SCIENCE CHINA
Information Sciences

August 2023, Vol. 66 180511:1–180511:2
https://doi.org/10.1007/s11432-022-3656-4

• LETTER •
Special Topic: Quantum Information

Secret key rate of continuous-variable quantum key distribution with finite codeword length

Yan FENG[1], Runhe QIU[1*], Kun ZHANG[2], Xue-Qin JIANG[1*], Meixiang ZHANG[3], Peng HUANG[4] & Guihua ZENG[4]

[1]*School of Information Science and Technology, Donghua University, Shanghai* 201620*, China;*
[2]*School of Electronics and Information, Soochow University, Suzhou* 215006*, China;*
[3]*School of Information Engineering, Yangzhou University, Yangzhou* 225127*, China;*
[4]*State Key Laboratory of Advanced Optical Communication Systems and Networks, Center of Quantum Sensing and Information Processing* (*QSIP*)*, Shanghai Jiao Tong University, Shanghai* 200240*, China*

Received 8 July 2022/Revised 11 September 2022/Accepted 6 December 2022/Published online 5 July 2023

Citation Feng Y, Qiu R H, Zhang K, et al. Secret key rate of continuous-variable quantum key distribution with finite codeword length. Sci China Inf Sci, 2023, 66(8): 180511, https://doi.org/10.1007/s11432-022-3656-4

In recent years, continuous-variable quantum key distribution (CV-QKD) has been proposed as a promising alternative to the most commonly implemented discrete-variable QKD [1]. A typical CV-QKD system includes mainly two phases: quantum transmission and post-processing. In the first phase, legitimate communicators Alice and Bob prepare and measure the coherent state through a private quantum channel, while they can obtain a weakly advantage over the eavesdropper Eve. To obtain the secret keys, Alice and Bob subsequently perform a post-processing phase that includes two main stages: reconciliation [2] and privacy amplification. Reconciliation has attracted much attention in recent years as it has a significant effect on the secret key rate and transmission distance of CV-QKD systems.

In CV-QKD, reconciliation is performed using an error correction code designed for a binary-input additive white Gaussian noise (BI-AWGN) channel, and the efficiency of the reconciliation can be measured by

$$\beta = \frac{R}{C(\eta)}. \tag{1}$$

Here, R is the rate of the error correction code, and $C(\eta)$ is the capacity at the signal-to-noise (SNR) η, which can be calculated by

$$C(\eta) = \frac{1}{2}\log_2(1+\eta). \tag{2}$$

Under ideal conditions, perfect error correction can be performed during reconciliation, and the theoretical secret key rate of the CV-QKD system is defined as follows:

$$K = \beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}, \tag{3}$$

where I_{AB} refers to the mutual information shared by legitimate parties, and χ_{BE} denotes the Holevo bound on the information leaked to Eve [3].

In practice, the entire frame with known errors must be discarded after decoding because it cannot be used as a secret key. Therefore, considering the frame error rate (FER) P_e, a more realistic expression for the secret key rate of the CV-QKD system is given by

$$K = (1-P_e)(\beta I_{\mathrm{AB}} - \chi_{\mathrm{BE}}). \tag{4}$$

It can be seen from (4) that both the reconciliation efficiency and reconciliation FER affect the secret key rate.

The channel capacity obtained using (2) is the maximum rate at which information can be transmitted under the condition of infinite codeword length. However, in practice, the codeword length cannot be infinite, and it is insufficient to consider only the SNR when calculating the channel capacity. In this study, we first calculated the channel capacity by considering the effect of the finite codeword length using (5). Then, the reconciliation efficiency with finite codeword length can be calculated using (6). Moreover, as the sphere-packing bound (SPB) of Shannon [4] provides the minimum SNR for a given FER to calculate the minimum channel capacity, the maximum reconciliation efficiency with finite codeword length can be obtained. Finally, the maximum secret key rate of the CV-QKD system with finite codeword length was obtained by substituting the SPB and maximum reconciliation efficiency into (4).

