ARTICLE IN PRESS

[Physics Letters A](http://dx.doi.org/10.1016/j.physleta.2017.01.058) ••• (••••) •••-•••

Contents lists available at [ScienceDirect](http://www.ScienceDirect.com/) 1 67

\mathbb{P}^n and \mathbb{P}^n are \mathbb{P}^n

www.elsevier.com/locate/pla

11 Uigh dimensional quantum loy distribution with the entangled $\frac{11}{12}$ High-dimensional quantum key distribution with the entangled $\frac{77}{78}$ ¹³ single-photon-added coherent state and the state of the state

 15 V₁₀ W₁₀ a¹, W₁₀ S₁₁ R₂₀ a¹, 15 K₁₁ Z₀ R₂₀ a¹, C_{h11} Zh₀₁₁ a¹, Ch₁₁ Ch₀ng Linga¹, ¹⁵ Yang Wang ^{a,b}, Wan-Su Bao ^{a,b,∗}, Hai-Ze Bao ^{a,b}, Chun Zhou ^{a,b}, Mu-Sheng Jiang ^{a,b}, and the same of the same o 17 83 Hong-Wei Li ^a*,*^b

18 84 ^a *Zhengzhou Information Science and Technology Institute, Zhengzhou, 450001, China*

¹⁹ Synergetic Innovation Center of Quantum Information and Quantum Physics, University of Science and Technology of China, Hefei, Anhui 230026, China

22 ARTICLE INFO ABSTRACT 88

23 89 *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

24 Article history: **Example 20 Terms** High-dimensional quantum key distribution (HD-QKD) can generate more secure bits for one detection 90 25 Received 13 November 2016 100 event so that it can achieve long distance key distribution with a high secret key capacity. In this 91 26 between the use of the letter, we present a decoy state HD-QKD scheme with the entangled single-photon-added coherent state 92
Accepted 30 January 2017 27 Available online xxxx
events and Eve's Holevo information and derive lower bounds on the secret key capacity and the secret 28 Communicated by A. Eisteld
34 key rate of our protocol. We also present finite-key analysis for our protocol by using the Chernoff bound. 29 **Reywords:** 29 **29 Example 20 29 Our numerical results show that our protocol using one decoy state can perform better than that of** 30 96 previous HD-QKD protocol with the spontaneous parametric down conversion (SPDC) using two decoy ³¹ High-dimensional states. Moreover, when considering finite resources, the advantage is more obvious. ⁹⁷ (ESPACS) source. We present two tight formulas to estimate the single-photon fraction of postselected

32 Single-photon-added coherent state the state of th

1. Introduction

40 106 Alice and Bob, to generate secret keys with proven theoretically 41 107 unconditional security. Since the first proposal was made based ⁴² on polarization photons [\[1\],](#page--1-0) QKD has developed into a diverse re- sion multiplexing networks. 43 search direction [\[2,3\].](#page--1-0) The topic on improving the secret key rate health protocols based on the time-energy entanglement 109 ⁴⁴ and the transmission distance of OKD is paid close attention. To have been proposed based on time-to-frequency conversion [\[12\],](#page--1-0) 110 45 solve this problem, one promising way is high-dimensional quan-
 46 112 tum key distribution (HD-QKD). Compared with qubit-based QKD 47 protocols [\[1\],](#page--1-0) HD-QKD can encode multiple bits of secret key to the CIFCM) to bound Eve's Holevo information, proposals in Refs. [13, the title] ⁴⁸ each photon and provide more resistance to noise [\[4\].](#page--1-0) Moreover, $\frac{14}{}$ have been proven to be secure against Gaussian collective at-
 49 HD-QKD protocols can use entangled photon pairs, which can be tacks. In the experimental implementation with security against 118 50 used to improve significantly the range of QKD by means of quan-
16 and the realisation collective attacks, Lee et al. [10] have demonstrated the range of the range of the ran ⁵¹ tum repeaters. These considerations motivate the research of HD- proposal based on dispersive optics and Zhong et al. [11] have 117 52 OKD 118 and the proposal based on a Franson interferometer. 118 Quantum key distribution (QKD) enables two remote parties, and the transmission distance of QKD is paid close attention. To QKD.

E-mail address: 2010thzz@sina.com (W.-S. Bao).

64 130 <http://dx.doi.org/10.1016/j.physleta.2017.01.058>

 65 $0375-9601$ / \odot 2017 Published by Elsevier B.V.

