opt} are 1.3650, 2.8165, and 4.3700. The result of the SKR is 0.0074, 0.0086, and 0.0083 bits/pulse, respectively.

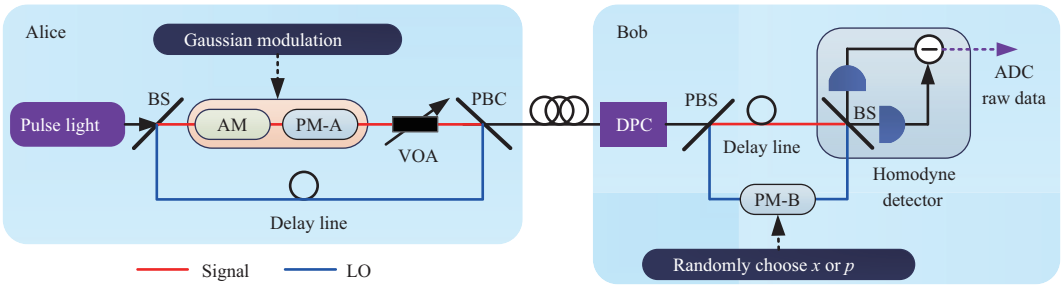

Figure 10 (Color online) Sketch of the CV-QKD system based on the GG02 protocol. PM-A/PM-B: phase modulator A/B; DPC: dynamic polarization controller; ADC: analog-to-digital converter.

the homodyne detector, which is proportional to the modulation value of the quadrature for signal light, was acquired by an ADC to obtain the raw data.

In our experiment, the transmission distance was 50 km, the block size N was set as 128×10^6, and n was set as $N/2$. The initial system parameters were estimated from the first data block, where $T = 0.1$, $v_{el} = 0.1465$, $\eta = 0.51$, $R = 0.1$, and $\xi = 0.0324$, which simulated the first launch of the CV-QKD system in a practical optical fiber condition. Based on the proposed method, the optimal value can be calculated, where $V_A^{opt} = 3.6608$. Then, we adjusted the modulation variance to V_A^{opt}. However, an inevitable slight parameter fluctuation could occur after the modification of the modulation variance, and we also cannot control V_A with arbitrary accuracy in the experiment, where the system parameters in the second block turn to $T = 0.1$, $v_{el} = 0.1507$, $\eta = 0.51$, $R = 0.1$, $V_A = 3.6588$, and $\xi = 0.0321$. The obtained SKR for the second data was $K_{experiment}^{opt} = 0.00380$ bits/pulse (red dot). As shown in Figure 11, the blue line is the optimized curve based on the first data block parameters, where $V_A^{opt} = 3.6608$ and the ideal theoretical optimal SKR $K_{first}^{opt} = 0.00385$ bits/pulse. The dashed line is the optimized curve based on the second data block parameters, where $V_A^{opt} = 3.6746$ and the ideal theoretical optimal SKR $K_{second}^{opt} = 0.00386$ bits/pulse. By comparing $K_{experiment}^{opt}$, K_{first}^{opt}, and K_{second}^{opt}, the deviation of the experimentally obtained SKR is <1.6%, which shows that the proposed method is feasible and robust for a practical system even with parameter fluctuations, and the available optimized result is very close to the ideal theoretical result.

4 Conclusion

In conclusion, we propose a systematic optimization method for a practical CV-QKD system with a restricted capacity of postprocessing, and the feasibility was verified theoretically and experimentally. Our simulation results show that the SKR can be improved by 24% and 200% with the proposed method compared with previous frequently used optimization methods with a transmission distance of 50 km.

