Physics Letters A ••• (••••) •••–•••

Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

High-dimensional quantum key distribution with the entangled single-photon-added coherent state

Yang Wang [a,b], Wan-Su Bao [a,b,*], Hai-Ze Bao [a,b], Chun Zhou [a,b], Mu-Sheng Jiang [a,b], Hong-Wei Li [a,b]

[a] Zhengzhou Information Science and Technology Institute, Zhengzhou, 450001, China
[b] Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

ARTICLE INFO

Article history:
Received 13 November 2016
Received in revised form 24 January 2017
Accepted 30 January 2017
Available online xxxx
Communicated by A. Eisfeld

Keywords:
Quantum key distribution
High-dimensional
Single-photon-added coherent state

ABSTRACT

High-dimensional quantum key distribution (HD-QKD) can generate more secure bits for one detection event so that it can achieve long distance key distribution with a high secret key capacity. In this Letter, we present a decoy state HD-QKD scheme with the entangled single-photon-added coherent state (ESPACS) source. We present two tight formulas to estimate the single-photon fraction of postselected events and Eve's Holevo information and derive lower bounds on the secret key capacity and the secret key rate of our protocol. We also present finite-key analysis for our protocol by using the Chernoff bound. Our numerical results show that our protocol using one decoy state can perform better than that of previous HD-QKD protocol with the spontaneous parametric down conversion (SPDC) using two decoy states. Moreover, when considering finite resources, the advantage is more obvious.

1. Introduction

Quantum key distribution (QKD) enables two remote parties, Alice and Bob, to generate secret keys with proven theoretically unconditional security. Since the first proposal was made based on polarization photons [1], QKD has developed into a diverse research direction [2,3]. The topic on improving the secret key rate and the transmission distance of QKD is paid close attention. To solve this problem, one promising way is high-dimensional quantum key distribution (HD-QKD). Compared with qubit-based QKD protocols [1], HD-QKD can encode multiple bits of secret key to each photon and provide more resistance to noise [4]. Moreover, HD-QKD protocols can use entangled photon pairs, which can be used to improve significantly the range of QKD by means of quantum repeaters. These considerations motivate the research of HD-QKD.

In the last decade, HD-QKD has been developed observably in both theory and experimental demonstration. Various HD-QKD protocols can apply a variety of photonic degrees of freedom and these schemes have been experimentally demonstrated by encoding information based on the linear transverse momentum [5], the orbital angular momentum (OAM) [6,7], time-energy entanglement [8–14]. Among them, HD-QKD protocols based on time-energy entanglement are promising candidates for implementations because HD-QKD protocols have been rigorously proven to be secure and time-energy correlations are robust in present telecommunications infrastructure and compatible with wavelength division multiplexing networks.

HD-QKD protocols based on the time-energy entanglement have been proposed based on time-to-frequency conversion [12], dispersive optics [13], and Franson and conjugate-Franson interferometers [14]. Specially, by using time–frequency covariance matrix (TFCM) to bound Eve's Holevo information, proposals in Refs. [13,14] have been proven to be secure against Gaussian collective attacks. In the experimental implementation with security against Gaussian collective attacks, Lee et al. [10] have demonstrated the proposal based on dispersive optics and Zhong et al. [11] have demonstrated the proposal based on a Franson interferometer.

In these HD-QKD experiments, the source is assumed that it only generates single-pair emissions. However, in practical implementation of HD-QKD, there are inevitably some imperfections. One of main imperfections is the imperfect source. Multipair emissions of the source can make the HD-QKD protocol assailable to the photon number splitting (PNS) attack [15,16]. Fortunately, the decoy-state method [17–19] can figure out the PNS attack and improve the performance of practical QKD systems. Therefore, Bunandar et al. [20] extended the decoy-state method to the HD-QKD protocol based on dispersive optics and presented its security analysis with one or two decoy states. For the practical

* Corresponding author at: Zhengzhou Information Science and Technology Institute, Zhengzhou, 450001, China.
E-mail address: 2010thzz@sina.com (W.-S. Bao).

http://dx.doi.org/10.1016/j.physleta.2017.01.058
0375-9601/© 2017 Published by Elsevier B.V.

problem on finite resources, the finite-key analysis for the decoy-state HD-QKD protocol based on dispersive optics was presented for collective attacks [21] and general attacks [22], respectively. In order to improve the protocol's performance, the detector-decoy method was introduced into the HD-QKD and a new scheme was proposed [23]. Meanwhile, other ways that can enhance the performance of decoy-state HD-QKD protocol should be further studied.

In order to improve the secret key rate and the transmission distance of QKD, one effective way is exploiting a source with a high single-photon probability. For example, different photon sources [24–28] are used to improve the performance of decoy state measurement-device-independent quantum key distribution (MDI-QKD) protocols [29]. Among these, a promising candidate is the single-photon-added coherent state (SPACS) [30], which has sub-Poissonian statistics in photon number distribution and possesses higher single-photon probability. Results in [28] showed that both the secret key rate and the transmission distance can be improved by using SPACS. Moreover, Zavatta et al. [31,32] have successfully experimentally generated the SPACS. The SPACS has various applications in quantum information because it can also produce entangled states [33,34]. Superposition of SPACS has been applied to quantum teleportation and QKD [35]. In previous decoy state HD-QKD protocol, the entanglemented photon pairs are generated by the process of spontaneous parametric down conversion (SPDC). The Poisson photon-number distribution of this source limits the secret key capacity (in bits per coincidence) and the secret key rate (in bits per second). Hence, it is interested to apply a source with a high single-photon probability to HD-QKD. In this Letter, we introduce the entangled single-photon-added coherent state (ESPACS) into the decoy-state HD-QKD based on dispersive optics. It is expected that the ESPACS can be alternatively applied to improve the performance of the HD-QKD protocol. Our results show that our proposal with only one decoy state could outperform the previous decoy-state HD-QKD in terms of secret key rates and transmission distances.

