Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier

Ying Guo, Renjie Li, Qin Liao [*], Jian Zhou, Duan Huang

School of Information Science and Engineering, Central South University, Changsha 410083, China

ARTICLE INFO

Article history:
Received 29 June 2017
Received in revised form 4 December 2017
Accepted 6 December 2017
Available online xxxx
Communicated by A. Eisfeld

Keywords:
Quantum key distribution
Discrete modulation
Continuous variable
Optical amplifier

ABSTRACT

Discrete modulation is proven to be beneficial to improving the performance of continuous-variable quantum key distribution (CVQKD) in long-distance transmission. In this paper, we suggest a construct to improve the maximal generated secret key rate of discretely modulated eight-state CVQKD using an optical amplifier (OA) with a slight cost of transmission distance. In the proposed scheme, an optical amplifier is exploited to compensate imperfection of Bob's apparatus, so that the generated secret key rate of eight-state protocol is enhanced. Specifically, we investigate two types of optical amplifiers, phase-insensitive amplifier (PIA) and phase-sensitive amplifier (PSA), and thereby obtain approximately equivalent improved performance for eight-state CVQKD system when applying these two different amplifiers. Numeric simulation shows that the proposed scheme can well improve the generated secret key rate of eight-state CVQKD in both asymptotic limit and finite-size regime. We also show that the proposed scheme can achieve the relatively high-rate transmission at long-distance communication system.

1. Introduction

As quantum technology develops, more and more real-world applications of quantum technology have been emerging. One of the most advanced applications is quantum cryptography [1]. Quantum key distribution (QKD) [2,3] is a branch of quantum cryptography that allows two distant legitimate partners, Alice and Bob, to share an one-time pad sequence of bits, namely a random secure key, over an insecure quantum channel controlled by an eavesdropper Eve.

Generally, QKD can be classified into two types, i.e. discrete-variable (DV) QKD, e.g. the Bennett–Brassard 1984 ($BB84$) protocol [4], and continuous-variable (CV) QKD [5,6]. DVQKD encodes information in properties of single photon pulses while CVQKD encodes key bits in the quadratures ($\hat{x}$ and $\hat{p}$) of the optical field. Compared with the DVQKD, CVQKD offers higher secret key rate, thus it spotlights a huge number of researchers. Up till now, various CVQKD protocols are proposed such as $GG02$ protocol [7], squeezed-state protocol [8], unidimensional protocol [9], no-switching protocol [10], entangle source-in-the-middle (ESIM) protocol [11] and measurement-device-independent (MDI) [12,13] protocol, as well as several experiments are realized [14–16]. Most of the above-mentioned protocols belong to Gaussian-modulated CVQKD [17–19], which is the most extensively applied in CVQKD and its unconditional security proofs in both collective attacks and coherent attacks [20,21] has been proposed [7]. However, Gaussian-modulated CVQKD is now facing the problem of transmission in the long-distance range compared with its DVQKD counterpart [22]. Theoretically, the overall signal-to-noise ratio (SNR) drops rapidly as transmission distance increases. Thus, this deterioration of channel conditions directly results in a rapid reduction of reconciliation efficiency. Unfortunately, Gaussian-modulated CVQKD can not break the limitation of low SNR or obtain high reconciliation efficiency under low SNR [22]. To break this limitation, discretely-modulated CVQKD protocol has been proposed [23] and its unconditional security proof has been shown in [23,24]. Thereinto, four-state CVQKD protocol has been implemented theoretically and experimentally [25]. Recently, a better discretely-modulated scheme with higher secret key rate and longer transmission distance, called eight-state protocol, was proposed [22], which improves the secret key rate and its transmission distance achieves more than 100 kilometers [26].

Since the discretely-modulated eight-state protocol exhibits excellent performance at low SNR, we further improve its capability by applying an optical amplifier (OA) [27]. The proposed scheme (eight-state protocol with an optical amplifier) can enhance the generated secret key rate of eight-state protocol by compensating

[*] Corresponding author.
E-mail address: llqqlq@csu.edu.cn (Q. Liao).

https://doi.org/10.1016/j.physleta.2017.12.011
0375-9601/© 2017 Elsevier B.V. All rights reserved.