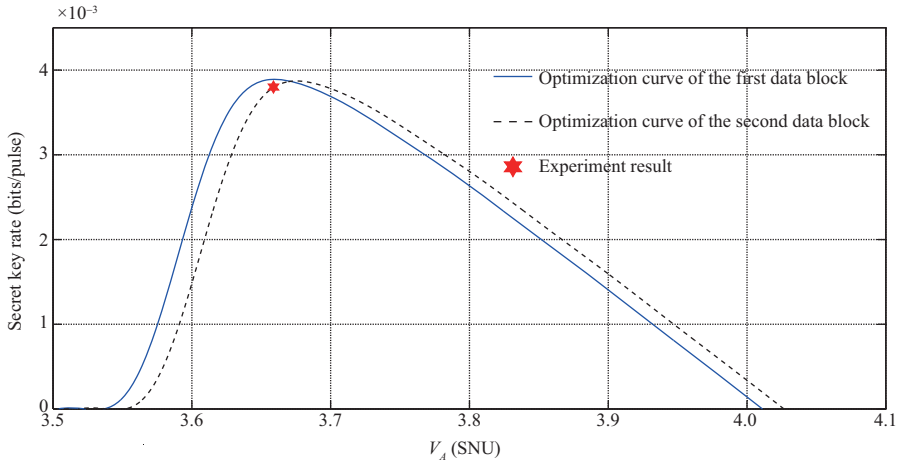

Figure 11 (Color online) Experiment results of the SKR with respect to V_A optimization. The parameters based on the first data block: $T = 0.1$, $v_{\mathrm{el}} = 0.1465$, $\eta = 0.51$, $R = 0.1$, and $\xi = 0.0324$. The parameters based on the second data block: $T = 0.1$, $v_{\mathrm{el}} = 0.1507$, $\eta = 0.51$, $R = 0.1$, $V_A = 3.6588$, $\xi = 0.0321$, and $K^{\mathrm{opt}}_{\mathrm{experiment}} = 0.00380$ bits/pulse (red dot). The blue line is the optimized curve based on the first data block parameters, where $V_A^{\mathrm{opt}} = 3.6608$ and $K^{\mathrm{opt}}_{\mathrm{first}} = 0.00385$ bits/pulse, and the dashed line is the optimized curve based on the second data block parameters for reference, where $V_A^{\mathrm{opt}} = 3.6746$ and $K^{\mathrm{opt}}_{\mathrm{second}} = 0.00386$ bits/pulse.

The experimental results demonstrate that the method is feasible and robust to be applied in an actual CV-QKD system, where the deviation between the experimentally obtained SKR and the ideal optimal value is <1.6% under system parameter fluctuation. Furthermore, the selection of optimal error correction matrices was studied with the proposed method, which provides a quantitative method to calculate the cost of the SKR if suboptimal matrices are chosen to reduce the decoding complexity in a practical CV-QKD system. This paper presents a method to improve the performance of CV-QKD systems in the field without modification of the hardware, which paves the way to deploy high-performance CV-QKD in the real world. Our method can also be effectively combined with other theoretical optimization methods, such as rate-adaptive algorithms, postselection, and add noise methods, which can be studied in the future.

Acknowledgements This work was supported in part by National Key Research and Development Program of China (Grant No. 2020YFA0309704), National Natural Science Foundation of China (Grant Nos. U19A2076, 62101516, 62171418, 62201530), Sichuan Science and Technology Program (Grant Nos. 2022ZYD0118, 2022YFG0330, 2022ZDZX0009), Basic Research Program of China (Grant No. JCKY2021210B059), Chengdu Key Research and Development Support Program (Grant No. 2021-YF05-02430-GX).

References

1 Pirandola S, Andersen U L, Banchi L, et al. Advances in quantum cryptography. Adv Opt Photon, 2020, 12: 1012–1236
2 Xu F, Ma X, Zhang Q, et al. Secure quantum key distribution with realistic devices. Rev Mod Phys, 2020, 92: 025002
3 Ren S, Wang Y, Su X. Hybrid quantum key distribution network. Sci China Inf Sci, 2022, 65: 200502
4 Joshi S K, Aktas D, Wengerowsky S, et al. A trusted node-free eight-user metropolitan quantum communication network. Sci Adv, 2020, 6: eaba0959
5 Su X, Wang M, Yan Z, et al. Quantum network based on non-classical light. Sci China Inf Sci, 2020, 63: 180503
6 Wang S, Yin Z Q, He D Y, et al. Twin-field quantum key distribution over 830-km fibre. Nat Photon, 2022, 16: 154–161
7 Lu C Y, Cao Y, Peng C Z, et al. Micius quantum experiments in space. Rev Mod Phys, 2022, 94: 035001
8 Zhang G W, Chen W, Fan-Yuan G J, et al. Polarization-insensitive quantum key distribution using planar lightwave circuit chips. Sci China Inf Sci, 2022, 65: 200506
9 Fan-Yuan G J, Chen W, Lu F Y, et al. A universal simulating framework for quantum key distribution systems. Sci China Inf Sci, 2020, 63: 180504
10 Bennett C H, Brassard G. Quantum cryptography: public key distribution and coin tossing. In: Proceedings of IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, 1984. 175–179
11 Ekert A K. Quantum cryptography based on Bell's theorem. Phys Rev Lett, 1991, 67: 661–663
12 Grosshans F, Grangier P. Continuous variable quantum cryptography using coherent states. Phys Rev Lett, 2002, 88: 057902
13 Weedbrook C, Lance A M, Bowen W P, et al. Quantum cryptography without switching. Phys Rev Lett, 2004, 93: 170504
14 Lupo C, Ottaviani C, Papanastasiou P, et al. Continuous-variable measurement-device-independent quantum key distribution: composable security against coherent attacks. Phys Rev A, 2018, 97: 052327
15 Weedbrook C, Pirandola S, García-Patrón R, et al. Gaussian quantum information. Rev Mod Phys, 2021, 84: 621–669
16 Jouguet P, Kunz-Jacques S, Leverrier A, et al. Experimental demonstration of long-distance continuous-variable quantum key distribution. Nat Photon, 2013, 7: 378–381
17 Diamanti E, Leverrier A. Distributing secret keys with quantum continuous variables: principle, security and implementations. Entropy, 2015, 17: 6072–6092
18 Guo H, Li Z, Yu S, et al. Toward practical quantum key distribution using telecom components. Fundamental Res, 2021, 1: 96–98

