Source monitor in quantum key distribution

Xiang Peng[1] and *Hong Guo*[2]

[1] Institute of Quantum Electronics, School of Electronics Engineering and Computer Science, Peking University, Beijing 100871, P.R. China. E-mail: xiangpeng@pku.edu.cn.

[2] As 1 but E-mail: hongguo@pku.edu.cn.

Abstract

The core value of a quantum-key-distribution (QKD) system is the unconditional security. In the standard security analysis, the characteristics of QKD source are assumed to be known and fixed. In a real QKD experiment, this assumption may be deviated. Especially, in commercial Plug&Play QKD system, the source is untrusted. Source monitor can close this security loophole. This paper analyzes passive source-monitor scheme, and shows that this scheme can be well implemented in practice.

1 Introduction

Quantum key distribution (QKD) establishes two parties (Alice and Bob) to share a secure key by a quantum channel and an authenticated classical channel [1]. The core value of a QKD system is the unconditional security based on quantum physics. Commonly, the QKD system is composed of three parts: source, channel, and detection. In theoretical security analysis [2], the characteristics of these three parts are assumed to be known and fixed to Alice and Bob. To guarantee the security of a real QKD experiment, one needs to carefully verify these assumptions. The main concern of this paper is the QKD source. Here, the untrusted QKD source is considered, which means that Eve has a full control of the photon source. This is a crucial assumption in the security proof of some QKD schemes, such as commercial Plug&Play system [3]. Recently, the QKD with untrusted source is studied [4-10]. With using active scheme, the security of untrusted source is proven [5]. This active scheme requires a fast random switch and a perfect "intensity monitor". However, in reality, this is not practical. Thus, a passive scheme, with a beam splitter and an imperfect detector, was proposed and verified experimentally [6]. In this paper, we review and discuss three ways to implement this passive scheme: inverse-Bernoulli transformation [6, 10], two-threshold detection[7, 8], and photon-number-resolving (PNR) detector [9].

2 Passive scheme with inverse-Bernoulli transformation

The passive schematic diagram of the setup for Alice to monitor the photon source is shown in Fig. 1. In the following discussion, Pi with $i = 1, \cdots, 6$, refers to Position i in Fig. 1. The inefficient detector can be treated as a virtual beam splitter placed in front of an ideal detector. Suppose that the probability of inputting n photons at P2 is p_n and the probability of detecting m photoelectrons by the detector is q_m, then q_m is the Bernoulli transformation of p_n and p_n can be theoretically recovered by the inverse-Bernoulli transformation of q_m [10]

$$q_m = B[p_n, \xi] = \sum_{n=m}^{\infty} p_n C_n^m \xi^m (1-\xi)^{n-m}, \quad \xi \in (0,1), \tag{1}$$

$$p_n = B^{-1}[q_m, \xi^{-1}] = \sum_{m=n}^{\infty} q_m C_m^n \xi^{-n} (1-\xi^{-1})^{m-n}, \quad \xi \in (0.5,1). \tag{2}$$

where C_n^m is the combinatorial number of picking m unordered outcomes from n possibilities, and $\xi = t_B t_D$. Formally, the direct and inverse transformations satisfy the duality relation if we interchange the role of m and n in Eq. (1), and replace ξ by ξ^{-1}, we obtain the inverse transformation in Eq. (2).

978-1-4244-6051-9/11/$26.00

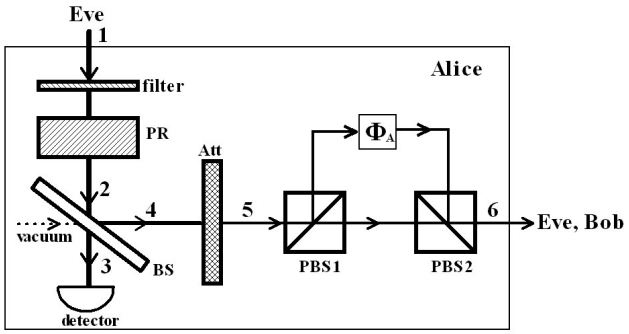

Figure 1: A schematic diagram of the setup on Alice's side. The untrusted photon source, prepared at P1 by Eve, passes through a low-bandwidth filter and a phase randomizer (PR). Then, a beam splitter (BS) (transmission: t_B) is used to separate it into two beams, 3 and 4. One beam goes to a photodetector (detection efficiency: t_D) at P3 and the other is prepared for QKD at P4. An attenuator (Att) between P4 and P5 has the attenuation coefficient η_s (η_d) for the signal (decoy) state. Two polarization beam splitters (PBS1 and PBS2) and a phase modulator (Φ_A) between P5 and P6 are used for phase encoding.