Please cite this article in press as: Y. Guo et al., Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier, Phys. Lett. A (2018), https://doi.org/10.1016/j.physleta.2017.12.011

the imperfection of the detector at Bob's side with only slight cost of transmission distance.

The performance of proposed scheme in asymptotic limit and finite-size regime is investigated. In asymptotic limit, we mainly focus on improvement of secret key rate and the trend of transmission distance reduction. In detail, we quantify and analyze the improvement of secret key rate by defining a novel parameter, improvement ratio, and thereby find that the OA has totally different effects on secret key rate under different transmission distance. As a result, a parameter called critical transmission distance is used to define the maximum transmission distance where OA exerts positive influence upon the performance of eight-state protocol. In finite-size regime, we obtain more practical result of the proposed scheme.

This paper is organized as follows: in Sec. 2 we give the description of eight-state protocol and detail the proposed eight-state scheme with an optic amplifier. Numerical simulation and discussion are shown in Sec. 3. Conclusion is drawn in Sec. 4. Detailed derivation of equations is included in the Appendix.

2. Eight-state CVQKD with an optical amplifier

In this section, we mainly elaborate discretely-modulated eight-state CVQKD protocol with an optical amplifier. To make the derivation self-contained, we briefly introduce the original eight-state CVQKD protocol first.

2.1. Eight-state CVQKD protocol

Alice first prepares eight coherent displaced states

$$|\beta_k\rangle = |\alpha e^{\frac{k\pi}{4}}\rangle\ ,\ k \in \mathbb{Z}, \tag{1}$$

where α is chosen to be a positive real number and $\mathbb{Z} = \{0, 1, 2, ..., 7\}$. Alice then randomly sends one of these eight coherent states to Bob with equal probability through an insecure quantum channel controlled by an eavesdropper called Eve. The quantum channel is characterized by the excess noise ϵ and the transmission efficiency T. The total noise added to Bob's input by effects of quantum channel can be expressed by $\chi_{line} = 1/T + \epsilon - 1$.

After receiving the state sent by Alice, Bob subsequently performs homodyne detection or heterodyne detection. Since Bob's apparatus is imperfect, detection efficiency η can hardly achieve 1 which denotes the perfect detection. Moreover, Bob's detector also introduces some thermal noise υ_{el} when Bob measures the received state. Taking effect of detection efficiency η and thermal noise υ_{el} into account, one can derive a conclusive quantity χ_h, where $\chi_{hom} = [(1-\eta) + \upsilon_{el}]/\eta$ and $\chi_{het} = [1 + (1-\eta) + 2\upsilon_{el}]/\eta$ are the case of homodyne detection and heterodyne detection, respectively. Consequently, the total quantity of noise χ_{tot} can be described as $\chi_{tot} = \chi_{line} + \chi_h/T$.

Finally, Alice and Bob share a string of the secret key by using error correction and privacy amplification.

Since the PM version is equal to the entanglement-based (EB) version, which is more convenient for security analysis. In EB version, Alice prepares a pure two-mode state,

$$|\Phi_8\rangle = \frac{1}{4}\sum_{k=0}^{7} |\psi_k\rangle|\beta_k\rangle, \tag{2}$$

where the states

$$|\psi_k\rangle = \frac{1}{2}\sum_{m=0}^{7} e^{\frac{i(4k+1)m\pi}{4}} |\phi_k\rangle, k \in \mathbb{Z}, \tag{3}$$

are orthogonal non-Gaussian states.

The state $|\phi_k\rangle$ could be described as follows,

$$|\phi_k\rangle = \frac{e^{-\frac{\alpha^2}{2}}}{\sqrt{\lambda_k}} \sum_{n=0}^{\infty} e^{\frac{\alpha^{(8n+k)}}{\sqrt{(8n+k)!}}} |8n+k\rangle,\ k \in \mathbb{Z} \tag{4}$$