19 Zhang Y, Li Z, Chen Z, et al. Continuous-variable QKD over 50 km commercial fiber. Quantum Sci Technol, 2019, 4: 035006
20 Zhang G, Haw J Y, Cai H, et al. An integrated silicon photonic chip platform for continuous-variable quantum key distribution. Nat Photon, 2019, 13: 839–842
21 Wang H, Pi Y, Huang W, et al. High-speed Gaussian-modulated continuous-variable quantum key distribution with a local local oscillator based on pilot-tone-assisted phase compensation. Opt Express, 2020, 28: 32882
22 Wang H, Li Y, Pi Y, et al. Sub-Gbps key rate four-state continuous-variable quantum key distribution within metropolitan area. Commun Phys, 2022, 5: 162
23 Pan Y, Wang H, Shao Y, et al. Experimental demonstration of high-rate discrete-modulated continuous-variable quantum key distribution system. Opt Lett, 2022, 47: 3307–3310
24 Wang X, Liu W, Wang P, et al. Experimental study on all-fiber-based unidimensional continuous-variable quantum key distribution. Phys Rev A, 2017, 95: 062330
25 Ren S, Yang S, Wonfor A, et al. Demonstration of high-speed and low-complexity continuous variable quantum key distribution system with local local oscillator. Sci Rep, 2021, 11: 9454
26 Huang D, Huang P, Lin D, et al. Long-distance continuous-variable quantum key distribution by controlling excess noise. Sci Rep, 2016, 6: 19201
27 Jain N, Chin H M, Mani H, et al. Practical continuous-variable quantum key distribution with composable security. Nat Commun, 2022, 13: 4740
28 Chin H M, Jain N, Zibar D, et al. Machine learning aided carrier recovery in continuous-variable quantum key distribution. npj Quantum Inf, 2021, 7: 20
29 Jain N, Derkach I, Chin H M, et al. Modulation leakage vulnerability in continuous-variable quantum key distribution. Quantum Sci Technol, 2021, 6: 045001
30 Lodewyck J, Debuisschert T, Tualle-Brouri R, et al. Controlling excess noise in fiber-optics continuous-variable quantum key distribution. Phys Rev A, 2005, 72: 762–776
31 Qi B, Lim C C W. Noise analysis of simultaneous quantum key distribution and classical communication scheme using a true local oscillator. Phys Rev Appl, 2018, 9: 054008
32 Shao Y, Wang H, Pi Y, et al. Phase noise model for continuous-variable quantum key distribution using a local local oscillator. Phys Rev A, 2021, 104: 032608
33 Jouguet P, Kunz-Jacques S, High performance error correction for quantum key distribution using polar codes. Quantum Inf Comput 2014, 14: 329
34 Milicevic M, Feng C, Zhang L M, et al. Quasi-cyclic multi-edge LDPC codes for long-distance quantum cryptography. npj Quantum Inf, 2018, 4: 21
35 Mani H, Gehring T, Grabenweger P, et al. Multiedge-type low-density parity-check codes for continuous-variable quantum key distribution. Phys Rev A, 2021, 103: 062419
36 Jouguet P, Kunz-Jacques S, Leverrier A. Long-distance continuous-variable quantum key distribution with a Gaussian modulation. Phys Rev A, 2011, 84: 062317
37 Li Q, Wen X, Mao H, et al. An improved multidimensional reconciliation algorithm for continuous-variable quantum key distribution. Quantum Inf Process, 2019, 18: 25
38 Jeong S, Ha J. Efficiently encodable multi-edge type LDPC codes for long-distance quantum cryptography. In: Proceedings of International Conference on Information and Communication Technology Convergence (ICTC), 2018. 720–724
39 Luby M G, Mitzenmacher M, Shokrollahi M A, et al. Improved low-density parity-check codes using irregular graphs. IEEE Trans Inform Theory, 2001, 47: 585–598
40 Jayasooriya S, Shirvanimoghaddam M, Ong L, et al. A new density evolution approximation for LDPC and multi-edge type LDPC codes. IEEE Trans Commun, 2016, 64: 4044–4056
41 Wang X Y, Zhang Y C, Li Z Y, el al. Efficient rate-adaptive reconciliation for continuous-variable quantum key distribution. Quantum Inf Comput 2017, 17: 1123–1134
42 Kreinberg S, Koltchanov I, Richter A. Adding artificial noise for code rate matching in continuous-variable quantum key distribution. 2019. ArXiv:1905.04925
43 Cheng J Y, Jiang X Q, Bai E J, et al. Rate adaptive reconciliation based on reed-solomon codes. In: Proceedings of the 6th International Conference on Communication, Image and Signal Processing (CCISP), 2021. 245–249
44 Zhang M, Hai H, Feng Y, et al. Rate-adaptive reconciliation with polar coding for continuous-variable quantum key distribution. Quantum Inf Process, 2021, 20: 318
45 Jeong S, Jung H, Ha J. Rate-compatible multi-edge type low-density parity-check code ensembles for continuous-variable quantum key distribution systems. npj Quantum Inf, 2022, 8: 1
46 Zhou C, Wang X, Zhang Y, et al. Continuous-variable quantum key distribution with rateless reconciliation protocol. Phys Rev Appl, 2019, 12: 054013
47 Symul T, Alton D J, Assad S M, et al. Security of post-selection based continuous variable quantum key distribution in the presence of Gaussian added noise. In: Proceedings of Quantum-Atom Optics Downunder, 2007
48 Fiurášek J, Cerf N J. Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution. Phys Rev A, 2012, 86: 060302
49 Walk N, Ralph T C, Symul T, et al. Security of continuous-variable quantum cryptography with Gaussian postselection. Phys Rev A, 2013, 87: 20303
50 García-Patrón R, Cerf N J. Continuous-variable quantum key distribution protocols over noisy channels. Phys Rev Lett, 2009, 102: 130501
51 Wang X, Zhang Y, Yu S, et al. High-speed implementation of length-compatible privacy amplification in continuous-variable quantum key distribution. IEEE Photon J, 2018, 10: 1–9
52 Pirandola S. Composable security for continuous variable quantum key distribution: trust levels and practical key rates in wired and wireless networks. Phys Rev Res, 2021, 3: 043014
53 Pirandola S. Limits and security of free-space quantum communications. Phys Rev Res, 2021, 3: 013279
54 Lodewyck J, Bloch M, García-Patrón R, et al. Quantum key distribution over 25 km with an all-fiber continuous-variable system. Phys Rev A, 2007, 76: 042305
55 Li Y, Zhang X, Li Y, et al. High-throughput GPU layered decoder of quasi-cyclic multi-edge type low density parity check codes in continuous-variable quantum key distribution systems. Sci Rep, 2020, 10: 14561
56 Pirandola S, Laurenza R, Ottaviani C, et al. Fundamental limits of repeaterless quantum communications. Nat Commun, 2021, 8: 15043

