IOPscience iopscience.iop.org

Home Search Collections Journals About Contact us My IOPscience

Experimental passive decoy-state quantum key distribution

This content has been downloaded from IOPscience. Please scroll down to see the full text.

2014 Laser Phys. Lett. 11 085202

(http://iopscience.iop.org/1612-202X/11/8/085202)

View the table of contents for this issue, or go to the journal homepage for more

Download details:

IP Address: 166.111.142.37
This content was downloaded on 26/11/2014 at 02:02

Please note that terms and conditions apply.

IOP Publishing | Astro Ltd Laser Physics Letters
Laser Phys. Lett. 11 (2014) 085202 (7pp) doi:10.1088/1612-2011/11/8/085202

# Experimental passive decoy-state quantum key distribution

**Qi-Chao Sun[1,3], Wei-Long Wang[2], Yang Liu[1], Fei Zhou[4], Jason S Pelc[5], M M Fejer[5], Cheng-Zhi Peng[1], Xianfeng Chen[3], Xiongfeng Ma[2], Qiang Zhang[1,4] and Jian-Wei Pan[1]**

[1] Shanghai Branch, Hefei National Laboratory for Physical Sciences at the Microscale and Department of Modern Physics, University of Science and Technology of China, Hefei, Anhui 230026, People's Republic of China
[2] Center for Quantum Information, Institute for Interdisciplinary Information Sciences, Tsinghua University, Beijing 100084, People's Republic of China
[3] Department of Physics, Shanghai Jiao Tong University, Shanghai, 200240, People's Republic of China
[4] Jinan Institute of Quantum Technology, Shandong Academy of Information and Communication Technology, Jinan 250101, People's Republic of China
[5] E. L. Ginzton Laboratory, Stanford University, 348 Via Pueblo Mall, Stanford, California 94305, USA

E-mail: xma@tsinghua.edu.cn, xfchen@sjtu.edu.cn and qiangzh@ustc.edu.cn

Received 23 April 2014, revised 19 May 2014
Accepted for publication 19 May 2014
Published 18 June 2014

**Abstract**
The decoy-state method is widely used in practical quantum key distribution systems to replace ideal single photon sources with realistic light sources of varying intensities. Instead of active modulation, the passive decoy-state method employs built-in decoy states in a parametric down-conversion photon source, which can decrease the side channel information leakage in decoy-state preparation and hence increase the security. By employing low dark count up-conversion single photon detectors, we experimentally demonstrate the passive decoy-state method over a 50 km long optical fiber and obtain a key rate of about 100 bit $s^{-1}$. Our result suggests that the passive decoy-state source is a practical candidate for future quantum communication implementation.

Keywords: quantum key distribution, passive decoy-state, parametric down conversion

(Some figures may appear in colour only in the online journal)

## 1. Introduction

Quantum key distribution (QKD) [1, 2] can provide unconditionally secure communication with ideal devices [3–5]. In reality, due to the technical difficulty of building up ideal single photon sources, most of the current QKD experiments use weak coherent-state pulses from attenuated lasers. Such a replacement opens up security loopholes that lead to QKD systems being vulnerable to quantum hacking, such as photon-number-splitting attacks [6]. The decoy-state method [7–11] has been proposed to close these photon source loopholes. It has been implemented in both optical fiber [12–17] and free space channels [18, 19].

The security of decoy-state QKD relies on the assumption of the photon-number channel model [11, 20, 21], where the photon source can be regarded as a mixture of Fock (number) states. In practice, this assumption can be guaranteed when the signal and decoy states are indistinguishable from the adversary party, Eve, other than the photon-number information. Otherwise, if Eve is able to distinguish between the signal and decoy states via other degrees of freedom, such as the frequency and timing of the pulses, the security of the decoy-state protocol would fail [13, 22]. In the original proposals, on the transmitter's side, Alice actively modulates the intensities of the pulses to prepare decoy states through an optical intensity modulator, as shown in figure 1(*a*). This active decoy-state method, however, might leak the signal/decoy information to Eve due to intensity modulation and increase the complexity of the system.

Another type of protocols, the passive decoy-state method, has been proposed, where the decoy states are prepared

 © 2014 IAEA, Vienna Printed in the UK

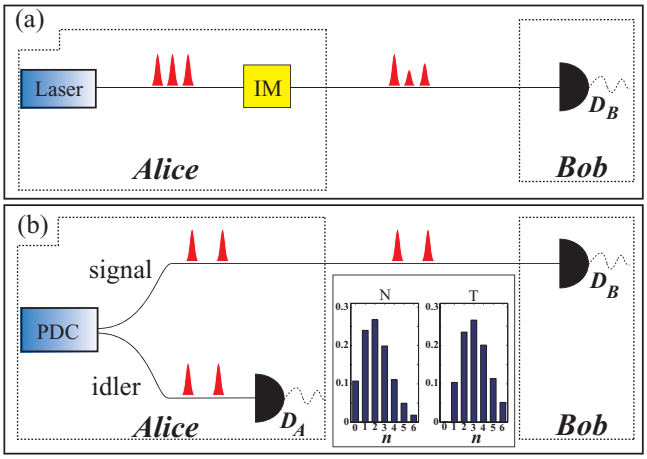


**Figure 1.** (*a*) In the active decoy-state method, Alice employs an intensity modulator (IM) to vary the average photon numbers of the attenuated weak coherent pulses. (*b*) In the passive decoy-state method, Alice infers the two different photon number distributions of the signal mode from the detection results of the idler mode, *N* (non-triggered) and *T* (triggered), respectively. The inset shows the photon number distributions conditioned on the detection results of the idler mode.

