Contents lists available at ScienceDirect

Physics Letters A

www.elsevier.com/locate/pla

Enhancing the performance of the measurement-device-independent quantum key distribution with heralded pair-coherent sources

Feng Zhu [a,b], Chun-Hui Zhang [a,b], Ai-Ping Liu [a,b], Qin Wang [a,b,c,*]

[a] Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
[b] Key Lab of Broadband Wireless Communication and Sensor Network Technology, Nanjing University of Posts and Telecommunications, Ministry of Education, Nanjing 210003, China
[c] Key Laboratory of Quantum Information, University of Science and Technology of China, Hefei 230026, China

ARTICLE INFO

Article history:
Received 21 October 2015
Received in revised form 16 February 2016
Accepted 18 February 2016
Available online 23 February 2016
Communicated by A. Eisfeld

Keywords:
Quantum key distribution
Heralded pair-coherent sources
Weak coherent light

ABSTRACT

In this paper, we propose to implement the heralded pair-coherent source into the measurement-device-independent quantum key distribution. By comparing its performance with other existing schemes, we demonstrate that our new scheme can overcome many shortcomings existing in current schemes, and show excellent behavior in the quantum key distribution. Moreover, even when taking the statistical fluctuation into account, we can still obtain quite high key generation rate at very long transmission distance by using our new scheme.

1. Introduction

The quantum key distribution (QKD) allows two distant parties, typically named Alice and Bob, to exchange secure cryptographic keys despite that in the presence of a malicious eavesdropper, Eve [1]. Its security has been theoretically proven under certain assumptions either on the sources or on the detection systems [2–4]. However, there exist imperfections in real-life QKD systems, thus Eve could make use of these imperfections and carry out attacks. For example, owing to the flaws in the sources, Eve could block the single-photon components, split all the multi-photon pulses, and transmit the left part to the receiver with a lossless channel, so as to possess the same information as the legitimate users. This is the so-called photon-number-splitting (PNS) attack [5–7].

In order to anti-attack the PNS attack, people invent the decoy-state method [8–13] and solve the problems in the light sources. On the other hand, to combat the attacks on the detection systems, some other strategies have been proposed, such as the device-independent quantum key distribution (DI-QKD) [14,15], or the measurement-device-independent quantum key distribution (MDI-QKD) [16,17]. Among them, the MDI-QKD looks most promising, since it can not only be realized with current experimental conditions, but also show pretty good performance.

Till today, many different proposals on how to implement the decoy-state MDI-QKD have been proposed [18–22]. Among them, either the weak coherent source (WCS) or the heralded single-photon source (HSPS) has been implemented. However, each of them has its own drawbacks. For example, there is unneglectable vacuum components in the WCS, and relative higher multi-photon probability in the HSPS, resulting in either quite limited secure transmission distance in the former case or the relatively lower key generation rate in the latter case. Interestingly, we find another source, the heralded pair-coherent source (HPCS) can indeed eliminate the shortcomings above, and show excellent behavior in the implementation of the decoy-state MDI-QKD.

This manuscript is arranged as follows: In Sec. 2, we firstly investigate the photon-number distribution of the HPCS, and compare it with other existing sources; In Sec. 3, we introduce in detail on how to implement the HPCS into the MDI-QKD; In Sec. 4, we consider the finite date size effect, and account for statistical fluctuation in our scheme; Finally, summary and conclusions are given out in Sec. 5.

2. Photon-number distribution of the HPCS

The pair-coherent state (PCS) was firstly investigated by Agarwal [23], but mainly focusing on its quantum mechanical characteristics. In recent years, people found that, by carrying out the photon-heralding technique [24–27] on the PCS, the probability of its empty components can be reduced to a neglectable level, generating the so-called heralded pair-coherent state (HPCS), which can

[*] Corresponding author at: Institute of Signal Processing Transmission, Nanjing University of Posts and Telecommunications, Nanjing 210003, China.
E-mail address: qinw@njupt.edu.cn (Q. Wang).

http://dx.doi.org/10.1016/j.physleta.2016.02.030
0375-9601/© 2016 Elsevier B.V. All rights reserved.

Table 1
Probabilities of the vacuums, the single-photons and multi-photons in the HPCS, WCS and HSPS, and the corresponding values of the second-order correlation function at zero time delay. Here we reasonably set the light intensity as 0.5 for all the WCS, HSPS and HPCS, the dark-count rate and the detection efficiency of the triggering detector are set as $d_A = 10^{-6}$ and $\eta_A = 0.75$ individually, both for the HPCS and HSPS [11,19].

Sources	HPCS	WCS	HSPS
Vacuum	4.93×10^{-6}	0.60653	1.94×10^{-6}
Single photon	0.9255	0.30326	0.72735
Multiphoton	0.0744508	0.09024	0.27265
$g^2(0)$	0.136032	1	0.43634

show excellent behavior in the implementation of QKDs [28,29]. According to the definition in Refs. [23,24], the PCS can be written in the Fock basis:

$$|\phi\rangle = \frac{1}{\sqrt{I_0(2\,|\mu|)}} \sum_{n=0}^{\infty} \frac{\mu^n}{n!} |n\rangle_1 |n\rangle_2 \tag{1}$$

where $\mu \in C$ and $I_0(x)$ is the modified Bessel's function of the first kind.

By using the photon-heralding technique, one mode of the HPCS can be locally triggered, and used to encode the behavior of the other mode. Then the n-photon number probability of the encoded pulse can be expressed as:

$$P_n(\mu) = \frac{1}{I_0(2\mu)} \frac{\mu^{2n}}{(n!)^2} [1 - (1 - \eta_A)^n + d_A] \tag{2}$$

here η_A and d_A each represents the detection efficiency and the dark count rate of the triggering detector individually; μ is the average intensity of the pulses; and $I_0(x)$ is the modified Bessel's function of the first kind.