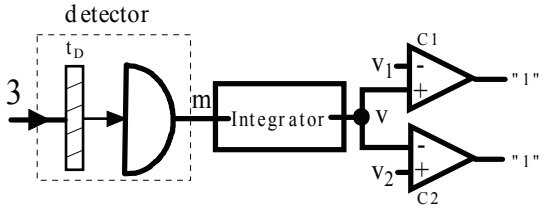

Figure 2: A two-threshold detection. The integrator converts the photoelectron number m to the voltage v. C1 (C2): comparator. "11" output from C1 and C2 means the voltage v between v_1 and v_2 and the photon number m falls in the range $[m_1, m_2]$, correspondingly.

However, when a large number of photons are monitored with a finite-resolution and noisy detector, it is challenging to implement the direct inversion of p_n based on Eq. (2) on computer. Actually, the inversion of photon-photoelectron counting problem is ill-posed. To resolve this practical issue, a new statistical inversion method, i.e., Bayesian method, is proposed, in which the coarse-graining strategies for treating realistic detection resolution and estimating parameters are applied. Using this new method, the reconstruction of p_n with the data set from an actual QKD experiment is carried out [10].

In the standard security analysis, it is important to estimate the lower (upper) bound of Δ_1 (e_1) which is the fraction of counts (quantum bit error rate, QBER) due to single photon state. From p_n, we can bound $N \in [N_{min}, N_{max}]$ with a probability $(1-\varepsilon)$ at P2 in Fig. 1. Then, following Ref. [6], one can get the bound of Δ_1 or e_1. Then, the secure key rate can be calculated.

3 Passive scheme with two-threshold detection

To implement the passive scheme more robustly, the detection mode at P3 in Fig. 1 needs to be simplified. In doing so, a two-threshold detection illustrated in Fig. 2 is used. For simplicity, we take the case, $t_B t_D = 1 - t_B$, as an example. To estimate the bound of Δ_1 or e_1, one can also estimate the bound of a probability Δ with which the photon number n_4 at P4 falls in the range $[m_1, m_2]$ [8]. Note that, as $t_B t_D = 1 - t_B$, the photon-number distribution $P(n_4)$ $\big(= B[p_n, (1-t_B)]\big)$ is equal to q_m $\big(= B[p_n, t_B t_D]\big)$. Thus, $\Delta = \sum_{m_1}^{m_2} P(n_4)$ can be monitored and estimated by the two-threshold detection at P3.

4 Passive scheme with photon-number-resolving detector

In the three-intensity decoy-state QKD protocol, Alice randomly sends three kinds of sources: vacuum, decoy and signal source, respectively. The quantum state of the decoy (signal) source is $\rho_d = \sum_{n=0}^{\infty} a_n |n\rangle \langle n|$ ($\rho_s = \sum_{n=0}^{\infty} a'_n |n\rangle \langle n|$). It is proved that [4]

$$\Delta_1 \geq \frac{{a'_1}^L \left({a'_2}^L Q_d - a_2^U Q_s - {a'_2}^L a_0^U Q_0 + a_2^U {a'_0}^L Q_0 \right)}{Q_s \left(a_1^U {a'_2}^L - {a'_1}^L a_2^U \right)}, \tag{3}$$

where Q_0, Q_d, or Q_s is the count rate of vacuum, decoy and signal source, respectively, and the superscript $L(U)$ means lower (upper) bound. If QBER E_s from the signal source is measured and known, one has $e_1 = E_s/\Delta_1$. Thus, to calculate the lower (upper) bound of Δ_1 (e_1), one needs to estimate the parameters $\{{a'_0}^L, a_0^U, {a'_1}^L, a_1^U, {a'_2}^L, a_2^U\}$.

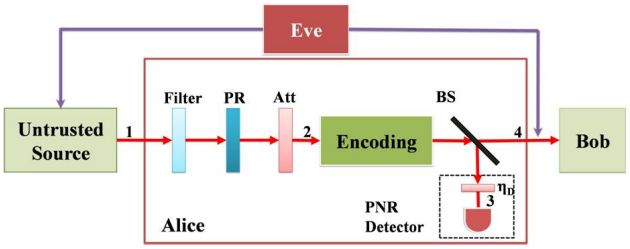

Figure 3: The untrusted source passes through an optical filter, a phase randomizer (PR), and an attenuator (Att). After the source is encoded, a beam splitter (BS) with transmittance t_B separates it into two beams: one goes to a photon-number-resolving (PNR) detector with efficiency t_D at P3 and the other is sent out of Alice's side at P4.

