Title for citation

SCIENCE CHINA
Information Sciences

• Supplementary File •

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, and Center of Quantum Sensing and Information Processing (QSIP), Shanghai Jiao Tong University, Shanghai* 200240*, China*

Appendix A Reconciliation efficiency with finite codeword length

In this section, we provide an example that compares $C(\eta_{p_e})$ with $C_{\text{fin}}(\eta_{p_e}, n, P_e)$, β with β_{fin} for the CV-QKD system. The performance of FER P_e utilizing advanced television system committee (ATSC) LDPC codes [1] is shown in Figure A1. As the SNR η_{p_e} of the virtual channel can be very low, error correction codes that have low code rates need to be applied in the CV-QKD system [2,3]. In this paper, the code rate R is set to 2/15. For a more intuitive comparison, the codeword lengths are set to 16200, 64800, and 648000. Furthermore, the secret key rate is affected by P_e and β_{fin}. P_e and β_{fin} are related. When P_e is extremely high, the secret key rate is extremely low. When P_e is too low, β_{fin} is too low to result in $(\beta_{\text{fin}} I_{\text{AB}} - \chi_{\text{BE}}) < 0$. Therefore, P_e should not be too high or too low. We adopt the frequently used $P_e = 0.1$ [4] to ensure that the secret key rate is not too low and that β_{fin} is sufficiently high to make $(\beta_{\text{fin}} I_{\text{AB}} - \chi_{\text{BE}}) > 0$.

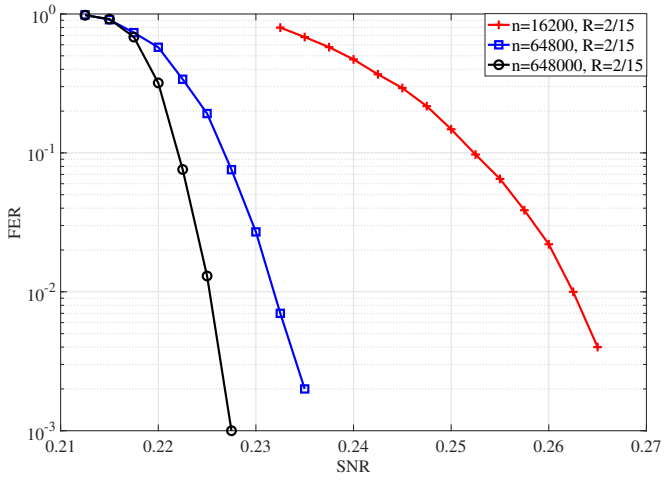

Figure A1 FER values utilizing ATSC LDPC codes with different codeword lengths and code rate $R = 2/15$.

It can be observed from Figure A1 that for a given SNR, the longer the codeword length, the lower the FER. From another perspective, for a given FER, the longer the codeword length, the lower is the SNR. For different codeword lengths and the given $P_e = 0.1$, we provide the channel capacities $C(\eta_{p_e})$ and $C_{\text{fin}}(\eta_{p_e}, n, P_e)$, and the corresponding reconciliation efficiencies β and β_{fin} in Table A1. As shown in the table, $C_{\text{fin}}(\eta_{p_e}, n, P_e)$ is lower than $C(\eta_{p_e})$. Accordingly, the reconciliation efficiency β_{fin} is higher than β. Furthermore, when the codeword length n increases, the gap between $C(\eta_{p_e})$ and $C_{\text{fin}}(\eta_{p_e}, n, P_e)$ decreases, as does the gap between β and β_{fin}. □

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

Table A1 The channel capacities $C(\eta_{p_e})$ and $C_{\text{fin}}(\eta_{p_e}, n, P_e)$, the corresponding reconciliation efficiencies β and β_{fin} for different codeword lengths and the given $P_e = 0.1$.

n	η_{p_e}	$C(\eta_{p_e})$	β	$C_{\text{fin}}(\eta_{p_e}, n, P_e)$	β_{fin}
16200	0.2524	0.1623	0.8213	0.1562	0.8538
64800	0.2266	0.1473	0.9050	0.1444	0.9236
648000	0.2217	0.1444	0.9231	0.1435	0.9291

Appendix B Maximum reconciliation efficiency with finite codeword length

In this example, we first provide the SPB values with different codeword lengths and code rate $R = 2/15$ in Figure B1. This clearly shows that under the same conditions, the SPB with codeword length $n = 648000$ is significantly lower than that with codeword lengths $n = 64800$ and $n = 16200$. Furthermore, the SPB values in Figure B1 are lower than the FER values in Figure A1.

