Passive Decoy State Quantum Key Distribution with Coherent Light

Marcos Curty,[1,§] Xiongfeng Ma,[2] Bing Qi,[3] Tobias Moroder,[2,4,5] and Norbert Lütkenhaus[2,4,5]

[1]*ETSI Telecomunicación, Department of Signal Theory and Communications, University of Vigo, Campus Universitario, E-36310 Vigo (Pontevedra), Spain*

[2]*Institute for Quantum Computing & Department of Physics and Astronomy, University of Waterloo, N2L 3G1 Waterloo, Ontario, Canada*

[3]*Center for Quantum Information and Quantum Control, Department of Physics and Department of Electrical & Computer Engineering, University of Toronto, M5S 3G4 Toronto, Ontario, Canada*

[4]*Quantum Information Theory Group, Institute of Theoretical Physics I, University of Erlangen-Nürnberg, 91058 Erlangen, Germany*

[5]*Max Planck Institute for the Science of Light, 91058 Erlangen, Germany*

[§]*Corresponding author: mcurty@com.uvigo.es*

Abstract: We propose a simple method for passive preparation of decoy states in quantum key distribution with coherent light. It involves linear optics together with a photo-detector. The performance is comparable to the active decoy schemes.

©2010 Optical Society of America

OCIS codes: (270.5565) Quantum communications; (270.5568) Quantum cryptography; (270.5290) Photon statistics.

1. Introduction

Decoy states have been proven to be a very useful method for significantly enhancing the performance of quantum key distribution (QKD) systems with practical signals. In this approach, the sender (Alice) varies, independently and at random, the mean photon number of each signal state she sends to the receiver (Bob) by employing different intensity settings [1-3]. This is typically performed by using a variable optical attenuator together with a random number generator. The eavesdropper (Eve) does not know a priori the mean photon number of each signal state sent by Alice. This means that her eavesdropping strategy can only depend on the photon number of these signals, but not on the particular intensity setting used to generate them. From the measurement results corresponding to different intensity settings, the legitimate users can obtain a better estimation of the behavior of the quantum channel. This translates into an enhancement of the achievable secret key rate and distance. This technique has been implemented in several recent experiments, and can give a key generation rate of linear behavior with the transmission efficiency of the channel, similar to the key rate expected from a single photon source.

While active modulation of the intensity of the pulses suffices to perform decoy state QKD in principle, in practice passive preparation might be desirable in some scenarios. For instance, in those setups operating at high transmission rates. Known passive methods usually rely on the use of a parametric down-conversion source together with a photo-detector [4-6]. Here we show that coherent states can also be used for the same purpose, *i.e.*, one does not need to employ a non-linear optics network preparing entangled states [7]. The main idea is rather simple, although it is counterintuitive. When two phase randomized coherent states interfere at a beam splitter (BS), the photon number statistics of the outcome signals are classically correlated. This effect contrasts with the one coming from the interference of two pure coherent states with fixed phase relation at a BS, where the photon number statistics of the output states is just the product of two Poissonian distributions. Then, by measuring one of the two outcome signals, the conditional photon number distribution of the other signal varies depending on the result obtained. This measurement can be performed, for instance, with a simple threshold photon detector [7]. Most importantly, in the asymptotic limit of an infinite long experiment, it turns out that the secret key rate provided by such a passive scheme is similar to the one delivered by an active decoy state setup with infinity decoy settings [7]. This technique can also be used with heralded single-photon sources showing non-Poissonian photon number statistics [8-10].

2. Passive decoy state QKD setup

The basic setup is illustrated in Fig. 1 (Case A). Suppose two phase randomized weak coherent pulses (WCPs) of mean photon number $\mu 1$ and $\mu 2$, respectively, interfere at a BS of transmittance t. The joint probability $p(n,m)$ of having n photons in mode a and m photons in mode b is given by

$$p(n,m)=\frac{v^{n+m}e^{-v}}{n!m!}\frac{1}{2\pi}\int_0^{2\pi}\gamma^n(1-\gamma)^m d\theta, \qquad (1)$$

OTuK5.pdf

where $v=\mu 1+\mu 2$, $\gamma=[\mu 1t+\mu 2(1-t)+\xi\cos(\theta)]/v$ and $\xi=2\sqrt{\mu 1\mu 2(1-t)t}$.

