Passive Decoy State Quantum Key Distribution

Marcos Curty[1], Tobias Moroder[2,3], Xiongfeng Ma[2], and Norbert Lütkenhaus[2,3]

[1] Department of Signal Theory and Communications, ETSI Telecomunicación, University of Vigo, E-36310 Vigo, Spain
mcurty@com.uvigo.es
[2] Institute for Quantum Computing, University of Waterloo, Waterloo, ON, N2L 3G1, Canada
[3] Quantum Information Theory Group, Institut für Theoretische Physik I, and Max Planck Institute for the Science of Light, University of Erlangen-Nürnberg, 91058 Erlangen, Germany

Abstract. The use of decoy states enhances the performance of practical quantum key distribution systems significantly by monitoring the quantum channel in a more detailed way. While active modulation of the intensity of the pulses is an effective way of preparing decoy states in principle, in practice passive preparation might be desirable in some scenarios. Known passive methods involve parametric down-conversion. In this paper we show how phase randomized coherent states can be used for the same purpose. Our method involves only linear optics together with a simple threshold photon detector. The performace is comparable to the active decoy methods.

Keywords: Quantum cryptography, quantum key distribution, quantum communication, threshold photon detector.

1 Introduction

Quantum key distribution (QKD) is the first quantum information task to reach the commercial market [1]. It allows two parties (typically called Alice and Bob) to generate a cryptographic key despite the computational and technological power of an eavesdropper (Eve), who interferes with the signals [2]. This secret key is the essential ingredient of the one-time-pad or Vernam cipher, which can provide information-theoretic secure communications.

After the first demonstration of its feasibility [3], several practical implementations of QKD have been realized in recent years [4], [5], [6]. These schemes are typically based on the transmission of weak coherent pulses (WCP); especially since single photon sources are still beyond our present experimental capability. This fact opens an important security loophole. Now, some of the signals contain more than one photon prepared in the same polarization state. In this scenario, Eve is no longer limited by the no-cloning theorem since in these events the signal itself provides her with perfect copies of the signal photon. She can perform, for instance, the so-called *Photon Number Splitting* attack on the multi-photon pulses [7], [8]. This attack provides Eve with full information about the part

A. Sergienko, S. Pascazio, and P. Villoresi (Eds.): QuantumCom 2009, LNICST 36, pp. 132–141, 2010.

of the key generated with the multi-photon signals, without causing any disturbance in the signal polarization. As a result, it turns out that the standard BB84 protocol [9] with WCP can deliver a key generation rate of order $O(\eta^2)$, where η denotes the transmission efficiency of the quantum channel [10,11]. This performance contrasts with the one expected from a QKD scheme using a single photon source, where the key generation rate scales linearly with η.

A significant improvement of the secret key rate can be obtained when the original hardware is slightly modified. In particular, it has been recently shown that decoy state QKD with WCP can basically reach the same performance as single photon sources [12], [13], [14]. In this approach, Alice varies, independently and at random, the mean photon number of each signal state she sends to Bob by employing different intensity settings. This is usually performed by using a variable optical attenuator together with a random number generator. 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 resulting secret key rate. This technique has been successfully implemented in several recent experiments [15], [16], [17], which show the practical feasibility of this method.

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 rely on the use of a parametric down-conversion source together with a photon detector [18], [19], [20]. In this paper we show that phase randomized WCP can also be used for the same purpose, *i.e.*, one does not need to employ a non-linear optics network preparing entangled states. The main idea is rather simple, although it is counter-intuitive [21]. 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 at a BS. By measuring one of the two outcome signals, the conditional photon number distribution of the other one varies depending on the result obtained. This measurement can be performed, for instance, with a simple threshold photon detector. In the asymptotic limit of an infinite long experiment, we show that our passive decoy scheme can provide a similar performance to the one achieved with an active source and infinity decoy settings. This idea can also be applied to other practical scenarios with different signals and detectors like, for example, those based on thermal states or even strong coherent pulses in conjunction with a regular photo-detector [22]. In this context, see also [23].