through measurements [23–25]. The passive method can rely on the usage of a parametric down-conversion (PDC) source where the photon numbers of two output modes are strongly correlated. As shown in figure 1(*b*), Alice first generates photon pairs through a PDC process and then detects the idler photons as triggers. Conditioned on Alice's detection outcome of the idler mode, trigger (*T*) or non-trigger (*N*), Alice can infer the corresponding photon number statistics of the signal mode, and hence obtain two conditional states for the decoy-state method. The photon numbers of these two states follow different distributions as shown in the appendix. From this point of view, the PDC source can be treated as a built-in decoy state source. Note that passive decoy-state sources with non-Poissonian light other than PDC sources are studied in [26–31]. The PDC source can also be used as a heralded single photon source in the active decoy-state method [32].

The key advantage of the passive decoy-state method is that it can substantially reduce the possibility of signal/decoy information leakage [25, 33]. In addition, the phases of signal photons are totally random due to the spontaneous feature of the PDC process. This intrinsic phase randomization improves the security of the QKD system [34] by making it immune to source attacks [35, 36]. The critical experimental challenge to implement passive decoy-state QKD is that the error rate for the non-trigger case is very high due to the high vacuum ration and background counts. Besides, as a local detector, the idler photons do not suffer from the modulation loss and channel loss, so the counting rate of Alice's detector is very high. Due to the high dark count rate and low maximum counting rate, commercial InGaAs/InP avalanche photodiodes (APD) are not suitable for these passive decoy-state QKD experiments. By developing up-conversion single photon detectors with high efficiency and low noise, we are able to suppress the error rate in the non-trigger events. Meanwhile, the up-conversion single photon detectors can reach a maximum counting rate

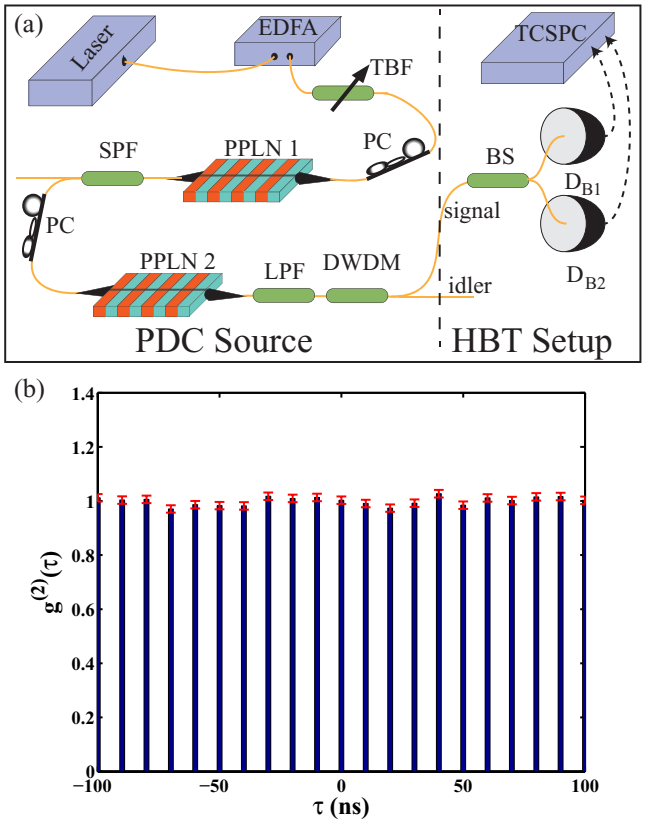


**Figure 2.** (*a*) A schematic diagram of the PDC source test. EDFA, erbium-doped fiber amplifier; TBF, tunable bandpass filter; PPLN, periodically poled lithium niobate; PC, polarization controller; SPF, short-pass filter; LPF, long-pass filter; DWDM, dense wavelength-division multiplexing; BS, 50 : 50 beam splitter; TCSPC, time correlated single photon counting. (*b*) Normalized second-order correlation function of the photons in the signal mode. The parameter $\tau$ represents the time delay between the photons of the two BS output arms. The value of $g^{(2)}(0)$ is 0.994 ± 0.014.

of about 20 MHz. With such detectors, we demonstrate the passive decoy-state method over a 50 km long optical fiber.

## 2. Photon number distribution of the PDC source

For the decoy-state method, the photon number distribution of the source is crucial for data postprocessing [25, 37]. Thus, we first investigate the photon number distribution of the PDC source used in the experiment, as shown in figure 2(*a*). An electronically driven distributed feedback laser, triggered by an arbitrary function generator, is used to provide a 100 MHz pump pulse train. After being amplified by an erbium-doped fiber amplifier (EDFA), the laser pulses with a 1.4 ns FWHM duration and 1556.16 nm central wavelength pass through a 3 nm tunable bandpass filter to suppress the amplified spontaneous emission noise from the EDFA. The light is then frequency doubled in a periodically poled lithium niobate (PPLN) waveguide. Since our waveguide only accepts TM-polarized light, an in-line fiber polarization controller is used to adjust the polarization of the input light. The generated second harmonic pulses are separated from the pump light by a short-pass filter with an extinction ratio of about