Let $C_{\mathrm{fin}}(\eta, n, P_e)$ denote the channel capacity considering the effect of codeword length n, SNR η, and FER P_e. According to [5], this satisfies

$$\begin{aligned} C_{\mathrm{fin}}(\eta, n, P_e) &= C(\eta) - \sqrt{\frac{V}{n}}Q^{-1}(P_e) + o\left(\frac{1}{\sqrt{n}}\right) \\ &\approx C(\eta) - \sqrt{\frac{V}{n}}Q^{-1}(P_e). \end{aligned} \tag{5}$$

Here, $V = \frac{\eta}{2}\frac{\eta+2}{(\eta+1)^2}\ln 2$, $Q^{-1}(\cdot)$ is the functional inverse of

* Corresponding author (email: qiurh@dhu.edu.cn, xqjiang@dhu.edu.cn)

the Q-function $Q(P_e)=\int_{P_e}^{+\infty}\frac{1}{\sqrt{2\pi}}\mathrm{e}^{-\frac{t^2}{2}}\mathrm{d}t$, and $o\big(\frac{1}{\sqrt{n}}\big)$ denotes that $\lim_{n\to\infty}\big(o\big(\frac{1}{\sqrt{n}}\big)/\frac{1}{\sqrt{n}}\big)=0$. The channel capacity obtained using (5) provides a more informative benchmark for a practical channel, and it is not contradictory to the traditional channel capacity analysis. Rather more accurately, it refines and strengthens the classical results as for any $P_e\in(0,1)$, we have $\lim_{n\to\infty}C_{\mathrm{fin}}(\eta,n,P_e)=C(\eta)$.

Note that the SNR value at which the reconciliation is performed depends on the FER value that can be tolerated by the CV-QKD system. Hereafter, the corresponding SNR for a given FER P_e is denoted by η_{p_e}. Therefore, for a given code, $C(\eta)$ and $C_{\mathrm{fin}}(\eta,n,P_e)$ are denoted as $C(\eta_{p_e})$ and $C_{\mathrm{fin}}(\eta_{p_e},n,P_e)$, respectively.

It should be noted that $\sqrt{\frac{V}{n}}Q^{-1}(P_e)$ indicates a gap between $C(\eta_{p_e})$ and $C_{\mathrm{fin}}(\eta_{p_e},n,P_e)$. This gap can be significant in practice, as for small n, $\sqrt{\frac{V}{n}}Q^{-1}(P_e)$ is large. Therefore, for a given code rate R, the reconciliation efficiency that is calculated using (1) is not accurate under the condition of finite codeword length. The reconciliation efficiency with finite codeword length should be calculated by

$$\beta_{\mathrm{fin}}=\frac{R}{C_{\mathrm{fin}}(\eta_{p_e},n,P_e)}. \tag{6}$$

Remark. The reconciliation efficiency β_{fin} relies on the codeword length n, FER P_e, and SNR η_{p_e}, which can be used to calculate the secret key rate of the CV-QKD system with finite codeword length.

An example comparing $C(\eta_{p_e})$ with $C_{\mathrm{fin}}(\eta_{p_e},n,P_e)$, β with β_{fin} is provided in Appendix A.

Shannon studied coding and decoding systems, and derived a classic lower bound, i.e., the SPB, on the FER. For codes with a specific codeword length n, SPB is derived as follows [4]:

$$P_e\geqslant P_t(\theta,\eta,n). \tag{7}$$

Here, $P_t(\theta,\eta,n)$ is the probability that an n-dimensional Gaussian random vector with mean $(\eta,0,\ldots,0)$ and covariance $I_{n\times n}$ (where $I_{n\times n}$ is an $n\times n$ identity matrix) falls outside an n-dimensional cone with a half-angle θ around its mean. The fractional solid angle within an n-dimensional cone with a half-angle θ can be denoted by $\Omega_n(\theta)$. The solid-angle function $\Omega_n(\theta)$ and the probability function $P_t(\theta,\eta,n)$ can be expressed as follows:

$$\Omega_n(\theta)=\int_0^{\theta}\frac{n-1}{n}\frac{\Gamma\left(\frac{n}{2}+1\right)}{\Gamma\left(\frac{n+1}{2}\right)\sqrt{\pi}}(\sin\phi)^{n-2}\,\mathrm{d}\phi, \tag{8}$$