2 Passive Decoy State QKD Setup

The basic setup is illustrated in Fig. 1 (Case A). Suppose two phase randomized WCP,

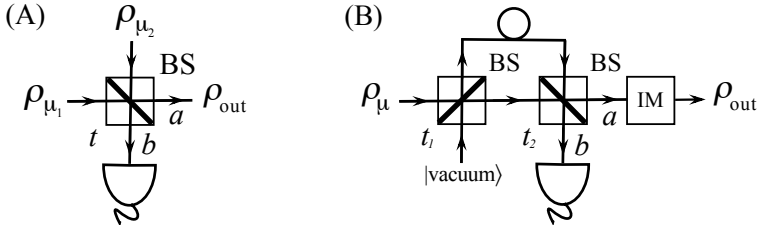

Fig. 1. (A) Basic setup of a passive decoy state QKD scheme: Interference of two phase randomized WCP, ρ_{μ_1} and ρ_{μ_2}, at a beam splitter (BS) of transmittance t. a and b represent the two output modes. (B) Alternative *active* setup with only one weak laser. The delay introduced by one arm of the interferometer is equal to the time difference between two pulses. The intensity modulator (IM) blocks either the even or the odd pulses.

$$\rho_{\mu_1} = e^{-\mu_1} \sum_{n=0}^{\infty} \frac{\mu_1^n}{n!} |n\rangle\langle n| \quad \text{and} \quad \rho_{\mu_2} = e^{-\mu_2} \sum_{n=0}^{\infty} \frac{\mu_2^n}{n!} |n\rangle\langle n| \,, \tag{1}$$

interfere at a BS of transmittance t. Here $|n\rangle$ denote Fock states with n photons. Then, it turns out that the photon number statistics of the two outcome signals are classically correlated [21]. To see this, let us first consider the interference of two pure coherent states with fixed phase relationship, $|\sqrt{\mu_1} e^{i\phi_1}\rangle$ and $|\sqrt{\mu_2} e^{i\phi_2}\rangle$, at a BS of transmittance t. The outcome signals are given by

$$|\sqrt{\mu_1 t} e^{i\phi_1} + i\sqrt{\mu_2(1-t)} e^{i\phi_2}\rangle_a \otimes |i\sqrt{\mu_1(1-t)} e^{i\phi_1} + \sqrt{\mu_2 t} e^{i\phi_2}\rangle_b \,. \tag{2}$$

The joint probability $p_{n,m}$ of having n photons in mode a and m photons in mode b is therefore given by the product of two Poissonian distributions:

$$p_{n,m} = e^{-\upsilon/2} \frac{(\upsilon\gamma)^n}{n!} \times e^{-\upsilon/2} \frac{[\upsilon(1-\gamma)]^m}{m!} \,, \tag{3}$$

with $\upsilon = \mu_1 + \mu_2$, $\gamma = [\mu_1 t + \mu_2(1-t) + \xi \cos\theta]/\upsilon$, $\xi = 2\sqrt{\mu_1 \mu_2 (1-t) t}$ and $\theta = \pi/2 + \phi_2 - \phi_1$. The case of two phase randomized WCP can be solved by just integrating $p_{n,m}$ over all angles θ. We obtain [21]

$$p_{n,m} = \frac{\upsilon^{n+m} e^{-\upsilon}}{n!m!} \frac{1}{2\pi} \int_0^{2\pi} \gamma^n (1-\gamma)^m d\theta \,. \tag{4}$$