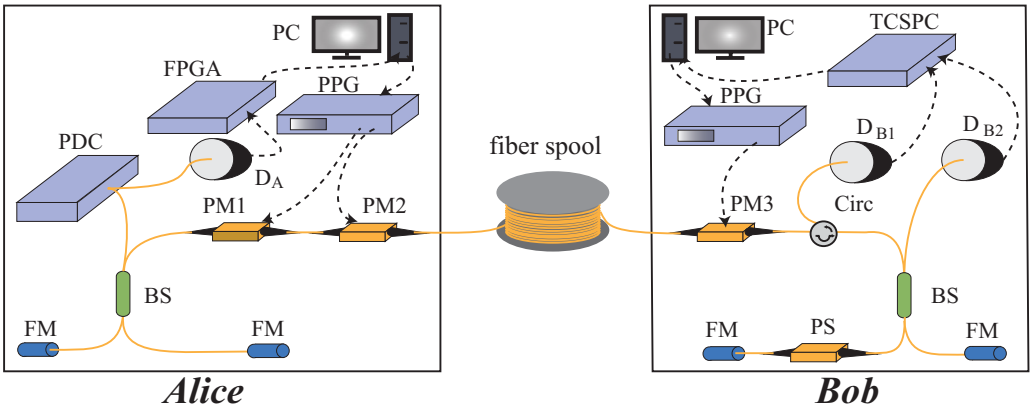


**Figure 3.** The schematic diagram of our experimental setup. BS, 50 : 50 beam splitter; FM, Faraday mirror; PM, phase modulator; FPGA, field programmable gate array; PPG, pulse pattern generator; Circ, optical circulator; PS, phase shifter. The detectors used in the experiment are up-conversion single photon detectors.

180 dB, and then used to pump the second PPLN waveguide to generate correlated photon pairs. Both PPLN waveguides are fiber pigtailed reverse-proton-exchange devices and each has a total loss of 5 dB. The generated photon pairs are separated from the pump light of the second PPLN waveguide by a long-pass filter with an extinction ratio of about 180 dB. The down converted signal and idler photons are separated by a 100 GHz dense wavelength-division multiplexing (DWDM) fiber filter. The central wavelengths of the two output channels of the DWDM filter are 1553.36 nm and 1558.96 nm.

For a spontaneous PDC process, the number of emitted photon pairs within a wave package follows a thermal distribution [38]. In the case where the system pulse length is longer than the wave package length, the distribution can be calculated by taking the integral of the thermal distributions. In the limit where the pulse length is much longer than the wave package length, the integrated distribution can be well estimated by a Poisson distribution [39, 40]. In our experiment, the pump pulse length is 1.4 ns, while the length of the down-conversion photon pair wave package is around 4 ps. Therefore, the photon pair's number statistics can be approximated by a Poisson distribution. To verify this, we built a Hanbury Brown–Twiss (HBT) setup [41] by inserting a 50 : 50 beam splitter (BS) in the signal mode followed by two single photon detectors, as shown in figure 2(*a*). Both detection signals are fed to a time correlated single photon counting (TCSPC) module for time correlation measurement. A time window of 2 ns is used to select the counts within the pulse duration. The interval between the peaks of counts is 10 ns, which is consistent with the 100 MHz repetition rate of our source. After accumulating about 5000 counts per time bin, we calculate the value of the normalized second-order correlation function $g^{(2)}(\tau)$ of the signal photons, which is shown in figure 2(*b*). The value of $g^{(2)}(0)$ is 0.994 ± 0.014, which confirms the Poisson distribution of the photon pair number.

## 3. Experimental setup and key rate

Our passive decoy-state QKD experimental setup is shown in figure 3. The PDC source is placed on Alice's side. The idler photons are detected by an up-conversion single photon detector whose outcomes are recorded by a field programmable gate array (FPGA) based data acquisition card and then transmitted to a computer. The up-conversion single photon detector used in our experiment consists of a frequency up-conversion stage in a nonlinear crystal followed by detection using a silicon APD (SAPD). As described in [42], a 1950 nm thulium doped fiber laser is employed as a pump light for the PPLN waveguide, which is used to up-convert the wavelength of the idler photons to 866 nm. After filtering the pump and other noise in the up-conversion process, we detect the output photons with an SAPD. By using the long-wavelength pump technology, we can suppress the noise to a very low level and achieve a detection efficiency of 15% and a dark count rate of 800 Hz.

For signal photons, we employ the phase-encoding scheme by using an unbalanced Faraday–Michelson interferometer and two phase modulators (PM), as shown in figure 3. The time difference between two bins is about 3.7 ns. The two PMs are driven by a 3.3 GHz pulse pattern generator (PPG). The first PM is utilized to choose the $X$ or $Y$ basis by modulating the relative phase of the two time bins into $\left\{0, \frac{1}{2}\pi\right\}$, respectively. The second PM is utilized to choose the bit value by modulating the relative phase into $\{0, \pi\}$. The encoded photons are transmitted to the receiver (Bob) through an optical fiber. Bob chooses a basis with a PM driven by another PPG and measures the relative phase of the two time bins via an unbalanced interferometer with the same time difference of 3.7 ns. The random numbers used in the experiment are generated by a quantum random number generator (IDQ Quantis-OEM) beforehand and stored on the memory of the PPGs. The detection efficiency and dark count rate of the up-conversion detectors on Bob's side are 14% and 800 Hz, respectively. Note that although the PM for encoding may also induce side channel leakage [22], the intent of this work is to close the loophole due to the decoy state preparation, not to close all the loopholes in one experiment. We would also remark that BB84 qubit encoding can also be done via passive means [43]. Such a step can be taken in future work.