and

$$P_t(\theta,\eta,n)=\int_{\theta}^{\pi}\frac{(n-1)(\sin\phi)^{n-2}}{2^{n/2}\sqrt{\pi}\Gamma\left(\frac{n+1}{2}\right)}\int_0^{\infty}s^{n-1}\mathrm{e}^{F}\mathrm{d}s\mathrm{d}\phi, \tag{9}$$

respectively, where $F=-(s^2+n\eta^2-2s\sqrt{n}\eta\cos\phi)/2$ and $\Gamma(\cdot)$ represents the gamma function. For simplicity, the SPB $P_t(\theta,\eta,n)$ is denoted by P_t in the remainder of this study.

Note that for a given n, the angle θ can be solved using (8), and SPB P_t can be solved using (9).

Substituting the exact function (9) into (7), the SPB for codes with a specific codeword length n can be written as follows:

$$P_e\geqslant P_t=\int_{\theta}^{\pi}\frac{(n-1)(\sin\phi)^{n-2}}{2^{n/2}\sqrt{\pi}\Gamma\left(\frac{n+1}{2}\right)}\int_0^{\infty}s^{n-1}\mathrm{e}^{F}\mathrm{d}s\mathrm{d}\phi. \tag{10}$$

It can be seen from (10) that the SPB is bounded by SNR η, codeword length n, and the value of angle θ, which can be calculated using (8).

The SPB can provide the minimum SNR, denoted by η_{p_t}, to achieve the given FER. The minimum SNR η_{p_t} can be employed to calculate the minimum channel capacity $C_{\mathrm{fin}}^{\min}(\eta_{p_t},n,P_t)$ using (5) when the channel capacity is calculated by considering the effect of the finite codeword length. Accordingly, the corresponding maximum reconciliation efficiency, $\beta_{\mathrm{fin}}^{\max}$, can be calculated using $R/C_{\mathrm{fin}}^{\min}(\eta_{p_t},n,P_t)$.

Remark. The maximum reconciliation efficiency $\beta_{\mathrm{fin}}^{\max}$ depends on the codeword length n, SPB P_t, and minimum SNR η_{p_t}, which leads to the maximum secret key rate of the CV-QKD system with finite codeword length.

An example comparing $C(\eta_{p_t})$ with $C_{\mathrm{fin}}^{\min}(\eta_{p_t},n,P_t)$, β with $\beta_{\mathrm{fin}}^{\max}$ is provided in Appendix B. The simulation result of the secret key rate with finite codeword length and the analysis result of the maximum secret key rate with finite codeword length are shown in Appendix C.

Acknowledgements This work was supported by National Natural Science Foundation of China (Grant No. 61971276), National Natural Science Foundation of Shanghai (Grant No. 20ZR1400700), Key R&D Program of Guangdong Province (Grant No. 2020B030304002), Shanghai Municipal Science and Technology Major Project (Grant No. 2019SHZDZX01), and Fundamental Research Funds for the Central Universities and Graduate Student Innovation Fund of Donghua University (Grant No. CUSF-DH-D-2020084).

Supporting information Appendixes A–C. The supporting information is available online at info.scichina.com and link.springer.com. The supporting materials are published as submitted, without typesetting or editing. The responsibility for scientific accuracy and content remains entirely with the authors.

References

1 Grosshans F, van Assche G, Wenger J, et al. Quantum key distribution using gaussian-modulated coherent states. Nature, 2003, 421: 238–241
2 Leverrier A, Alléaume R, Boutros J, et al. Multidimensional reconciliation for a continuous-variable quantum key distribution. Phys Rev A, 2008, 77: 042325
3 Fossier S, Diamanti E, Debuisschert T, et al. Improvement of continuous-variable quantum key distribution systems by using optical preamplifiers. J Phys B-At Mol Opt Phys, 2009, 42: 114014
4 Shannon C E. Probability of error for optimal codes in a Gaussian channel. Bell Syst Technical J, 1959, 38: 611–656
5 Polyanskiy Y, Poor H V, Verdu S. Channel coding rate in the finite blocklength regime. IEEE Trans Inform Theory, 2010, 56: 2307–2359