By measuring one outcome signal, the conditional photon number statistics of the remaining signal varies depending on the result obtained. For simplicity, from now on we shall consider that this measurement is realized with a simple threshold photon detector. The analysis of other practical scenarios with different signals and detectors can be found in [22]. Such a detector can be characterized by a *Positive Operator Valued Measure* which contains two elements, F_{vac} and F_{click}, given by [24]

$$F_{\text{vac}} = (1-\epsilon) \sum_{n=0}^{\infty} (1-\eta_{\text{d}})^n |n\rangle\langle n| \,, \tag{5}$$

and $F_{\text{click}} = \mathbb{1} - F_{\text{vac}}$. The parameter η_{d} denotes the detection efficiency of the detector, and ϵ represents its probability of having a dark count. That is, the outcome of F_{vac} corresponds to no click in the detector, whereas the operator F_{click} gives precisely one detection click, which means at least one photon is detected.

Whenever one ignores the result of the measurement in mode b, the total probability of finding n photons in mode a can be expressed as

$$p_n^t = \sum_{m=0}^{\infty} p_{n,m} = \frac{\upsilon^n}{n!}\frac{1}{2\pi}\int_0^{2\pi} \gamma^n e^{-\upsilon\gamma} d\theta \ , \tag{6}$$

which turns out to be a non-Poissonian probability distribution. The joint probability for seeing n photons in mode a and no click in the threshold photon detector has the form

$$p_n^{\bar{c}} = (1-\epsilon)\sum_{m=0}^{\infty}(1-\eta_{\text{d}})^m p_{n,m} = (1-\epsilon)\frac{\upsilon^n e^{-\eta_{\text{d}}\upsilon}}{n!}\frac{1}{2\pi}\int_0^{2\pi} \gamma^n e^{-(1-\eta_{\text{d}})\upsilon\gamma} d\theta \ . \tag{7}$$

If the detector produces a click, the joint probability of finding n photons in mode a is given by

$$p_n^c = p_n^t - p_n^{\bar{c}} \ . \tag{8}$$

Fig. 2 (Cases A and B) shows the conditional photon number statistics of the outcome signal in mode a depending on the result of the detector (click and no click): $q_n^c \equiv p_n^c/(1-N)$ and $q_n^{\bar{c}} \equiv p_n^{\bar{c}}/N$, with

$$N \equiv \sum_{n=0}^{\infty} p_n^{\bar{c}} = (1-\epsilon)e^{-\eta_{\text{d}}[\mu_1(1-t)+\mu_2 t]} I_{0,\eta_{\text{d}}\xi} \ , \tag{9}$$

and where $I_{q,z}$ represents the modified Bessel function of the first kind [26]. This function is defined as [26]

$$I_{q,z} = \frac{1}{2\pi i}\oint e^{(z/2)(t+1/t)} t^{-q-1} dt \ . \tag{10}$$

This figure includes as well a comparison between q_n^c and a Poissonian distribution of the same mean photon number (Cases C and D). Both distributions, q_n^c and $q_n^{\bar{c}}$, are also non-Poissonian.

The passive decoy state setup illustrated in Fig. 1 (Case A) requires that Alice uses two pulsed sources of WCP. A similar result can also be obtained with only one source of phase randomized WCP. For instance, Alice could employ the scheme showed as Case B in Fig. 1. This setup has only one laser diode, but includes an intensity modulator (IM) to block either all the even or all the odd outcome pulses. It is, therefore, an active scheme. Still, this setup might be easier to implement than those standard active decoy state schemes where an IM is used to modulate each outcome pulse depending on the result of a random number generator. The main reason to have to block half of the outcome pulses is to