One challenge in the experimental setup is to stabilize the relative phase of the two unbalanced arms in the two

**Table 1.** Experimental results. The number of pulses sent by Alice in each case is $N = 6 \times 10^{10}$. $N_A$ is the total number of photons detected by Alice. $\eta$ represents the transmittance, taking channel loss, modulation loss and detection efficiency on Bob's side into account.

| Parameter | 0 km | 25 km | 50 km |
|---|---|---|---|
| $\mu$ | 0.035 | 0.036 | 0.028 |
| $N_A$ | $4.22 \times 10^9$ | $4.14 \times 10^9$ | $3.99 \times 10^9$ |
| $\eta$ | 21.8 dB | 25.2 dB | 30.4 dB |
| $Q_T$ | $2.21 \times 10^{-5}$ | $1.02 \times 10^{-5}$ | $2.50 \times 10^{-6}$ |
| $Q_N$ | $2.13 \times 10^{-4}$ | $1.02 \times 10^{-4}$ | $2.43 \times 10^{-5}$ |
| $E_T$ | 1.97% | 2.81% | 3.06% |
| $E_N$ | 2.12% | 3.15% | 3.99% |

separated unbalanced interferometers, which is very sensitive to temperature or mechanical vibration. We place a piezoelectric phase shifter in one arm of the interferometer on Bob's side for active phase feedback. After every second of QKD, Alice sends time-bin qubits without encoding and Bob records the detection results without choosing a basis. The detection results are used for feedback to control the piezoelectric phase shifter.

After quantum transmission, Alice provides Bob with the basis and trigger ($T$ or $N$) information. Bob groups his detection events accordingly and evaluates the gain $Q_j$ and quantum bit error rate (QBER) $E_j$, where $j = T, N$. They can distill a secret key from both $N$ and $T$ events. Thus, the total key generation rate is given by

$$R = R_N + R_T, \tag{1}$$

where $R_N$ and $R_T$ are key rates distilled from $N$ and $T$ events, respectively. Following the security analysis of the passive decoy state scheme [25], the secret key rate is given by

$$R_j \geq q\left\{-fQ_jH(E_j) + Q_{j,1}[1-H(e_1)] + Q_{j,0}\right\}, \tag{2}$$

where $j = N, T$; $q$ is the raw data sift factor (in the standard BB84 protocol $q = 1/2$); $f$ is the error correction inefficiency (instead of implementing the error correction, we estimated the key rate by taking $f = 1.2$, which can be realized by the low-density parity-check code [44]); $Q_j$ and $E_j$ are the gain and QBER; $Q_{j,1}$ and $e_1$ are the gain and error rate of the single-photon component; $Q_{j,0}$ is the background count rate; $H(x) = -x\log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function. Alice and Bob can obtain the gains and QBERs, $Q_N$, $Q_T$, $E_N$, $E_T$, directly from the experiment result. The variables for the privacy amplification part, $Q_{j,1}$, $e_1$ and $Q_{j,0}$, need to be estimated by the decoy-state method. Details of the decoy-state estimation as well as the method of postprocessing and simulation used later can be found in the appendix.

We perform the passive decoy-state QKD over optical fibers of 0 km, 25 km and 50 km. For each distance, we run the system for 20 min, half of which is used for phase feedback control. Thus the effective QKD time is 10 min and the system repetition rate is 100 MHz. Therefore, the number of pulses sent by Alice for each distance is $N = 60$ Gbit. We analyze the time correlation of the detection results and calibrate the average photon number generated in the PDC source, $\mu_0$, using the measurement value of the coincidence to accidental

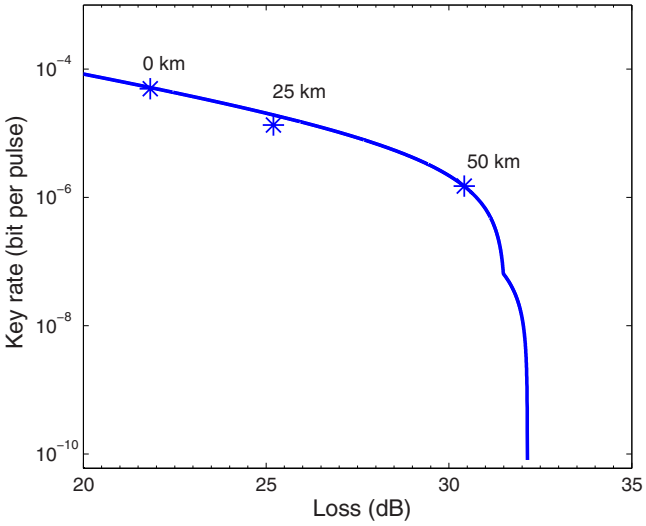


**Figure 4.** Comparison of theoretical values and experimental results of the key rate. The loss consists of the loss of channel and the modulation loss and detection efficiency on Bob's side. The solid line represents the simulation values of the key rate. The stars are the experimental results.

coincidence ratio [45]. The average photon number Alice sends to the channel, $\mu$, can be calculated as $\mu = \eta_s \mu_0$, where $\eta_s = 19.2$ dB is the loss including the transmission loss of the PDC source and the modulation loss of Alice. The experimental results are listed in table 1. After the postprocessing, we obtain a final key of 2.53 Mbit, 805 kbit and 89.8 kbit for 0 km, 25 km and 50 km, respectively.