where

$$\begin{aligned}
\lambda_{0(4)} &= \frac{1}{4}e^{-\alpha^2}[\cosh(\alpha^2) + \cos(\alpha^2) \pm 2\cos(\frac{\alpha^2}{\sqrt{2}})\cosh(\frac{\alpha^2}{\sqrt{2}})], \\
\lambda_{1(5)} &= \frac{1}{4}e^{-\alpha^2}[\sinh(\alpha^2) + \sin(\alpha^2) \pm 2\cos(\frac{\alpha^2}{\sqrt{2}})\sinh(\frac{\alpha^2}{\sqrt{2}}) \\
&\quad \pm \sqrt{2}\sin(\frac{\alpha^2}{\sqrt{2}})\cosh(\frac{\alpha^2}{\sqrt{2}})], \\
\lambda_{2(6)} &= \frac{1}{4}e^{-\alpha^2}[\cosh(\alpha^2) - \cos(\alpha^2) \pm 2\sin(\frac{\alpha^2}{\sqrt{2}})\sinh(\frac{\alpha^2}{\sqrt{2}})], \\
\lambda_{3(7)} &= \frac{1}{4}e^{-\alpha^2}[\sinh(\alpha^2) - \sin(\alpha^2) \mp 2\cos(\frac{\alpha^2}{\sqrt{2}})\sinh(\frac{\alpha^2}{\sqrt{2}}) \\
&\quad \pm \sqrt{2}\sin(\frac{\alpha^2}{\sqrt{2}})\cosh(\frac{\alpha^2}{\sqrt{2}})].
\end{aligned} \tag{5}$$

Alice prepares the entangled state $|\Phi_8\rangle$ with variance $V = V_a + 1$ and $V_a = 2\alpha^2$, where she implements projective measurements on one of the set $|\psi_k\rangle\langle\psi_k|$ for $k \in \mathbb{Z}$ to the first half of $|\Phi_8\rangle$ and projects the second half of set $|\psi_k\rangle\langle\psi_k|$ on one of the eight coherent states $|\beta_k\rangle$. After modulation, the modulated state is sent to Bob through an untrusted quantum channel. The covariance matrix of modulated state can be expressed by

$$\gamma_8 = \begin{bmatrix} V I_2 & Z_8\sigma_Z \\ Z_8\sigma_Z & V I_2 \end{bmatrix}, \tag{6}$$

where $V = V_a + 1$, $I_2 = \text{diag}[1, 1]$, $\sigma_Z = \text{diag}[1, -1]$, and the covariance $Z_8 = V_a \sum_{k=0}^{7} \lambda_{k-1}{}^{\frac{3}{2}} \lambda_k{}^{-\frac{1}{2}}$.

Bob's detection efficiency is modeled by a beam splitter with transmission efficiency η. An EPR state with variance N_d is used to model the thermal noise υ_{el} that is introduced by the process of Bob's detector, where $N_d = \eta\chi_{hom}/(1-\eta)$ is for homodyne detection and $N_d = (\eta\chi_{het} - 1)/(1-\eta)$ is for heterodyne detection.

After that, Bob implements the reverse reconciliation and privacy amplification to generate the final bit string of secret key shared with Alice.

2.2. The improved eight-state scheme with an optical amplifier

Due to the imperfection in Bob's apparatus, the detection process cannot be ideal, thus final secret key rate is lower than expectation. Fortunately, the impact of imperfect apparatus can be reduced by applying an optical amplifier. In what follows, we elaborate the proposed eight-state CVQKD with an optical amplifier placed at Bob's side. Fig. 1 shows the Entanglement-based (EB) version of the proposed scheme against Eve's collective attacks.

Firstly, Alice prepares an entangled state $|\Phi_8\rangle$. After modulation, one mode of modulated state with variance $V = V_a + 1$ is sent to Bob through an insecure quantum channel.

After the quantum channel, the mode go through an optical amplifier placed in input of Bob's apparatus and is detected by Bob's apparatus. In the viewpoint of calculating secret key rate, this can be deemed trusted detection noise [28]. Here we mainly take two types of OA: phase-sensitive amplifier (PSA) and phase-insensitive amplifier (PIA) into consideration, as shown in the light green box of Fig. 1, these two types of optical amplifiers are described as follows.

Please cite this article in press as: Y. Guo et al., Performance improvement of eight-state continuous-variable quantum key distribution with an optical amplifier, Phys. Lett. A (2018), https://doi.org/10.1016/j.physleta.2017.12.011