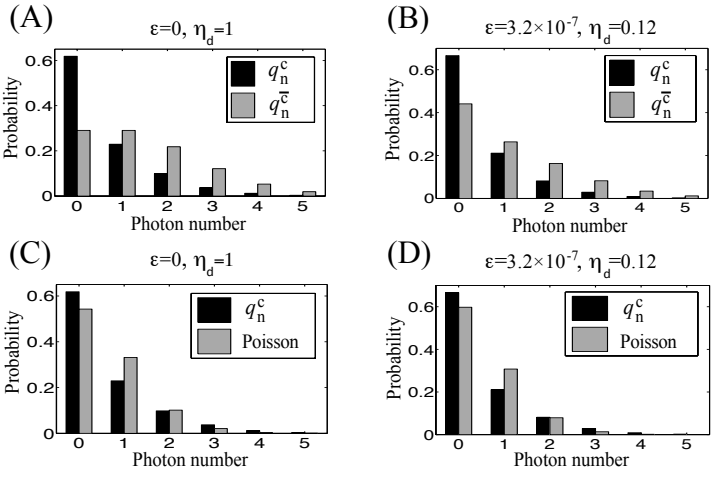

Fig. 2. Conditional photon number distribution in mode a (see Case A in Fig. 1): q_n^c (black) and $q_n^{\bar{c}}$ (grey) for the case $\mu_1 = \mu_2 = 1$ and $t = 1/2$. We consider two situations: (A) A perfect threshold photon detector, *i.e.*, $\epsilon = 0$ and $\eta_{\rm d} = 1$ [21], and (B) $\epsilon = 3.2{\times}10^{-7}$ and $\eta_{\rm d} = 0.12$. These last data correspond to the experiment reported in [25]. The Cases C and D represent q_n^c (black) versus a Poissonian distribution of the same mean photon number for the two scenarios described above (perfect and imperfect threshold photon detector).

suppress correlations between them. That is, the action of the IM guarantees that the outcome signals consist of tensor product of classical mixtures of Fock states. Thanks to the one-pulse delay introduced by one arm of the interferometer, together with a proper selection of the transmittance t_1, it can be shown that both cases, A and B in Fig. 1, are equivalent, except from the resulting secret key rate. Specifically, the secret key rate in Case B is half the one that can be obtained in Case A, since half of the pulses are now discarded.

3 Lower Bound on the Secret Key Rate

We consider that Alice and Bob treat no click and click events separately, and they distill secret key from both of them. We use the secret key rate formula provided by [11], [27],

$$R \geq \max\{R^c, 0\} + \max\{R^{\bar{c}}, 0\} \, , \tag{11}$$

with

$$\begin{aligned} R^c \geq \; & q\{-Q^c f(E^c) H(E^c) + p_1^c Y_1 [1 - H(e_1)] + p_0^c Y_0\} \\ \geq \; & q\{-Q^c f(E^c) H(E^c) + (p_1^c Y_1 + p_0^c Y_0)[1 - H(e_1^u)]\} \, , \end{aligned} \tag{12}$$

and similarly for $R^{\bar{c}}$. The parameter q is the efficiency of the protocol ($q = 1/2$ for the standard Bennett-Brassard 1984 protocol [9], and $q \approx 1$ for its efficient version [28]), Q^c is the overall gain of the signals, E^c represents the overall quantum bit error rate (QBER), $f(E^c)$ is the error correction efficiency [typically $f(E^c) \geq 1$ with Shannon limit $f(E^c) = 1$], Y_n denotes the yield of a n-photon signal, *i.e.*, the conditional probability of a detection event on Bob's side given that Alice transmits an n-photon state, e_1 is the single photon error rate, e_1^u represents an upper bound on e_1, and $H(x) = -x \log_2(x) - (1-x)\log_2(1-x)$ is the binary Shannon entropy function.

The quantities Q^c, E^c, $Q^{\bar{c}}$, and $E^{\bar{c}}$ are directly accessible from the experiment. They can be expressed as

$$Q^c = \sum_{n=0}^{\infty} p_n^c Y_n \quad \text{and} \quad Q^c E^c = \sum_{n=0}^{\infty} p_n^c Y_n e_n \,, \tag{13}$$

and similarly for the case of a no click event. Here e_n denotes the error rate of a n-photon signal ($e_0 = 1/2$ for random background).