To compare the experimental results of the key rate with QKD simulation, we set the values of the simulation parameters, $\mu$, $N_A$ and $\eta_s$, to the parameters used in the 50 km QKD experiment. We also calibrate our system to obtain a few parameters for simulation: $e_d = 1.2\%$ is the error rate of Bob's detector and $Y_0 = 1.6 \times 10^{-6}$ is the background count rate of Bob's detection. The comparison is shown in Figure 4. As one can see, the experimental results are consistent with the simulation results. Note that there is an inflection point at about 31.7 dB, where $R_N$ drops to 0 and $R_T$ is still positive.

## 4. Conclusions

We have investigated a parametric down-conversion photon source pumped by a pulse laser for usage in passive decoy-state QKD. The experimental result suggests that the photon-pair number of the PDC source can be well approximated by a Poisson distribution. With this source, we have experimentally demonstrated a passive decoy-state QKD scheme. In our experiment, the transmission loss of the PDC source is about 7 dB, the total modulation loss caused by the two UFMIs and the three PMs is about 21 dB. These losses result in a significantly reduced key rate. However, there is room for improvement: if new-type Mach–Zehnder interferometers (MZIs) [16] are used, the modulation loss of our system can be reduced by 9 dB; we can have a reduction of about 3 dB if a state-of-the-art PPLN waveguide is used. Aiming for long distance QKD, we can also improve the up-conversion single photon detector, by

using a volume Bragg grating as a filter, and achieve a detection efficiency of about 30% with a dark count rate of less than 100 Hz [42]. In addition, the repetition rate of our system can be raised to 10 GHz [45]. These feasible improvements mean it is potential to perform passive decoy-state QKD over 150 km in optical fibers. Beside the PDC based scheme used in our experiment, there are other practical scenarios of passive decoy-state QKD, for example those based on thermal states or phase randomized coherent states [26–28]. However, the physics and applications of these protocols demand further theoretical and experimental studies.


## Acknowledgments

We acknowledge insightful discussions with Z Cao, X Yuan and Z Zhang. This work was supported by the National Basic Research Program of China Grants No. 2011CB921300, No. 2013CB336800, No. 2011CBA00300 and No. 2011CBA00301, and the Chinese Academy of Sciences. QCS and WLW contributed equally to this work.


## Appendix A. Method of postprocessing and simulation

The model of our passive decoy-state QKD experiment setup is shown in figure A1. $\mu_0$ denotes the average photon pair number of the PDC source. $\eta_s$ denotes Alice's internal transmittance, including the transmission loss of the PDC source and Alice's modulation loss. $\mu$ denotes the average photon number of the signals sent to Bob, thus

$$\mu = \eta_s \mu_0 . \tag{A.1}$$

$\eta_A$ denotes the transmittance of the idler mode, taking into account transmission loss of the source and detection efficiency. $\eta$ denotes the transmittance, taking channel loss, modulation loss and detection efficiency on Bob's side into account. All the parameters can be characterized by Alice before the experiment, except for $\eta$ which could be controlled by Eve.

Since Alice uses threshold detectors, the probabilities that Alice's detector does not click ($N$) and clicks ($T$) when $i$ photons arrive are

$$P_{N|i} = (1 - Y_{0A})\left(1-\eta_A\right)^i \simeq \left(1-\eta_A\right)^i , \tag{A.2}$$

$$P_{T|i} = 1 - P_{N|i}, \tag{A.3}$$

where $Y_{0A}$ denotes the dark count rate of Alice's detection, which is about the order of $10^{-6}$, so we just ignore it.

The joint probabilities that Alice has $N/T$ detection and $i$ photons are sent to Bob are given by

$$P_N(i) = \sum_{j=i}^{\infty} \frac{(\mu_0)^j}{j!} \mathrm{e}^{-\mu_0} \left(1-\eta_A\right)^j \binom{j}{i} \eta_{\mathrm{s}}^i \left(1-\eta_{\mathrm{s}}\right)^{j-i} \tag{A.4}$$

$$= \frac{\mu^i}{i!} \mathrm{e}^{-\mu} \left(1-\eta_A\right)^i \mathrm{e}^{-(\mu_0-\mu)\eta_A}, \tag{A.5}$$

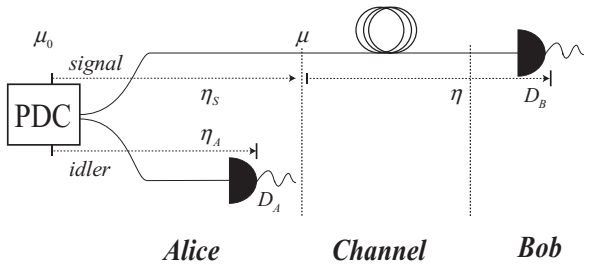


**Figure A1.** Model of the passive decoy-state QKD experimental setup.

$$P_T(i) = \sum_{j=i}^{\infty} \frac{(\mu_0)^j}{j!} \mathrm{e}^{-\mu_0} \left[1-\left(1-\eta_A\right)^j\right] \binom{j}{i} \eta_{\mathrm{s}}^i \left(1-\eta_{\mathrm{s}}\right)^{j-i} \tag{A.6}$$

$$= \frac{(\mu)^i}{i!} \mathrm{e}^{-\mu} \left[1-\left(1-\eta_A\right)^i \mathrm{e}^{-(\mu_0-\mu)\eta_A}\right]. \tag{A.7}$$