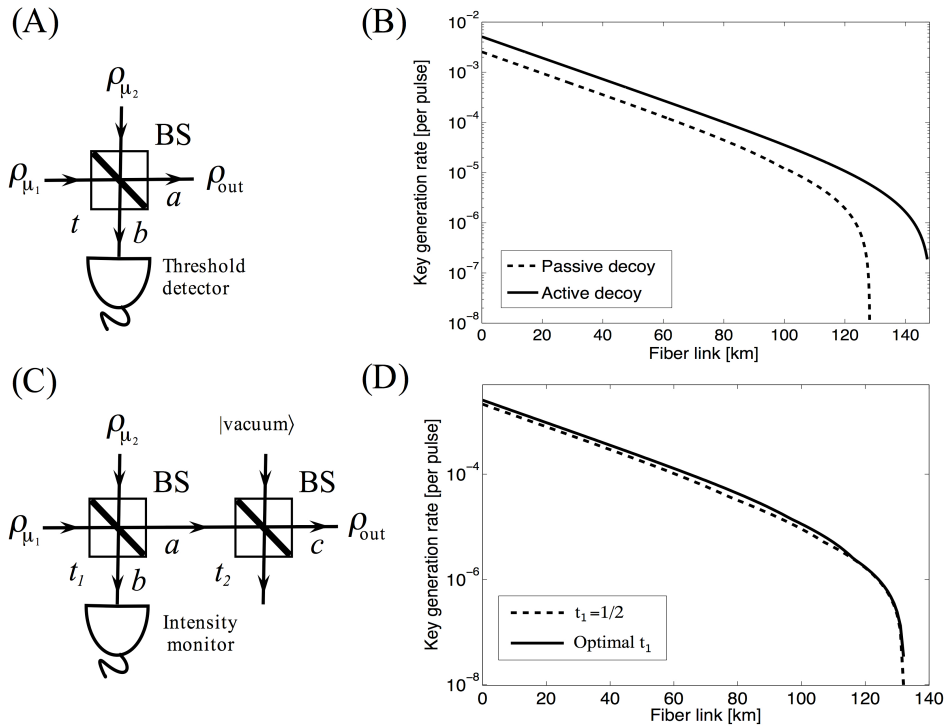

Fig. 1. (Case A) Basic setup of a passive decoy state QKD scheme with WCPs; a and b represent the two output modes. (Case B) Lower bound on the secret key rate in logarithmic scale for the passive setup illustrated in Case A with two intensity settings. The transmittance of the BS is t=1/2. We consider two possible scenarios: (1) a perfect threshold photon detector, and (2) a threshold photon detector with a detection efficiency of 12 % and a dark count rate equal to $3.2\text{x}10^{-7}$ [16]. Both cases provide approximately the same final key rate and they cannot be distinguished with the resolution of this figure (dashed line). The solid line represents a lower bound on the secret key rate for an active asymptotic decoy state system [2]. (Case C) Basic scheme of a passive decoy state QKD system with strong coherent light. The mean photon number of the input signals is quite high; for instance, around 10^8 photons. t1 and t2 represent, respectively, the transmittances of the two BSs, and a,b, and c denote output modes. (Case D) Lower bound on the secret key rate for the passive setup illustrated in Case C with two intensity settings. We consider two situations: (1) We impose t1=1/2 and we optimize the parameter t2 (dashed line), and (2) we optimize both t1 and t2.

By measuring the outcome signal in mode b , then the conditional photon number statistics in mode a vary depending on the result obtained. For instance, if Alice uses a threshold photon detector, then she can only obtain two possible results: click and no click. We consider that Alice and Bob treat these two events separately, and they distill secret key from both of them. We use the secret key rate formula provided in [11,12],

$$R\geq max\{Rc,0\}+max\{Rnc,0\}, \qquad (2)$$

where Rc (Rnc) denotes the secret key rate associated to the click (no click) events. It is given by

$$Rc\geq q\{-Qc\,f(Ec)\,H(Ec)+p1c\,Y1[1-H(e1)]+p0c\,Y0\}, \qquad (3)$$

and similarly for Rnc . The parameter q is the efficiency of the protocol ($q=1/2$ for the standard Bennett-Brassard 1984 protocol [13], and $q\approx 1$ for its efficient version [14]), Qc is the overall gain of the signals, Ec represents the overall quantum bit error rate (QBER), $f(Ec)$ is the error correction efficiency [typically $f(Ec)\geq 1$ with Shannon limit $f(Ec)=1$], Yn denotes the yield of an n-photon signal, *i.e.*, the conditional probability of a detection event on Bob's side given that Alice transmits an n-photon state, $e1$ is the single photon error rate, and $H(x)$ is the binary Shannon entropy function.