SPB leads to the minimum SNR η_{p_t} which can be applied to calculating the minimum channel capacity. Accordingly, the maximum reconciliation efficiency can be obtained using the minimum channel capacity. For different codeword lengths and the given $P_t = 0.1$, we provide the channel capacity $C(\eta_{p_t})$ and minimum channel capacity $C_{\text{fin}}^{\min}(\eta_{p_t}, n, P_t)$ in Table B1. Correspondingly, the reconciliation efficiency β and maximum reconciliation efficiency $\beta_{\text{fin}}^{\max}$ are also calculated in Table B1. As shown in Table B1, the minimum channel capacity $C_{\text{fin}}^{\min}(\eta_{p_t}, n, P_t)$ decreases as the codeword length n increases. Accordingly, the maximum reconciliation efficiency $\beta_{\text{fin}}^{\max}$ increases as the codeword length n increases. Furthermore, the maximum reconciliation efficiency achieves 99.95% for $n = 648000$ and $P_t = 0.1$. □

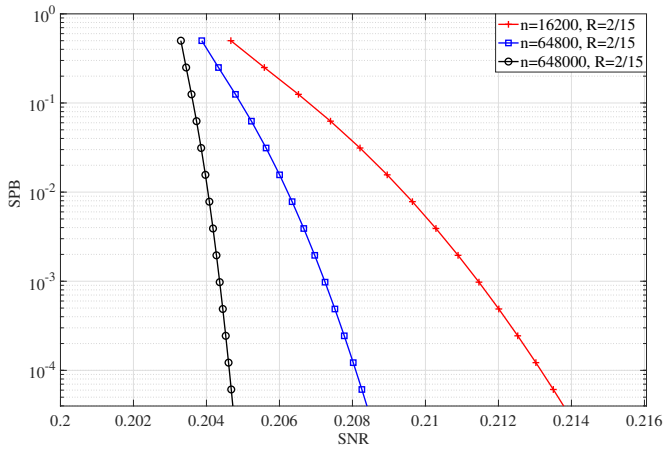

Figure B1 SPB values utilizing ATSC LDPC codes with different codeword lengths and code rate $R = 2/15$.

Table B1 The channel capacities $C(\eta_{p_t})$ and $C_{\text{fin}}^{\min}(\eta_{p_t}, n, P_t)$, the corresponding reconciliation efficiencies β and $\beta_{\text{fin}}^{\max}$ for different codeword lengths and the given $P_t = 0.1$.

n	η_{p_t}	$C(\eta_{p_t})$	β	$C_{\text{fin}}^{\min}(\eta_{p_t}, n, P_t)$	$\beta_{\text{fin}}^{\max}$
16200	0.2067	0.1355	0.9838	0.1338	0.9965
64800	0.2049	0.1345	0.9914	0.1336	0.9978
648000	0.2036	0.1337	0.9974	0.1334	0.9995

Appendix C Secret key rate of the CVQKD system with finite codeword length

In Appendix A and Appendix B, we know that for a given P_e, the reconciliation efficiency β_{fin} is more accurate than β, which assumes infinite codeword length when calculating the channel capacity. Consequently, the secret key rates K and K_{fin} can be obtained using β and β_{fin}, respectively. For a given P_t, the corresponding SNR η_{p_t} on the SPB curve can be used to calculate the minimum channel capacity $C_{\text{fin}}^{\min}(\eta_{p_t}, n, P_t)$. Therefore, the maximum reconciliation efficiency $\beta_{\text{fin}}^{\max}$ and the maximum secret key rate $K_{\text{fin}}^{\max}$ can also be obtained.

Figure C1 shows the secret key rate versus the transmission distance of the CV-QKD system with different codeword lengths for the given $P_e = 0.1$ and the values of reconciliation efficiency in Table A1. In general, the CV-QKD system has the following parameters: excess noise $\xi = 0.001$, detection efficiency $\kappa = 0.9$, electronic noise $V_{el} = 0.005$, and attenuation factor of the quantum channel $\varphi = 0.2$ dB/km [5]. As can be seen from Figure C1, for $n = 648000$, the secret key rate K_{fin} achieves 4×10^{-3} bits/pulse at 27.5 km, and K is approximately 1×10^{-3} bits/pulse at 27.5 km. This indicates that the secret key rate considering the effect of finite codeword length when calculating the channel capacity is higher than that obtained assuming infinite codeword length when calculating the channel capacity.