Define the yield $Y_i$ as the conditional probability that Bob gets a detection, given that Alice sends $i$ photons into the channel and $e_i$ is the corresponding error rate. Then the gains that Alice has an $N/T$ detection and Bob has an $i$-photon detection are given by

$$Q_{N,i} = P_N(i)\, Y_i = \frac{\mu^i}{i!} \mathrm{e}^{-\mu} \left(1-\eta_A\right)^i \mathrm{e}^{-(\mu_0-\mu)\eta_A} Y_i, \tag{A.8}$$

$$Q_{T,i} = P_T(i)\, Y_i = \frac{(\mu)^i}{i!} \mathrm{e}^{-\mu} \left[1-\left(1-\eta_A\right)^i \mathrm{e}^{-(\mu_0-\mu)\eta_A}\right] Y_i. \tag{A.9}$$

Thus, the overall gains when Alice gets an $N/T$ detection are

$$Q_N = \sum_{i=0}^{\infty} Q_{N,i} = \sum_{i=0}^{\infty} \frac{(\mu)^i}{i!} \mathrm{e}^{-\mu} \left(1-\eta_A\right)^i \mathrm{e}^{-(\mu_0-\mu)\eta_A} Y_i, \tag{A.10}$$

$$Q_T = \sum_{i=0}^{\infty} Q_{T,i} = \sum_{i=0}^{\infty} \frac{(\mu)^i}{i!} \mathrm{e}^{-\mu} \left[1-\left(1-\eta_A\right)^i \mathrm{e}^{-(\mu_0-\mu)\eta_A}\right] Y_i. \tag{A.11}$$

The corresponding quantum bit error rates (QBERs) are given by

$$E_N Q_N = \sum_{i=0}^{\infty} e_i Q_{N,i} \tag{A.12}$$

$$= \sum_{i=0}^{\infty} \frac{\mu^i}{i!} \mathrm{e}^{-\mu} \left(1-\eta_A\right)^i \mathrm{e}^{-(\mu_0-\mu)\eta_A} e_i Y_i, \tag{A.13}$$

$$E_T Q_T = \sum_{i=0}^{\infty} e_i Q_{T,i} \tag{A.14}$$

$$= \sum_{i0}^{\infty} \frac{\mu^i}{i!} \mathrm{e}^{-\mu} \left[1-\left(1-\eta_A\right)^i \mathrm{e}^{-(\mu_0-\mu)\eta_A}\right] e_i Y_i. \tag{A.15}$$

For simulation purpose, we consider the case when Eve does not change $Y_i$ and $e_i$. These are given by

$$Y_i = 1-(1-Y_0)\,(1-\eta)^i , \tag{A.16}$$

$$e_i Y_i = e_{\mathrm{d}} Y_i + (e_0 - e_{\mathrm{d}})\, Y_0, \tag{A.17}$$

where $Y_0$ is the dark count rate of Bob's detection, $e_0 = 1/2$ is the error rate of the dark count, and $e_d$ is the intrinsic error rate of Bob's detection.

The gains of single-photon and vacuum states are given by

$$Q_{N,1} = \mu e^{-\mu}\left(1-\eta_A\right)e^{-(\mu_0-\mu)\eta_A}Y_1, \tag{A.18}$$

$$Q_{T,1} = \mu e^{-\mu}\left[1-\left(1-\eta_A\right)e^{-(\mu_0-\mu)\eta_A}\right]Y_1, \tag{A.19}$$

$$Q_{N,0} = e^{-[\mu+(\mu_0-\mu)\eta_A]}Y_0, \tag{A.20}$$

$$Q_{T,0} = e^{-\mu}[1-e^{-(\mu_0-\mu)\eta_A}]\,Y_0. \tag{A.21}$$

Note that, for postprocessing, the values of $Q_N$, $Q_T$, $E_N$, $E_T$ should be obtained directly from the experiment. The overall gains when Alice gets an $N/T$ detection are given by

$$Q_N = e^{-\mu_0\eta_A}[1-(1-Y_0)\,e^{\mu\eta(\eta_A-1)}], \tag{A.22}$$

$$Q_T = 1-(1-Y_0)\,e^{-\mu\eta}-e^{-\mu_0\eta_A}[1-(1-Y_0)\,e^{\mu\eta(\eta_A-1)}], \tag{A.23}$$

$$E_NQ_N = e_dQ_N + (e_0-e_d)\,Y_0e^{-\mu_0\eta_A}, \tag{A.24}$$

$$E_TQ_T = e_dQ_T + (e_0-e_d)\,Y_0(1-e^{-\mu_0\eta_A}). \tag{A.25}$$

Denote $Q$ and $E$ as the gain and QBER of Bob getting a detection,

$$Q = Q_N + Q_T = 1-(1-Y_0)\,e^{-\mu\eta}, \tag{A.26}$$

$$EQ = E_NQ_N + E_TQ_T = e_dQ + (e_0-e_d)\,Y_0. \tag{A.27}$$

The final key, which can be extracted from both non-triggered and triggered detection events, and the key rate, R, is given by

$$R = R_N + R_T, \tag{A.28}$$

where $R_N$ and $R_T$ are the key rates distilled from $N$ and $T$ events, respectively. Note that both $R_N$ and $R_T$ should be non-negative, and if either of them is negative we set it to 0. Following the security analysis of the passive decoy-state scheme [25], $R_N$ and $R_T$ are obtained by

$$R_j \geq q\left\{-fQ_jH(E_j) + Q_{j,1}[1-H(e_1)] + Q_{j,0}\right\}, \tag{A.29}$$