To apply the secret key rate formula given by Eq. (11) one needs to estimate a lower bound on the quantity $p_1^c Y_1 + p_0^c Y_0$, together with an upper bound on e_1. For that, we follow the procedure proposed in [29]. This method requires that p_n^t and $p_n^{\bar{c}}$ satisfy certain conditions that we checked numerically. Note, however, that many other estimation techniques are also available, like, for instance, linear programming tools [30]. We find that

$$p_1^c Y_1 + p_0^c Y_0 \geq p_1^c Y_1^l + p_0^c Y_0^u \,, \tag{14}$$

with

$$Y_1^l \equiv \max\left\{0, \frac{p_2^{\bar{c}} Q^t - p_2^t Q^{\bar{c}} - (p_2^{\bar{c}} p_0^t - p_2^t p_0^{\bar{c}}) Y_0^u}{p_2^{\bar{c}} p_1^t - p_2^t p_1^{\bar{c}}}\right\} , \tag{15}$$

where $Q^t = Q^c + Q^{\bar{c}}$, and Y_0^u denotes an upper bound on the background rate Y_0 given by

$$Y_0^u \equiv \min\left\{\frac{2E^{\bar{c}} Q^{\bar{c}}}{p_0^{\bar{c}}}, \frac{2E^t Q^t}{p_0^t}\right\} . \tag{16}$$

The error rate e_1 can be upper bounded as

$$e_1 \leq e_1^u \equiv \min\left\{\frac{E^{\bar{c}} Q^{\bar{c}} - p_0^{\bar{c}} Y_0^l e_0}{p_1^{\bar{c}} Y_1^l}, \frac{E^c Q^c - p_0^c Y_0^l e_0}{p_1^c Y_1^l}, \frac{p_0^{\bar{c}} E^t Q^t - p_0^t E^{\bar{c}} Q^{\bar{c}}}{(p_0^{\bar{c}} p_1^t - p_0^t p_1^{\bar{c}}) Y_1^l}\right\} , \tag{17}$$

with $Q^t E^t = Q^c E^c + Q^{\bar{c}} E^{\bar{c}}$, and where Y_0^l denotes a lower bound on Y_0 given by

$$Y_0 \geq Y_0^l \equiv \max\left\{0, \frac{p_1^t Q^{\bar{c}} - p_1^{\bar{c}} Q^t}{p_1^t p_0^{\bar{c}} - p_1^{\bar{c}} p_0^t}\right\} . \tag{18}$$

The only relevant statistics to evaluate Y_0^l, Y_0^u, Y_1^l, and e_1^u are p_n^t and $p_n^{\bar{c}}$, with $n = 0, 1, 2$. These probabilities can be obtained by solving Eqs. (6)-(7). They are given in the Appendix.

4 Evaluation

For simulation purposes we employ the channel model used in [13], [29]. This model reproduces a normal behavior of a quantum channel, *i.e.*, in the absence of eavesdropping. It allows us to calculate the observed experimental parameters $Q^{\bar{c}}$, $E^{\bar{c}}$, Q^t, and E^t. Our results, however, can also be applied to any other quantum channel, as they only depend on the observed gains and QBERs. In the scenario considered, the yields have the form

$$Y_n = 1 - (1 - Y_0)(1 - \eta_{\rm sys})^n \ , \tag{19}$$

where $\eta_{\rm sys}$ represents the overall transmittance of the system [13], [29]. That is, $\eta_{\rm sys}$ includes the transmission efficiency of the quantum channel and that of Bob's detection apparatus. This parameter can be related with a transmission distance l measured in km for the given QKD scheme as $\eta_{\rm sys} = 10^{-\frac{\alpha l}{10}}$, where α represents the loss coefficient of the optical fiber measured in dB/km. The product $Y_n e_n$ can be expressed as

$$Y_n e_n = Y_0 e_0 + (Y_n - Y_0) e_d \ , \tag{20}$$

where e_d is the probability that a photon hits the wrong detector due to the misalignment in the quantum channel and in Bob's detection setup [13], [29]. After substituting these definitions into the gain and QBER formulas we obtain