The rest of this paper is organized as follows. In Sec. 2, we introduce the description of our protocol. In Sec. 3, we present the security analysis for the protocol without and with statistical fluctuations. The numerical simulations are shown in Sec. 4 and the conclusion is summarized in Sec. 5.

2. Protocol description

In previous decoy state HD-QKD protocol, the time-energy entanglement is always generated by the SPDC process. Zavatta et al. [31,32] used a conditional preparation technique by the SPDC process to generate SPACS. Specifically, SPACS can be generated by injecting a coherent state $|\alpha\rangle$ into the signal mode of an optical parametric amplifier. The conditional preparation of the target state can take place every time that a single photon is detected in the correlated idler mode. That means photons between signal states and idler states are correlated in time domain. In the ideal condition, the energy should be constant that is correlated with mean photon numbers. Though a coherent state is injected into the signal mode, the energy between signal states and idler states is still anti-correlated. The time-energy entanglement of photon generated by SPDC is not broken. So combining with techniques in experimental demonstrations of time-energy entangled HD-QKD, it is possible to implement the SPACS into the time-energy entangled HD-QKD.

The decoy-state HD-QKD based on dispersive optics works as follows [13,20]:

a. Biphoton preparation and transmission: In each round, Alice generates entangled photon pairs from the ESPACS source. She also modulates the intensity $\lambda \in \{\mu, \nu\}$ at random with probabilities p_μ and $p_\nu = 1 - p_\mu$, respectively, where μ is the signal setting, ν is the decoy setting. She retains one of photon pairs and sends the other to Bob through the quantum channel. Here, the number of alphabet characters per photon pulse is $d = \sigma_{coh}/\sigma_{cor}$, where σ_{cor} is the correlation time between two photons, σ_{coh} is the coherence time of the pump field, which is always larger than σ_{cor}.

b. Measurement: Alice and Bob measure their photons by randomly and independently choosing one of two bases (the time basis T and the conjugate-time basis W) with probabilities p_T and $p_W = 1 - p_T$, respectively.

c. Post-processing: After all N signals are distributed, Alice and Bob publicly announce their lists of bases and intensity choices via an authenticated classical channel. They retain the measurement outcome using the same bases and discard the measurement outcome using mismatched bases. The secret key is extracted only from the events whereby Alice and Bob both select the T basis, while Eve's information is estimated from the events whereby Alice and Bob both select the W) basis. Using the detailed security analysis presented below, Alice and Bob could estimate their information advantage over Eve. If this is less than zero, they abort the protocol. Otherwise, they apply the error correction process and the privacy amplification process to generate the secret key.

3. Security analysis

3.1. Parameter estimation without statistical fluctuations

In the decoy state HD-QKD based on dispersive optics, the probability of Alice and Bob recording at least one detection event, which is also called postselection probability P_λ, can be expressed as [20]

$$P_\lambda = \sum_{k=0}^{\infty} P_k(\lambda) C_k, \tag{1}$$

where P_λ is the probability of sending k-photon pairs, λ is the intensity of Alice's source, and C_k is the conditional probability of measuring at least one detection event when Alice sends k-photon pairs, which can be written as [20]

$$C_k = [1 - (1 - p_d)(1 - \eta_A)^k][1 - (1 - p_d)(1 - \eta_B t)^k]. \tag{2}$$

Here, p_d is Alice's and Bob's dark count rate, η_A and η_B are their detection efficiencies, t is the fiber transmittance between Alice and Bob.

In HD-QKD with SPDC source, when the SPDC source is weakly pumped, the photon number statistics of an SPDC source statistics approaches the Poissonian distribution [20]. Analogously, we can control and make the statistics of the distribution to approach the statistics of the non-entangled SPACS source in theory. So in our scheme, we assume that the photon number distribution of Alice's ESPACS source, which is also the probability of sending k-photon pairs, is given by [28]

$$P_k(\lambda) = \frac{e^{-|\alpha|^2}}{1 + |\alpha|^2} \frac{|\alpha|^{2(k-1)} k}{(k-1)!} = \frac{e^{-\zeta}}{1 + \zeta} \frac{\zeta^{k-1} k}{(k-1)!} (k \geq 1), \tag{3}$$

where λ is the intensity of Alice's ESPACS source, $\zeta = |\alpha|^2$ is the intensity of the initial coherent state and the relation between λ and ζ is expressed by

$$\zeta = \left(\sqrt{\lambda^2 - 2\lambda + 5} + \lambda - 3\right)/2. \tag{4}$$

When the key length is infinite, the bound on the secret key capacity (in bits per coincidence) is expressed as [20]

$$\Delta I \geq \beta I(A;B) - (1 - F_\lambda) n_R - F_\lambda \chi^{\mathrm{U}}_{\xi_t, \xi_\omega}(A;E), \tag{5}$$