The passive scheme for estimating the parameters $\{{a'_0}^L, a_0^U, {a'_1}^L, a_1^U, {a'_2}^L, a_2^U\}$ is shown in Fig. 3, where a photon-number-resolving (PNR) detector that can discriminate the photon number of $n = 0$, $n = 1$, $n = 2$, $n \geq 3$ is used. For simplicity, on can calibrate the setup to satisfy $t_D(1 - t_B) = t_B$. Under this condition, the photon-number distribution (PND) at position 4 is the same to that at position 3 in Fig. 3. Thus, the parameters $\{{a'_0}^L, a_0^U, {a'_1}^L, a_1^U, {a'_2}^L, a_2^U\}$ is estimated by PNR detector.

5 Discussion and Conclusion

Intuitively, if the characteristics of the untrusted source infinitely approaches to that of the trusted source, Alice needs to verify the PND of QKD source. Theoretically, in the passive scheme as Fig. 1, the inverse-Bernoulli transformation can reconstruct the PND of untrusted source with inefficient detector. Furthermore, the coarse-graining idea and Bayesian methods provide a more practical way to deal with the inverse problem even after considering the finite resolution and noisy in monitoring detector. However, the smoothness of the untrusted-source PND is assumed in these methods no matter that this assumption is reasonable and physically relevant in practice. It is challenging to develop more advanced algorithm to remove this assumption.

As the PNR detection is concerned, the difficult is to develop the PNR detector to discriminate the photon number of $n = 0$, $n = 1$, $n = 2$, $n \geq 3$. Fortunately, the time multiplexing detector (TMD), transition-edge sensor (TES), a threshold detector together with a variable attenuator, etc., is developing to remove this difficulty.

Relatively, the passive scheme with two-threshold detection is simpler and robust in practice. Without

complicated postprocessing, this scheme can realize the real-time source monitor with high speed. At present, this method seems to be more applicable to practical QKD system.

6 Acknowledgments

This work is supported by the Key Project of National Natural Science Foundation of China (Grant No. 60837004). X. Peng acknowledges financial support from the China Postdoctoral Science Foundation.

7 References

1. V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, "The security of practical quantum key distribution," *Rev. Mod. Phys.*, **81**, September 2009, pp. 1301-1350.

2. D. Gottesman, H. K. Lo, N. Lütkenhaus, and J. Preskill, "Security of quantum key distribution with imperfect devices," *Quantum Inf. Comput.*, **4**, September 2004, pp. 325-360.

3. D. Stucki, N. Gisin, O. Guinnard, G. Ribordy, and H. Zbinden, "Quantum key distribution over 67 km with a 'Plug&Play' system," *New J. of Phys.*, **4**, July 2002, p. 41.

4. X. B. Wang, T. Hiroshima, A. Tomita, and M. Hayashi, "Quantum information with Gaussian states," *Phys. Rep.*, **448**, May 2007, pp. 1-111.

5. Y. Zhao, B. Qi, and H. K. Lo, "Quantum key distribution with an unknown and untrusted Source," *Phys. Rev. A*, **77**, May 2008, p. 052327.

6. X. Peng, H. Jiang, B. Xu, X. Ma, and H. Guo, 'Experimental quantum-key distribution with an untrusted source," *Opt. Letts.*, **33**, September 2008, pp. 2077-2079.

7. Y. Zhao, B. Qi, H. K. Lo, and L. Qian, "Security analysis of an untrusted source for quantum key distribution: passive approach," *New J. of Phys.*, **12**, February 2010, p. 023024.

8. X. Peng, B. Xu, and H. Guo, "Passive-scheme analysis for solving the untrusted source problem in quantum key distribution," *Phys. Rev. A*, **81**, April 2010, p. 042320.

9. B. Xu, X. Peng, and H. Guo, "Passive scheme with a photon-number-resolving detector for monitoring the untrusted source in a plug-and-play quantum-key-distribution system," *Phys. Rev. A*, **82**, October 2010, p. 042301.

10. J. D. Wu, T. J. Li, X. Peng, and Hong Guo, "Statistical method for resolving the photon-photoelectron-counting inversion problem," *J. Comput. Phys.*, **230**, February 2011, 726-743.