66 and the contract of the con

37 **1. Introduction 1. Introduction 103 10** 38 104 energy entanglement are promising candidates for implementa-39 Cuantum key distribution (OKD) enables two remote parties. Itions because HD-QKD protocols have been rigorously proven to be 105 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 dispersive optics [\[13\],](#page--1-0) and Franson and conjugate-Franson interferometers [\[14\].](#page--1-0) Specially, by using time–frequency covariance matrix (TFCM) to bound Eve's Holevo information, proposals in Refs. [\[13,](#page--1-0) [14\]](#page--1-0) have been proven to be secure against Gaussian collective attacks. In the experimental implementation with security against Gaussian collective attacks, Lee et al. [\[10\]](#page--1-0) have demonstrated the proposal based on dispersive optics and Zhong et al. [\[11\]](#page--1-0) have

53 In the last decade, HD-QKD has been developed observably in these HD-QKD experiments, the source is assumed that it 54 in both theory and experimental demonstration. Various HD-QKD only generates single-pair emissions. However, in practical imple-
 55 protocols can apply a variety of photonic degrees of freedom and mentation of HD-QKD, there are inevitably some imperfections. 121 ⁵⁶ these schemes have been experimentally demonstrated by encod-
122 57 ing information based on the linear transverse momentum $[5]$, sions of the source can make the HD-QKD protocol assaulable 123 58 the orbital angular momentum (OAM) [\[6,7\],](#page--1-0) time-energy entan-
 58 the orbital angular momentum (OAM) [6,7], time-energy entan-59 125 the decoy-state method [\[17–19\]](#page--1-0) can figure out the PNS attack 60 126 and improve the performance of practical QKD systems. There- $\overline{}$ $\overline{}$ $\overline{}$ $\overline{}$ for $\overline{}$ for $\overline{}$ and hor at: Thengzhou Information Science and Technology Insti-
 $\overline{}$ for $\overline{}$ Bunandar et al. [\[20\]](#page--1-0) extended the decoy-state met 62 tute, Zhengzhou, 450001, China. The second based on dispersive optics and presented its se-

HD-QKD protocol based on dispersive optics and presented its se-

128 63 F-mail address: 2010thzz@sina.com (W.-S. Bao). The states are curity analysis with one or two decoy states. For the practical 129 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 [\[15,16\].](#page--1-0) Fortunately,

8 74 9 року процесси в селото на 1950 година в 1950 година
В 1950 година в 1950 годин 10 76 14 80 20 and the contract of the con 21 века в област в о 33 99 34 100 35 36 102

Corresponding author at: Zhengzhou Information Science and Technology Institute, Zhengzhou, 450001, China.

ARTICLE IN PRESS

mance of decoy-state HD-QKD protocol should be further studied.