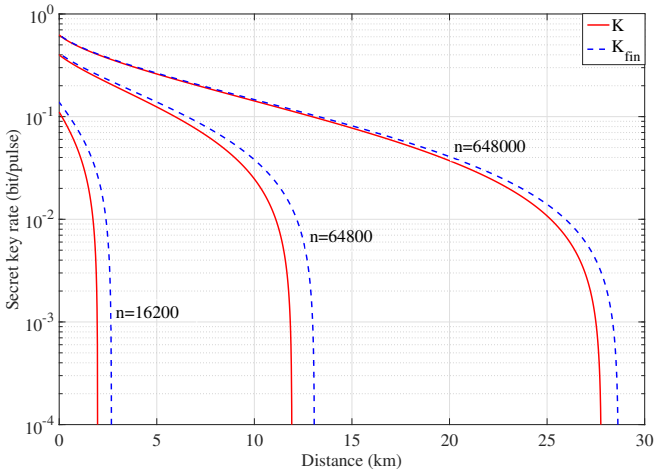

Figure C1 Secret key rate versus transmission distance of the CV-QKD system with different codeword lengths for $P_e = 0.1$. The parameters of the CV-QKD system are as follows: excess noise $\xi = 0.001$, detection efficiency $\kappa = 0.9$, electronic noise $V_{el} = 0.005$, and the attenuation factor of the quantum channel $\varphi = 0.2$ dB/km.

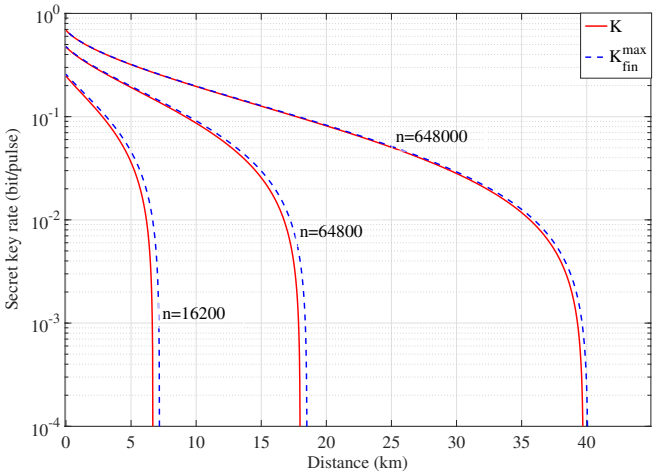

Figure C2 Secret key rate versus transmission distance of the CV-QKD system with different codeword lengths for $P_t = 0.1$. The parameters of the CV-QKD system are as follows: excess noise $\xi = 0.001$, detection efficiency $\kappa = 0.9$, electronic noise $V_{el} = 0.005$, and the attenuation factor of the quantum channel $\varphi = 0.2$ dB/km.

For the given $P_t = 0.1$, the reconciliation efficiencies $\beta_{\text{fin}}^{\max}$ and β are given in Table B1. Based on these results, Figure C2 depicts the corresponding maximum secret key rate $K_{\text{fin}}^{\max}$ and the secret key rate K versus the transmission distance of the CV-QKD system with different codeword lengths for the given $P_t = 0.1$. The parameters of the CV-QKD system are the same as those described in Fig. C1. As shown in Figure C2, the secret key rate $K_{\text{fin}}^{\max}$ is greater than K. Moreover, the maximum secret key rate $K_{\text{fin}}^{\max}$ is higher than 3×10^{-2} bits/pulse at 27.5 km when the codeword length n is 648000.

References

1 Kim K J, Myung S, Park S I, et al. Low-density parity- check codes for ATSC 3.0. IEEE Trans Broadcast, 2016, 62: 189-196
2 Zhang Y, Chen Z, Pirandola S, et al. Long-distance continuous-variable quantum key distribution over 202.81 km of fiber. Phys Rev Lett, 2020, 125: 010502
3 Zhang K, Jiang X-Q, Feng Y, et al. High efficiency continuous-variable quantum key distribution based on ATSC 3.0 LDPC codes. Entropy, 2020, 22: 1087
4 Jiang X-Q, Yang S Y, Huang P, et al. High-speed reconciliation for CVQKD based on spatially coupled LDPC codes. IEEE Photonics J, 2018, 10: 04
5 Feng Y, Wang Y-J, Qiu R, et al. Virtual channel of multidimensional reconciliation in a continuous-variable quantum key distribution. Phys Rev A, 2021, 103: 032603