$$\begin{aligned} Q^{\bar{c}} &= N - (1-\epsilon)(1-Y_0) e^{(\eta_{\rm d} - \eta_{\rm sys})\omega - \eta_{\rm d}\upsilon} I_{0,(\eta_{\rm d} - \eta_{\rm sys})\xi} \ , \\ Q^{\bar{c}} E^{\bar{c}} &= (e_0 - e_d) Y_0 N + e_d Q^{\bar{c}} \ , \\ Q^t &= 1 - (1 - Y_0) e^{-\eta_{\rm sys}\omega} I_{0,\eta_{\rm sys}\xi} \ , \\ Q^t E^t &= (e_0 - e_d) Y_0 + e_d Q^t \ , \end{aligned} \tag{21}$$

with $\omega = \mu_1 t + \mu_2 (1 - t)$.

The resulting lower bound on the secret key rate is illustrated in Fig. 3. The experimental parameters are [25]: $Y_0 = 1.7 \times 10^{-6}$, $e_d = 0.033$, $\alpha = 0.21$ dB/km, and Bob's detection efficiency equal to 0.045. We assume that $q = 1$, $f(E^c) = f(E^{\bar{c}}) = 1.22$, and $t = 1/2$, *i.e.*, we consider a simple $50 : 50$ BS. We study two different situations: (1) $\epsilon = 0$ and $\eta_{\rm d} = 1$ [21], and (2) $\epsilon = 3.2 \times 10^{-7}$ and $\eta_{\rm d} = 0.12$ [25]. In both cases the optimal values of the intensities μ_1 and μ_2 are almost constant with the distance. One of them is quite weak (around 10^{-4}), while the other one is around 0.5. Fig. 3 includes as well the case of an active asymptotic decoy state QKD system [13]. 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, one may employ a photon number resolving detector instead of a simple threshold photon detector, or use more threshold detectors in combination with BS [22]. 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.

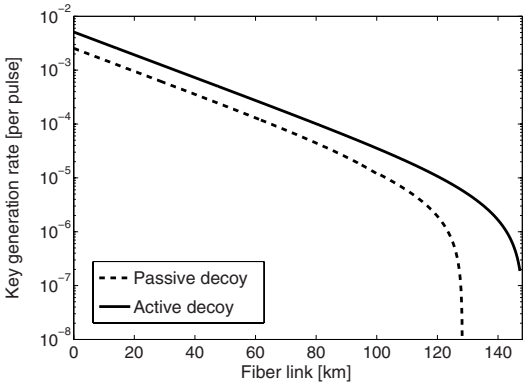

Fig. 3. Lower bound on the secret key rate R given by Eq. (11) in logarithmic scale for the passive decoy state setup given by Fig. 1 (Case A) with two intensity settings. The transmittance of the BS is $t = 1/2$. We consider two possible scenarios: (1) $\epsilon = 0$ and $\eta_{\rm d} = 1$ [21] (*i.e.*, a perfect threshold photon detector), and (2) $\epsilon = 3.2 \times 10^{-7}$ and $\eta_{\rm d} = 0.12$ [25]. 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 R for an active asymptotic decoy state system [13].

5 Conclusion

We have presented a passive decoy state QKD system with phase randomized WCP. This setup uses only linear optical elements and a simple threshold photon detector. It represents an alternative to those active schemes based on the use of a variable optical attenuator together with a random number generator. Moreover, in the asymptotic limit of an infinite long experiment, we have shown that this passive system can provide a similar performance to the one achieved with an active source and infinity decoy settings.

Acknowledgments. The authors wish to thank R. Kaltenbaek, H.-K. Lo, B. Qi, and Y. Zhao for very useful discussions, and in particular M. Koashi for pointing out a reference. M.C. especially thanks the Institute for Quantum Computing (University of Waterloo) for hospitality and support during his stay in this institution. This work was supported by the European Projects SECOQC and QAP, by the NSERC Discovery Grant, Quantum Works, CSEC, and by Xunta de Galicia (Spain, Grant No. INCITE08PXIB322257PR).