57 Jeong S, Ha J. On the design of multi-edge type low-density parity-check codes. IEEE Trans Commun, 2019, 67: 6652–6667
58 Hu X Y, Eleftheriou E, Arnold D M. Regular and irregular progressive edge-growth tanner graphs. IEEE Trans Inform Theory, 2005, 51: 386–398

Appendix A SKR calculation

In (1) and (5), $I^{\mathrm{hom/het}}(x:y)$ can be calculated as [52, 53]

$$f_{I^{\mathrm{hom/het}}(x:y)}(V_A) = I^{\mathrm{hom/het}}(x:y) = \frac{v_{\mathrm{det}}}{2}\log_2\left(\frac{V+\chi^f_{\mathrm{tot}}}{1+\chi^f_{\mathrm{tot}}}\right), \tag{A1}$$

where $V = V_A + 1$, and χ^f_{tot} represents the total noise referred to the channel input, $\chi^f_{\mathrm{tot}} = \chi^f_{\mathrm{line}} + \chi_{\mathrm{hom/het}}/T_{\mathrm{min}}$, and $\chi^f_{\mathrm{line}} = (1-T_{\mathrm{min}})/T_{\mathrm{min}} + \xi_{\mathrm{max}}$ is the total channel added noise referred to the channel input, and $\chi_{\mathrm{hom/het}} = v_{\mathrm{det}}(1+v_{\mathrm{el}})/\eta - 1$ is the total added noise introduced by the realistic homodyne/heterodyne detector referred to Bob's input. It is proved in [52, 53] that