where $j = N, T$; $q$ is the raw data sift factor ($q = \frac{1}{2}$ in standard BB84 protocol); $f$ is the error correction inefficiency, and we use $f = 1.2$ here; and $H(x) = -x\log_2(x)-(1-x)\log_2(1-x)$ is the binary Shannon entropy function. To get the lower bound of the key generation rate, we can lower bound $Y_1$ and upper bound $e_1$. By $(1-\eta_A)^2 \times Q - Q_N$, one obtains

$$Y_1 \geq Y_1^L = \frac{1}{\mu\eta_A(1-\eta_A)}[e^{\mu+\mu_0\eta_A-\mu\eta_A}Q_N \tag{A.30}$$

$$-(1-\eta_A)^2\,e^{\mu}Q-(2\eta_A-\eta_A^2)\,Y_0], \tag{A.31}$$

Then $e_1$ can be simply estimated by

$$e_1 \leq e_1^U = \frac{E_TQ_T}{Q_1^L} = \frac{e^{\mu}E_TQ_T}{\mu\left[1-\left(1-\eta_A\right)e^{-(\mu_0-\mu)\eta_A}\right]Y_1^L}. \tag{A.32}$$

Here, we also take statistical fluctuation into account [37]. Assume that there are $N$ pulses sent by Alice to Bob.

$$Q_N^L = Q_N\left(1-\frac{u_\alpha}{\sqrt{NQ_N}}\right), \tag{A.33}$$

$$Q^U = Q\left(1+\frac{u_\alpha}{\sqrt{NQ}}\right), \tag{A.34}$$

$$(E_TQ_T)^U = E_TQ_T\left(1+\frac{u_\alpha}{\sqrt{NE_TQ_T}}\right), \tag{A.35}$$

$$(E_NQ_N)^U = E_NQ_N\left(1+\frac{u_\alpha}{\sqrt{NE_NQ_N}}\right), \tag{A.36}$$

$$Y_0^U = \frac{e^{\mu+(\mu_0-\mu)\eta_A}(E_NQ_N)^U}{e_0}, \tag{A.37}$$

where $Q_N$, $Q$, $E_TQ_T$, $E_NQ_N$ and $EQ$ are measurement outcomes that can be obtained directly from the experiment and 'L' and 'U' denote lower bound and upper bound, respectively. Note that, for triggered events, we need not consider fluctuation when using equation (A.32) to estimate the upper bound of $e_1$. But for non-triggered events, we must take statistical fluctuation into account, which means

$$e_1^U = \frac{(E_TQ_T)^U}{Q_1^L}. \tag{A.38}$$

In the standard error analysis assumption, $u_\alpha$ is the number of standard deviations chosen for the statistical fluctuation analysis. In the postprocessing and simulation, we set the value of $u_\alpha$ to 5, corresponding to a failure probability of $5.733 \times 10^{-7}$.

## References


[1] Bennett C H and Brassard G 1984 Quantum cryptography: public key distribution, coin tossing *Proc. of the IEEE Int. Conf. on Computers, Systems, Signal Processing* (IEEE Press: New York) pp 175–9

[2] Ekert A K 1991 Quantum cryptography based on Bell's theorem *Phys. Rev. Lett.* **67** 661–3

[3] Mayers D 2001 Unconditional security in quantum cryptography *J. ACM* **48** 351–406

[4] Lo H-K and Chau H F 1999 *Science* **283** 2050

[5] Shor P W and Preskill J 2000 Simple proof of security of the BB84 quantum key distribution protocol *Phys. Rev. Lett.* **85** 441

[6] Brassard G, Lütkenhaus N, Mor T and Sanders B C 2000 Limitations on practical quantum cryptography *Phys. Rev. Lett.* **85** 1330–3

[7] Hwang W-Y 2003 Quantum key distribution with high loss: toward global secure communication *Phys. Rev. Lett.* **91** 057901

[8] Lo H-K 2004 Quantum key distribution with vacua or dim pulses as decoy states *Proc. Int. Symp. on Information Theory ISIT* (*Chicago, July 2004*) (Piscataway, NJ: IEEE) p 137