 8 In order to improve the secret key rate and the transmission basis T and the conjugate-time basis W) with probabilities p_T and $^{-74}$ ⁹ distance of QKD, one effective way is exploiting a source with $p_W = 1 - p_T$, respectively. ¹⁰ a high single-photon probability. For example, different photon **c. Post-processing:** After all N signals are distributed, Alice and ⁷⁶ ¹¹ sources [\[24–28\]](#page--1-0) are used to improve the performance of decoy Bob publicly announce their lists of bases and intensity choices 77 ¹² state measurement-device-independent quantum key distribution via an authenticated classical channel. They retain the measure- 78 ¹³ (MDI-QKD) protocols [\[29\].](#page--1-0) Among these, a promising candidate is ment outcome using the same bases and discard the measurement 79 ¹⁴ the single-photon-added coherent state (SPACS) [\[30\],](#page--1-0) which has all outcome using mismatched bases. The secret key is extracted only 80 ¹⁵ sub-Poissonian statistics in photon number distribution and pos-
¹⁵ sub-Poissonian statistics in photon number distribution and pos-
from the events whereby Alice and Bob bath select the T basis, ¹⁶ sesses higher single-photon probability. Results in [\[28\]](#page--1-0) showed while Eve's information is estimated from the events whereby Al- ⁸² ¹⁷ that both the secret key rate and the transmission distance can ice and Bob both select the W) basis. Using the detailed security 83 ¹⁸ be improved by using SPACS. Moreover, Zavatta et al. [\[31,32\]](#page--1-0) have analysis presented below, Alice and Bob could estimate their infor- 84 ¹⁹ successfully experimentally generated the SPACS. The SPACS has mation advantage over Eve. If this is less than zero, they abort the ⁸⁵ ²⁰ various applications in quantum information because it can also protocol. Otherwise, they apply the error correction process and ⁸⁶ ²¹ produce entangled states [\[33,34\].](#page--1-0) Superposition of SPACS has been the privacy amplification process to generate the secret key. 87 22 88 applied to quantum teleportation and QKD [\[35\].](#page--1-0) In previous de-²³ coy state HD-QKD protocol, the entanglemented photon pairs are $\,$ 3. Security analysis $\,$ ²⁴ generated by the process of spontaneous parametric down conver-²⁵ sion (SPDC). The Poisson photon-number distribution of this source $\frac{31}{2}$ Parameter estimation without statistical fluctuations ⁹¹ ²⁶ limits the secret key capacity (in bits per coincidence) and the se-**2022 12.1 and the secret secret we** 22 ²⁷ cret key rate (in bits per second). Hence, it is interested to apply a state headed was the HD-OKD based on dispersive ontics the prob-²⁸ a source with a high single-photon probability to HD-QKD. In this ability of Alice and Bob recording at least one detection event ⁹⁴ 29 Letter, we introduce the entangled single-photon-added coherent which is also called postselection probability P_2 can be expressed 30 state (ESPACS) into the decoy-state HD-QKD based on dispersive $\frac{1}{25}$ [20] 31 97 optics. It is expected that the ESPACS can be alternatively applied ³² to improve the performance of the HD-QKD protocol. Our results ∞ ∞ 33 show that our proposal with only one decoy state could outper- $P_{\lambda} = \sum_{i} P_{k}(\lambda) C_{k}$, (1) 99 34 form the previous decoy-state HD-QKD in terms of secret key rates $k=0$ 35 and transmission distances. $\frac{101}{201}$ is the probability of earlier the prince $\frac{1}{2}$ is the $\frac{101}{201}$ In order to improve the secret key rate and the transmission

36 102 The rest of this paper is organized as follows. In Sec. 2, we intensity of Alice's course and C is the conditional probability of 37 introduce the description of our protocol. In Sec. 3, we present $\frac{36}{2}$ measuring at least one detection with then like ends helten that 38 the security analysis for the protocol without and with statistical $\frac{1}{2}$ in the security as $\frac{1}{2}$ is the security analysis of the protocol without and with statistical $\frac{1}{2}$ is the security of $\frac{1}{2}$ in 39 fluctuations. The numerical simulations are shown in Sec. [4](#page--1-0) and $\frac{1}{2}$ and $\frac{1}{2}$ multiple in the strict is $\frac{1}{2}$ multiple in the strict is $\frac{1}{2}$ multiple in the strict is $\frac{1}{2}$ multiple in the strict 40 106 the conclusion is summarized in Sec. [5.](#page--1-0)

2. Protocol description

⁴⁴ In previous decoy state HD-QKD protocol, the time-energy and Bob. The state of the state of the state the state $\frac{110}{2}$ ⁴⁵ entanglement is always generated by the SPDC process. Za- In HD-QKD with SPDC source, when the SPDC source is weakly ¹¹¹ ⁴⁶ vatta et al. [\[31,32\]](#page--1-0) used a conditional preparation technique by the pumped, the photon number statistics of an SPDC source statistics 112 ⁴⁷ SPDC process to generate SPACS. Specifically, SPACS can be gener- approaches the Poissonian distribution [20]. Analogously, we can ¹¹³ 48 ated by injecting a coherent state $|\alpha\rangle$ into the signal mode of an control and make the statistics of the distribution to approach the ¹¹⁴ ⁴⁹ optical parametric amplifier. The conditional preparation of the tar-
⁴⁹ optical parametric amplifier. The conditional preparation of the tar-
statistics of the non-entangled SPACS source in theory. So in our ¹¹⁵ ⁵⁰ get state can take place every time that a single photon is detected scheme, we assume that the photon number distribution of Alice's ¹¹⁶ ⁵¹ in the correlated idler mode. That means photons between signal ESPACS source, which is also the probability of sending k -photon 117 ⁵² states and idler states are correlated in time domain. In the ideal pairs, is given by [28] 53 119 condition, the energy should be constant that is correlated with 54 mean photon numbers. Though a coherent state is injected into $e^{-|\alpha|^2}$ $|\alpha|^{2(k-1)}k$ $e^{-\zeta}$ $\zeta^{k-1}k$ \ldots \ldots 120 55 the signal mode, the energy between signal states and idler states $F_k(\lambda) = \frac{1}{1 + |\alpha|^2} \frac{1}{(k-1)!} = \frac{1}{1 + \lambda} \frac{1}{(k-1)!} (k \ge 1)$, (3) 121 56 122 is still anti-correlated. The time-energy entanglement of photon ⁵⁷ generated by SPDC is not broken. So combining with techniques in where λ is the intensity of Alice's ESPACS source, $\zeta = |\alpha|^2$ is the ¹²³ ⁵⁸ experimental demonstrations of time-energy entangled HD-QKD, it intensity of the initial coherent state and the relation between λ ¹²⁴ ⁵⁹ is possible to implement the SPACS into the time-energy entangled and ζ is expressed by 60 126 HD-QKD.