References

1. idQuantique, Geneva (Switzerland), `www.idquantique.com`; MagiQ Technologies, Inc., New York., `www.magiqtech.com`; and Smartquantum, Lannion (France), `www.smartquantum.com`

2. Scarani, V., Bechmann-Pasquinucci, H., Cerf, N.J., Dušek, M., Lütkenhaus, N., Peev, M.: The Security of Practical Quantum Key Distribution. Rev. Mod. Phys. (accepted for publication, 2009), Preprint quant-ph/0802.4155
3. Bennett, C.H., Bessette, F., Brassard, G., Salvail, L., Smolin, J.: Experimental Quantum Cryptography. Cryptology 5, 3–28 (1992)
4. Marand, C., Townsend, P.D.: Quantum key distribution over distances as long as 30 km. Opt. Lett. 20, 1695–1697 (1995)
5. Muller, A., Zbinden, H., Gisin, N.: Underwater quantum coding. Nature 378, 449–449 (1995)
6. Hughes, R., Morgan, G., Peterson, C.G.: Quantum key distribution over a 48km optical fibre network. J. Mod. Opt. 47, 533–547 (2000)
7. Huttner, B., Imoto, N., Gisin, N., Mor, T.: Quantum Cryptography with Coherent States. Phys. Rev. A 51, 1863–1869 (1995)
8. Brassard, G., Lütkenhaus, N., Mor, T., Sanders, B.C.: Limitations on Practical Quantum Cryptography. Phys. Rev. Lett. 85, 1330–1333 (2000)
9. Bennett, C.H., Brassard, G.: Quantum cryptography: public key distribution and coin tossing. In: IEEE International Conference on Computers, Systems and Signal Processing, pp. 175–179. IEEE Press, New York (1984)
10. Inamori, H., Lütkenhaus, N., Mayers, D.: Unconditional security of practical quantum key distribution. Eur. Phys. J. D 41, 599–627 (2007)
11. Gottesman, D., Lo, H.-K., Lütkenhaus, N., Preskill, J.: Security of quantum key distribution with imperfect devices. Quantum Inf. Comput. 4, 325–360 (2004)
12. Hwang, W.-Y.: Quantum Key Distribution with High Loss: Toward Global Secure Communication. Phys. Rev. Lett. 91, 57901 (2003)
13. Lo, H.-K., Ma, X., Chen, K.: Decoy State Quantum Key Distribution. Phys. Rev. Lett. 94, 230504 (2005)
14. Wang, X.-B.: Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography. Phys. Rev. Lett. 94, 230503 (2005)
15. Zhao, Y., Qi, B., Ma, X., Lo, H.-K., Qian, L.: Experimental Quantum Key Distribution with Decoy States. Phys. Rev. Lett. 96, 070502 (2006)
16. Rosenberg, D., Harrington, J.W., Rice, P.R., Hiskett, P.A., Peterson, C.G., Hughes, R.J., Lita, A.E., Nam, S.W., Nordholt, J.E.: Long-Distance Decoy-State Quantum Key Distribution in Optical Fiber. Phys. Rev. Lett. 98, 010503 (2007)
17. Schmitt-Manderbach, T., Weier, H., Fürst, M., Ursin, R., Tiefenbacher, F., Scheidl, T., Perdigues, J., Sodnik, Z., Kurtsiefer, C., Rarity, J.G., Zeilinger, A., Weinfurter, H.: Experimental Demonstration of Free-Space Decoy-State Quantum Key Distribution over 144 km. Phys. Rev. Lett. 98, 010504 (2007)
18. Mauerer, W., Silberhorn, C.: Quantum Key Distribution with Passive Decoy State Selection. Phys. Rev. A 75, 050305(R) (2007)
19. Adachi, Y., Yamamoto, T., Koashi, M., Imoto, N.: Simple and Efficient Quantum Key Distribution with Parametric Down-Conversion. Phys. Rev. Lett. 99, 180503 (2007)
20. Ma, X., Lo, H.-K.: Quantum Key Distribution with Triggering Parametric Down-Conversion Sources. New J. Phys. 10, 073018 (2008)
21. Curty, M., Moroder, T., Ma, X., Lütkenhaus, N.: Non-Poissonian statistics from Poissonian light sources with application to passive decoy state quantum key distribution. Accepted for publication in Opt. Lett. (2009)
22. Curty, M., Ma, X., Qi, B., Moroder, T., Lütkenhaus, N.: In preparation (2009)
23. Adachi, Y., Yamamoto, T., Koashi, M., Imoto, N.: Passive decoy-state quantum cryptography with pseudo-single-photon sources. In: 8th Asian Conference on Quantum Information Science (AQIS 2008), Seoul, pp. 25–26 (2008)