To apply the secret key rate formula given by Eq. (3) one needs to estimate a lower bound on $Y1$ and $Y0$ together with an upper bound on $e1$. For that, we follow the procedure proposed in [15]. Note, however, that many other estimation techniques are also available, like, for instance, linear programming tools. For simulation purposes we consider the channel model used in [2,15]. This model reproduces a normal behavior of the quantum channel, *i.e.*, in the absence of eavesdropping. It allows us to calculate the observed experimental parameters

Qc , Ec , Qnc , and Enc .

The resulting lower bound on the secret key rate is illustrated in Fig. 1 (Case B). The experimental parameters are the ones reported in [16]. We assume that $q=1$, $f(Ec)=f(Enc)=1.22$, and $t=1/2$, *i.e.*, we consider a simple 50:50 BS. Fig. 1 (Case B) includes as well the case of an active asymptotic decoy state QKD system [2]. The cutoff points where the secret key rate drops down to zero are $l\approx 128\,km$ (passive setup with two intensity settings) and $l\approx 147\,km$ (active asymptotic setup). One could reduce this gap further by using a passive scheme with more intensity settings. For instance, Alice may employ a photon number resolving detector instead of a simple threshold photon detector, or use more threshold detectors in combination with BSs [10]. From these results we see that the performance of the passive scheme is comparable to the active one, thus showing the practical interest of the passive setup.

This idea can also be applied to other practical scenarios with different signals and detectors like, for example, those based on strong coherent pulses in conjunction with a regular photo-detector. The basic setup is illustrated in Fig. 1 (Case C). This scheme presents two main differences with respect to the passive system analyzed above. In particular, the mean photon number of the input signal states is now very high; for instance, around 10^8 photons. This fact allows Alice to use a simple regular photo-detector to measure the pulses in mode b , instead of a single photon detector. Moreover, it has an extra BS of transmittance $t2$ to attenuate the signal states in mode a and bring them to the QKD regimen. The resulting secret key rate is illustrated in Fig. 1 (Case D) [10]. We study two different situations: (1) We impose $t1=1/2$ and we optimize the parameter $t2$, and (2) we optimize both parameters. The cutoff point where the secret key rate drops down to zero is $l\approx 132\,km$ in both scenarios. This better result arises from the different form of the photon number distributions of the signals in mode a .

3. References

[1] W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett. **91**, 057901 (2003).

[2] H.-K. Lo, X. Ma and K. Chen, "Decoy State Quantum Key Distribution," Phys. Rev. Lett. **94**, 230504 (2005).

[3] X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," Phys. Rev. Lett. **94**, 230503 (2005).

[4] W. Mauerer and C. Silberhorn, "Quantum Key Distribution with Passive Decoy State Selection," Phys. Rev. A **75**, 050305(R) (2007).

[5] Y. Adachi, T. Yamamoto, M. Koashi and N. Imoto, "Simple and Efficient Quantum Key Distribution with Parametric Down-Conversion," Phys. Rev. Lett. **99**, 180503 (2007).

[6] X. Ma and H.-K. Lo, "Quantum Key Distribution with Triggering Parametric Down-Conversion Sources," New J. Phys. **10**, 073018 (2008).

[7] M. Curty, T. Moroder, X. Ma and N. Lütkenhaus, "Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution," accepted for publication in Opt. Lett. (2009). Preprint arXiv:0909.5519.

[8] Y. Adachi, T. Yamamoto, M. Koashi and N. Imoto, "Passive decoy-state quantum cryptography with pseudo-single-photon sources," in Proceedings of the 8th Asian Conference on Quantum Information Science (AQIS'08, Seoul, 2008), pp. 25-26.

[9] Y. Adachi, T. Yamamoto, M. Koashi and N. Imoto, "Boosting up quantum key distribution by learning statistics of practical single photon sources," preprint arXiv:0909.5527.

[10] M. Curty, X. Ma, B. Qi, T. Moroder and N. Lütkenhaus, "Passive decoy state quantum key distribution with practical light sources," in preparation (2009).

[11] D. Gottesman, H.-K. Lo, N. Lütkenhaus and J. Preskill, "Security of quantum key distribution with imperfect devices," Quantum Inf. Comput. **4**, 325-360 (2004).

[12] H.-K. Lo, "Getting something out of nothing," Quantum Inf. Comput. **5**, 413-418 (2005).

[13] C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, (IEEE Press, New York, 1984), pp. 175-179.

[14] H.-K. Lo, H. F. Chau and M. Ardehali, "Efficient quantum key distribution scheme and a proof of Its unconditional security," J. Cryptology **18**, 133-165 (2005).

[15] X. Ma, B. Qi, Y. Zhao and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005).

[16] C. Gobby, Z. L. Yuan and A. J. Shields, "Quantum key distribution over 122 km of standard telecom fiber," Appl. Phys. Lett. **84**, 3762-3764 (2004).