62 **follows** [\[13,20\]:](#page--1-0) **the contract of the con**

63 129 **a. Biphoton preparation and transmission:** In each round, Alice ⁶⁴ generates entangled photon pairs from the ESPACS source. She also capacity (in bits per coincidence) is expressed as [20] 130 65 modulates the intensity $\lambda \in \{\mu, \nu\}$ at random with probabilities p_{μ} and the intensity $\lambda \in \{\mu, \nu\}$ at random with probabilities p_{μ} and the intensity $\lambda \in \{\mu, \nu\}$ at random with probabilities p_{μ}

http://dx.doi.org/10.1016/j.physleta.2017.01.058

¹ problem on finite resources, the finite-key analysis for the decoy- the decoy setting. She retains one of photon pairs and sends the ⁶⁷ 2 state HD-QKD protocol based on dispersive optics was presented ather to Bob through the quantum channel. Here, the number of 68 ³ for collective attacks [\[21\]](#page--1-0) and general attacks [\[22\],](#page--1-0) respectively. In alphabet characters per photon pulse is $d = \sigma_{coh}/\sigma_{cor}$, where σ_{cor} 69 ⁴ order to improve the protocol's performance, the detector-decoy is the correlation time between two photons, σ_{coh} is the coherence ⁷⁰ ⁵ method was introduced into the HD-QKD and a new scheme was time of the pump field, which is always larger than σ_{cor} . 71 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, *σcoh* is the coherence time of the pump field, which is always larger than *σcor*.

⁶ proposed [\[23\].](#page--1-0) Meanwhile, other ways that can enhance the perfor-**b. Measurement:** Alice and Bob measure their photons by ran-⁷ mance of decoy-state HD-QKD protocol should be further studied. domly and independently choosing one of two bases (the time ⁷³ **b. Measurement:** Alice and Bob measure their photons by ran $p_W = 1 - p_T$, 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 [\[20\]](#page--1-0)

$$
P_{\lambda} = \sum_{k=0}^{\infty} P_k(\lambda) C_k,
$$
\n(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 [\[20\]](#page--1-0)

40 the conclusion is summarized in Sec. 5.
\n
$$
C_k = [1 - (1 - p_d)(1 - \eta_A)^k][1 - (1 - p_d)(1 - \eta_B t)^k].
$$
\n(2) 10¹⁰⁶

42 **2. Protocol description Alternative Server and** *n***_{***B***} and** *n***_B are the server and** *n***_B are the server and** *n***_B are ¹⁰⁸** 43 109 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 [\[28\]](#page--1-0)

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

The decoy-state HD-QKD based on dispersive optics works as
$$
\zeta = \left(\sqrt{\lambda^2 - 2\lambda + 5} + \lambda - 3\right)/2.
$$
 (4) 127 follows [13.20]:

When the key length is infinite, the bound on the secret key capacity (in bits per coincidence) is expressed as [\[20\]](#page--1-0)

66 and
$$
p_v = 1 - p_\mu
$$
, respectively, where μ is the signal setting, v is $\Delta I \ge \beta I(A; B) - (1 - F_\lambda)n_R - F_\lambda \chi^U_{\xi_t, \xi_\omega}(A; E)$, (5) 132

^ξt,ξω (A; *^E),* (5)Please cite this article in press as: Y. Wang et al., High-dimensional quantum key distribution with the entangled single-photon-added coherent state, Phys. Lett. A (2017),

Download English Version:

<https://daneshyari.com/en/article/5496867>

Download Persian Version:

<https://daneshyari.com/article/5496867>

[Daneshyari.com](https://daneshyari.com/)