In our scheme, we need the following condition hold true for any $\mu' \geq \mu$ and $n \geqslant 2$:

$$\frac{P_n(\mu')}{P_n(\mu)} \geq \frac{P_2(\mu')}{P_2(\mu)} \geq \frac{P_1(\mu')}{P_1(\mu)} \tag{3}$$

which follows from

$$\frac{P_n(\mu')}{P_n(\mu)} - \frac{P_{n-1}(\mu')}{P_{n-1}(\mu)} = \frac{I_0(2\mu)}{I_0(2\mu')} (\frac{\mu'}{\mu})^{2n} [1 - (\frac{\mu}{\mu'})^2] \geqslant 0 \tag{4}$$

According to Eq. (2), the photon-number distribution for the HSPS can be numerically simulated, as shown in Table 1.

In Table 1, we compare the probabilities of the vacuum components, the single photons, the multi-photons, and the second-order correlation function at zero time delay among the HPCS, the WCS and the HSPS. We can easily find from Table 1 that, the HPCS contains almost neglectable vacuum component, which is significant lower than in WCS, and with comparable level as in HSPS. Moreover, it possesses significantly higher probability of the single-photon pulses and extremely lower probabilities for the multi-photon pulses compared with both the HSPS and the WCS. As a result, the HPCS exhibits extremely lower value of the second-order correlation function at zero time delay, and shows very good sub-poissonian photon-number distribution. It is indeed more suitable for implementing into QKDs.

3. Implementing the HPCS into the MDI-QKD

3.1. Bounds Y_{11}^L and e_{11}^U

As is known, the MDI-QKD is aimed at removing all possible side-channel attacks, and its security has been theoretically proven [16,17]. The decoy-state MDI-QKDs based on WCS and HSPS have been widely investigated [18–22]. Here we propose to implement the HPCS into the MDI-QKD, and carry out corresponding investigation on its performance. The schematic of our experimental setup is shown in Fig. 1.

In MDI-QKD, we know that when the two-pulse signal from Alice and Bob arrives at the untrusted third party (UTP), and successfully projects onto one of the Bell states, it is denoted as a successful event. Here the UTP can even be controlled by Eve. In order to distill the secure key from those successful event, we should estimate the counting rate and the quantum-bit error rate (QBER) caused by the single-photon pluses. In this paper, we implement the three-intensity decoy-state MDI-QKD with HPCS. In the method, three different states (0, μ_i, μ_i', $i = A, B$) need to be randomly prepared by Alice and Bob. Here μ_A (μ_B) represents the intensity for the decoy state, μ_A' (μ_B') corresponds to the signal state, and $0 < \mu_i < \mu_i'$, ($i = A, B$). In the following, we denote the intensity used by Alice and Bob as x and y, respectively, $x \in \{\mu_A, \mu_A'\}$ and $y \in \{\mu_B, \mu_B'\}$. The corresponding average counting rate and quantum-bit error rate can be written as

$$S_{x,y}^W = \sum_{m,n=0}^{\infty} P_n(x) P_n(y) Y_{nm}^W \tag{5}$$

$$E_{x,y}^W S_{x,y}^W = \sum_{m,n=0}^{\infty} P_n(x) P_n(y) e_{nm}^W Y_{nm}^W \tag{6}$$

where W represents the X or Z basis; Y_{nm}^W and E_{nm}^W each corresponds to the yield or the QBER, when Alice send out an n-photon

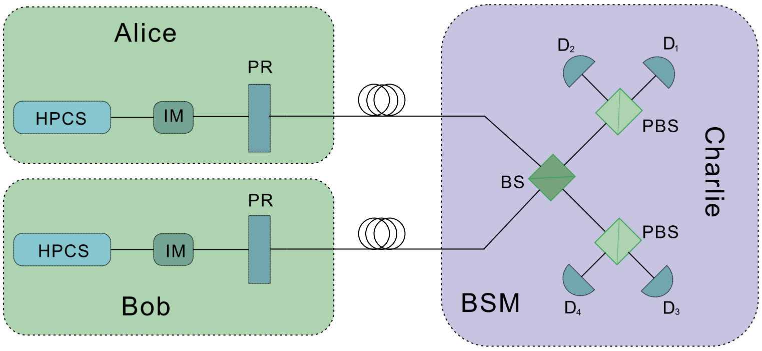

Fig. 1. (Color online.) The schematic setup of the MDI-QKD with heralded pair-coherent sources. Alice and Bob randomly prepare the heralded pair-coherent sources into one of the four BB84 polarization states with a polarization rotator (PR) for each pulse. The intensity modulator (IM) is used to randomly modulating the intensity of each pulse into different values, i.e., the decoy or the signal state. At the UTP's (Charlie's) side, pulses from Alice and Bob interfere at a 50:50 beam splitter (BS), and each enters a polarizing beam-splitter (PBS). Four single-photon detectors (D_3–D_4) are used for detecting the photons, and corresponding detections results are public announced after the signal transmission. A click in D_1, D_4 or D_2, D_3 indicates a projection into the Bell state $|\psi^-\rangle = 1/\sqrt{2}(|HV\rangle - |VH\rangle)$, while a click in D_1, D_2 or D_3, D_4 reveals a projection into the Bell state $|\psi^+\rangle = 1/\sqrt{2}(|HV\rangle + |VH\rangle)$.