24. Rohde, P.P., Ralph, T.C.: Modelling photo-detectors in quantum optics. J. Mod. Opt. 53, 1589–1603 (2006)
25. Gobby, C., Yuan, Z.L., Shields, A.J.: Quantum key distribution over 122 km of standard telecom fiber. Appl. Phys. Lett. 84, 3762–3764 (2004)
26. Arfken, G.: Mathematical Methods for Physicists, 3rd edn. Academic Press, London (1985)
27. Lo, H.-K.: Getting something out of nothing. Quantum Inf. Comput. 5, 413–418 (2005)
28. Lo, H.-K., Chau, H.F., Ardehali, M.: Efficient quantum key distribution scheme and a proof of Its unconditional security. J. Cryptology 18, 133–165 (2005)
29. Ma, X., Qi, B., Zhao, Y., Lo, H.-K.: Practical decoy state for quantum key distribution. Phys. Rev. A 72, 012326 (2005)
30. Bazaraa, M.S., Jarvis, J.J., Sherali, H.D.: Linear Programming and Network Flows, 3rd edn. Wiley, Chichester (2004)

Appendix: Probabilities p_n^t and $p_n^{\bar{c}}$

In this Appendix we provide explicit expressions for the probabilities p_n^t and $p_n^{\bar{c}}$, with $n = 0, 1, 2$. In particular, we have that

$$\begin{aligned} p_0^t &= I_{0,\xi} e^{-\omega} \,, \\ p_1^t &= (\omega I_{0,\xi} - \xi I_{1,\xi}) e^{-\omega} \,, \\ p_2^t &= \frac{1}{2}[\omega^2 I_{0,\xi} + (1-2\omega)\xi I_{1,\xi} + \xi^2 I_{2,\xi}] e^{-\omega} \,, \end{aligned} \tag{22}$$

with $\omega = \mu_1 t + \mu_2(1-t)$. The probabilities $p_n^{\bar{c}}$ have the form

$$\begin{aligned} p_0^{\bar{c}} &= \tau I_{0,(1-\eta_{\rm d})\xi} \,, \\ p_1^{\bar{c}} &= \tau\Big(\omega I_{0,(1-\eta_{\rm d})\xi} - \xi I_{1,(1-\eta_{\rm d})\xi}\Big) \,, \\ p_2^{\bar{c}} &= \frac{\tau}{2}\Big\{\omega^2 I_{0,(1-\eta_{\rm d})\xi} + \Big[\frac{1}{1-\eta_{\rm d}} - 2\omega\Big]\xi I_{1,(1-\eta_{\rm d})\xi} + \xi^2 I_{2,(1-\eta_{\rm d})\xi}\Big\} \,, \end{aligned} \tag{23}$$

where $\tau = (1-\epsilon)e^{-[\eta_{\rm d}\upsilon + (1-\eta_{\rm d})\omega]}$.