High performance long-distance discrete-modulation continuous-variable quantum key distribution: supplementary document

This document provides supplementary information to "High performance long-distance discrete-modulation continuous-variable quantum key distribution", showing the calculation method of the secret key rate for discrete-modulation CVQKD.

1. SECRET KEY RATE

In our previous work [1], the DM CVQKD protocol studied by Jie Lin et al. [2] has been extended to the two ring multi-constellation protocol beyond quadrature phase shift keying (QPSK). In this work, we demonstrate the two-ring constellation modulation protocol with 16 signal states. The following is an introduction to this protocol and the method of calculating the security key rate.

First, Alice randomly prepares 16 coherent states $|\alpha_x\rangle = \left|\alpha_k e^{ix\pi/4}\right\rangle$ with two different amplitudes $\{\alpha_k\} = \{\alpha_1, \alpha_2\}$. The eight states in the inner ring $\left\{|\alpha_x\rangle = \left|\alpha_1 e^{ix\pi/4}\right\rangle\right\}_{x=0,1,\ldots,7}$ with amplitude α_1 are chosen with an equal probability p_1, and the eight states in the outer ring $\left\{|\alpha_x\rangle = \left|\alpha_2 e^{ix\pi/4}\right\rangle\right\}_{x=8,9,\ldots,15}$ with amplitude α_2 are chosen with an equal probability p_2. The values of p_1 and p_2 satisfy the relationship of $p_1 + p_2 = 1/8$. Next, Alice sends the prepared states to Bob via a quantum channel. After Bob received the states, he uses the heterodyne detector to measure them and get the measurement outcome $y = |y| e^{i\theta} \in \mathbb{C}$, where $\theta \in \left[-\frac{\pi}{8}, \frac{15\pi}{8}\right)$. The discretized raw keys z are obtained according to the key mapping rules as follows:

$$z = \begin{cases} j, & \text{if } \theta \in \left[\frac{(2j-1)\pi}{8}, \frac{(2j+1)\pi}{8}\right) \text{ and } |y| \in [0, \alpha_c) \\ j, & \text{if } \theta \in \left[\frac{(2j-17)\pi}{8}, \frac{(2j-15)\pi}{8}\right) \text{ and } |y| \in [\alpha_c, \infty) \end{cases}, \tag{S1}$$

where $j \in \{0, 1, \ldots, 15\}$ and α_c denotes the amplitude boundary between the inner and outer rings. The region operators are defined as follows [1, 2]:

$$R_j = \begin{cases} \frac{1}{\pi} \int_0^{\alpha_c} \int_{(2j-1)\pi/8}^{(2j+1)\pi/8} r \left|re^{i\theta}\right\rangle \left\langle re^{i\theta}\right| d\theta dr & j \in [0, 7] \\ \frac{1}{\pi} \int_{\alpha_c}^{\infty} \int_{(2j-17)\pi/8}^{(2j-15)\pi/8} r \left|re^{i\theta}\right\rangle \left\langle re^{i\theta}\right| d\theta dr & j \in [8, 15] \end{cases}. \tag{S2}$$

The post-selection process may improve the key rate and suppress the amount of raw key. In our previous work [1], it is shown that the optimal value of the post-selection parameter Δ_a is zero for the 12 states two-ring constellation modulation. In current work, we neglect the post-selection process.

With the reverse reconciliation, the asymptotic secret key rate against collective attacks is expressed as [1, 2]:

$$R^{\infty} = \min_{\rho_{AB} \in \mathcal{S}} D\left[\mathcal{G}\left(\rho_{AB}\right) \parallel \mathcal{Z}\left(\mathcal{G}\left(\rho_{AB}\right)\right)\right] - p_{\text{pass}} \delta_{EC}, \tag{S3}$$

where the set $\mathcal{S}$ contains all density operators compatible with experimental observations. In this formula, $D\left(\rho \parallel \sigma\right) = Tr\left(\rho \log_2 \rho\right) - Tr\left(\rho \log_2 \sigma\right)$ is the quantum relative entropy. The completely positive and trace nonincreasing map for postprocessing steps is defined as $\mathcal{G} = K\sigma K^{\dagger}$ with the post-processing map $K = \sum |j\rangle_R \otimes \mathbb{I}_A \otimes \left(\sqrt{R_j}\right)_B$. $\mathcal{Z}$ denotes a pinching quantum channel that reads out the result of key map and satisfies $\mathcal{Z}\left(\sigma\right) = \sum_{j=0}^{3} \left(|j\rangle \langle j|_R \otimes \mathbb{I}_{AB}\right) \sigma \left(|j\rangle \langle j|_R \otimes \mathbb{I}_{AB}\right)$. p_{pass}

is the sifting probability of data for key generation. δ_{EC} represents the leaked information of the per-signal pulse during the error correction phase and can be obtained as follows:

$$\begin{aligned}\delta_{\mathrm{EC}} &= H(Z) - \beta I(X:Z) \\ &= (1-\beta)H(Z) + \beta H(Z|X)\end{aligned}, \tag{S4}$$

where β denotes the reconciliation efficiency, and X and Z denote the raw key string of Alice and Bob, respectively. Based on the convex optimization approach [1, 2] and the two-step procedure [3], the optimization problem of the security key rate of our protocol can be numerically calculated.

REFERENCES

1. P. Wang, Y. Zhang, Z. Lu, X. Wang, and Y. Li, "Discrete-modulation continuous-variable quantum key distribution with a high key rate," New J. Phys. **25**, 023019 (2023).
2. J. Lin and N. Lütkenhaus, "Trusted detector noise analysis for discrete modulation schemes of continuous-variable quantum key distribution," Phys. Rev. Appl. **14**, 064030 (2020).
3. A. Winick, N. Lutkenhaus, and P. J. Coles, "Reliable numerical key rates for quantum key distribution," Quantum (2017).