$$T_{\mathrm{min}} = \frac{\tau_{\mathrm{min}}}{\eta} = \frac{\tau-\Delta\tau}{\eta} = \frac{\tau}{\eta} - \frac{2w}{\eta}\sqrt{\frac{2\tau^2 V_A + \tau\sigma_z^2}{m_p V_A}}, \tag{A2}$$

$$\xi_{\mathrm{max}} = \xi + \frac{2w\sigma_z^2}{\tau\sqrt{2m_p}}, \tag{A3}$$

where $\tau = \eta T$ and $\sigma_z^2 = \eta T\xi + v_{\mathrm{det}}v_{\mathrm{el}} + v_{\mathrm{det}}$. Alice and Bob randomly and jointly choose m of the N distributed signals for parameter estimation, and the corresponding $m_p = v_{\mathrm{det}}m$. v_{det} is the quantum duty ("qu-duty") associated with detection: $v_{\mathrm{det}} = 1$ for homodyne and $v_{\mathrm{det}} = 2$ for heterodyne. Confidence parameter w is determined by the tolerable error probability $\varepsilon_{\mathrm{pe}}$, which typically set as $w = 6.34$, $\varepsilon_{\mathrm{pe}} = 2^{-33}$ [52, 53].

$\chi^{\mathrm{hom/het}}(y:E)$ can be estimated as [52, 53]

$$f_{\chi^{\mathrm{hom/het}}(y:E)}(V_A) = \chi^{\mathrm{hom/het}}(y:E) = \sum_{i=1}^{2} G\left(\frac{\lambda_i - 1}{2}\right) - \sum_{i=3}^{5} G\left(\frac{\lambda_i - 1}{2}\right), \tag{A4}$$

where $G(x) = (x+1)\log_2(x+1) - x\log_2 x$, and λ_i are the symplectic eigenvalues of the covariance matrix γ_{AB} between Alice and Bob. $\lambda_{1,2}$ is given by

$$\lambda^2_{1,2} = \frac{1}{2}[A \pm \sqrt{A^2 - 4B}]. \tag{A5}$$

Similarly, the $\lambda_{3,4,5}$ is given by

$$\lambda^2_{3,4} = \frac{1}{2}[C \pm \sqrt{C^2 - 4D}], \quad \lambda_5 = 1. \tag{A6}$$

In GG02 protocol with homodyne detection,

$$\begin{aligned} A =& V^2(1-2T_{\mathrm{min}}) + 2T_{\mathrm{min}} + T^2_{\mathrm{min}}(V+\chi^f_{\mathrm{line}})^2, \\ B =& T^2_{\mathrm{min}}(V\chi^f_{\mathrm{line}} + 1)^2, \\ C =& \frac{V\sqrt{B} + T_{\mathrm{min}}(V+\chi^f_{\mathrm{line}}) + A\chi_{\mathrm{hom}}}{T_{\mathrm{min}}(V+\chi^f_{\mathrm{tot}})}, \\ D =& \frac{\sqrt{B}(V+\sqrt{B}\chi_{\mathrm{hom}})}{T_{\mathrm{min}}(V+\chi^f_{\mathrm{tot}})}, \end{aligned} \tag{A7}$$

and in the no-switching protocol with heterodyne detection,

$$\begin{aligned} A =& V^2(1-2T_{\mathrm{min}}) + 2T_{\mathrm{min}} + T^2_{\mathrm{min}}(V+\chi^f_{\mathrm{line}})^2, \\ B =& T^2_{\mathrm{min}}(V\chi^f_{\mathrm{line}} + 1)^2, \\ C =& \frac{1}{(T_{\mathrm{min}}(V+\chi^f_{\mathrm{tot}}))^2}[A\chi^2_{\mathrm{het}} + B + 1 + 2\chi_{\mathrm{het}}(V\sqrt{B} + T_{\mathrm{min}}(V+\chi^f_{\mathrm{line}})) + 2T_{\mathrm{min}}(V^2-1)], \\ D =& \left(\frac{V+\sqrt{B}\chi_{\mathrm{het}}}{T_{\mathrm{min}}(V+\chi^f_{\mathrm{tot}})}\right)^2. \end{aligned} \tag{A8}$$