[9] Ma X 2004 Security of quantum key distribution with realistic devices *Master's Thesis* University of Toronto (arXiv: quant-ph/0503057)
[10] Wang X-B 2005 Beating the pns attack in practical quantum cryptography *Phys. Rev. Lett.* **94** 230503
[11] Lo H-K, Ma X and Chen K 2005 Decoy state quantum key distribution *Phys. Rev. Lett.* **94** 230504
[12] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 Experimental quantum key distribution with decoy states *Phys. Rev. Lett.* **96** 070502
[13] Zhao Y, Qi B, Ma X, Lo H-K and Qian L 2006 Simulation, implementation of decoy state quantum key distribution over 60 km telecom fiber *Proc. of IEEE ISIT* (*Seattle July* 2006) p 2094
[14] Rosenberg D, Harrington J W, Rice P R, Hiskett P A, Peterson C G, Hughes R J, Lita A E, Nam S W and Nordholt J E 2007 Long-distance decoy-state quantum key distribution in optical fiber *Phys. Rev. Lett.* **98** 010503
[15] Peng C-Z, Zhang J, Yang D, Gao W-B, Ma H-X, Yin H, Zeng H-P, Yang T, Wang X-B and Pan J-W 2007 Experimental long-distance decoy-state quantum key distribution based on polarization encoding *Phys. Rev. Lett.* **98** 010505
[16] Yuan Z L, Sharpe A W and Shields A J 2007 *Appl. Phys. Lett.* **90** 011118
[17] Liu Y *et al* 2010 Decoy-state quantum key distribution with polarized photons over 200 km *Opt. Express* **18** 8587–94
[18] Schmitt-Manderbach T *et al* 2007 Experimental demonstration of free-space decoy-state quantum key distribution over 144 km *Phys. Rev. Lett.* **98** 010504
[19] Wang J Y *et al* 2013 Direct and full-scale experimental verifications towards ground-satellite quantum key distribution *Nat. Photonics* **7** 387–93
[20] Lo H-K and Lütkenhaus N 2007 Quantum cryptography: from theory to practice *Phys. Can.* **63** 191
[21] Ma X 2008 Quantum cryptography: from theory to practice *PhD Thesis* University of Toronto
[22] Jiang M-S, Sun S-H, Li C-Y and Liang L-M 2012 Wavelength-selected photon-number-splitting attack against plug-and-play quantum key distribution systems with decoy states *Phys. Rev.* A **86** 032310
[23] Mauerer W and Silberhorn C 2007 Passive decoy state quantum key distribution: closing the gap to perfect sources *Phys. Rev.* A **75** 050305
[24] Adachi Y, Yamamoto T, Koashi M and Imoto N 2007 Simple and efficient quantum key distribution with parametric down-conversion *Phys. Rev. Lett.* **99** 180503
[25] Ma X and Lo H-K 2008 Quantum key distribution with triggering parametric down conversion sources *New J. Phys.* **10** 073018
[26] Curty M, Moroder T, Ma X and Lütkenhaus N 2009 Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution *Opt. Lett.* **34** 3238–40
[27] Curty M, Ma X, Qi B and Moroder T 2010 Passive decoy-state quantum key distribution with practical light sources *Phys. Rev.* A **81** 022310
[28] Zhang Y *et al* 2010 Practical Non-Poissonian light source for passive decoy state quantum key distribution *Opt. Lett.* **35** 3393–5
[29] Hu J-Z and Wang X-B 2010 Reexamination of the decoy-state quantum key distribution with an unstable source *Phys. Rev.* A **82** 012331
[30] Zhen-Qiang Y, Wei C, Wen-Ye L, Hong-Wei L, Guang-Can G, Zheng-Fu H, Yang Z and Shuang W 2012 Experimental demonstration of passive decoy state quantum key distribution *Chin. Phys.* B **21** 100307
[31] Li Y, Bao W-S, Li H-W, Zhou C and Wang Y 2014 Passive decoy-state quantum key distribution using weak coherent pulses with intensity fluctuations *Phys. Rev.* A **89** 032329
[32] Wang Q, Chen W, Xavier G, Swillo M, Zhang T, Sauge S, Tengner M, Han Z-F, Guo G-C and Karlsson A 2008 Experimental decoy-state quantum key distribution with a sub-Poissonian heralded single-photon source *Phys. Rev. Lett.* **100** 090501
[33] Hu J-Z and Wang X-B 2010 Reexamination of the decoy-state quantum key distribution with an unstable source *Phys. Rev.* A **82** 012331
[34] Lo H-K and Preskill J 2007 Security of quantum key distribution using weak coherent states with nonrandom phases *Quantum Inform. Comput.* **7** 0431
[35] Tang Y-L *et al* Source attack of decoy-state quantum key distribution using phase information *Phys. Rev.* A **88** 022308
[36] Sun S-H, Gao M, Jiang M-S, Li C-Y and Liang L-M 2012 Partially random phase attack to the practical two-way quantum-key-distribution system *Phys. Rev.* A **85** 032304
[37] Ma X, Qi B, Zhao Y and Lo H-K 2005 Practical decoy state for quantum key distribution *Phys. Rev.* A **72** 012326
[38] Yurke B and Potasek M 1987 Obtainment of thermal noise from a pure quantum state *Phys. Rev.* A **36** 3464–6
[39] Tapster P R and Rarity J G 1998 Photon statistics of pulsed parametric light *J. Mod. Opt.* **45** 595–604
[40] De Riedmatten H, Scarani V, Marcikic I, Acin A, Tittel W, Zbinden H and Gisin N 2004 Two independent photon pairs versus four-photon entangled states in parametric down conversion *J. Mod. Opt.* **51** 1637–49
[41] Brown R H and Twiss R Q 1956 A test of a new type of stellar interferometer on Sirius *Nature* **178** 1046–8
[42] Shentu G-L, Pelc J S, Wang X-D, Sun Q-C, Zheng M-Y, Fejer M M, Zhang Q and Pan J-W 2013 Ultralow noise up-conversion detector and spectrometer for the telecom band *Opt. Express* **21** 13986–91
[43] Curty M, Ma X, Lo H-K and Lütkenhaus N 2010 Passive sources for the bennett-brassard quantum-key-distribution protocol with practical signals *Phys. Rev.* A **82** 052325
[44] Elkouss D, Leverrier A, Alleaume R, Boutros J J 2009 Efficient reconciliation protocol for discrete-variable quantum key distribution *IEEE Inter. Symp. on Information Theory (Seoul June 2009)* (Piscataway, NJ: IEEE) 1–4
[45] Zhang Q, Xie X, Takesue H, Nam S W, Langrock C, Fejer M M and Yamamoto Y 2007 Correlated photon-pair generation in reverse-proton-exchange ppln waveguides with integrated mode demultiplexer at 10 GHz clock *Opt. Express* **15** 10288–93