Long-distance practical quantum key distribution by entanglement swapping

Artur Scherer,* Barry C. Sanders, and Wolfgang Tittel

Institute for Quantum Information Science, University of Calgary, Calgary, AB, Canada T2N 1N4

**ascherer@ucalgary.ca*

Abstract: We develop a model for practical, entanglement-based long-distance quantum key distribution employing entanglement swapping as a key building block. Relying only on existing off-the-shelf technology, we show how to optimize resources so as to maximize secret key distribution rates. The tools comprise lossy transmission links, such as telecom optical fibers or free space, parametric down-conversion sources of entangled photon pairs, and threshold detectors that are inefficient and have dark counts. Our analysis provides the optimal trade-off between detector efficiency and dark counts, which are usually competing, as well as the optimal source brightness that maximizes the secret key rate for specified distances (i.e. loss) between sender and receiver.

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

References and links

1. http://www.idquantique.com, http://www.magiqtech.com
2. N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, "Quantum cryptography," Rev. Mod. Phys. **74**, 145–195 (2002).
3. E. Waks, A. Zeevi, and Y. Yamamoto, "Security of quantum key distribution with entangled photons against individual attacks," Phys. Rev. A **65**, 052310 (2002).
4. B. C. Jacobs, T. B. Pittman, and D. Franson, "Quantum relays and noise suppression using linear optics," Phys. Rev. A **66**, 052307 (2002).
5. H. de Riedmatten, I. Marcikic, W. Tittel, H. Zbinden, D. Collins, and N. Gisin, "Long Distance Quantum Teleportation in a Quantum Relay Configuration," Phys. Rev. Lett. **92**, 047904 (2004).
6. D. Collins, N. Gisin, and H. de Riedmatten, "Quantum relays for long distance quantum cryptography," J. Mod. Opt. **52**, 735–753 (2005).
7. H. J. Briegel, W. Dür, J. I. Cirac, and P. Zoller, "Quantum Repeaters: The Role of Imperfect Local Operations in Quantum Communication," Phys. Rev. Lett. **81**, 5932–5935 (1998).
8. M. Żukowski, A. Zeilinger, M. A. Horne, and A. K. Ekert, "'Event-ready-detectors' Bell experiment via entanglement swapping," Phys. Rev. Lett. **71**, 4287–4290 (1993).
9. A. Scherer, G. Howard, B. C. Sanders, and W. Tittel, "Quantum states prepared by realistic entanglement swapping," Phys. Rev. A **80**, 062310 (2009).
10. 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**, 1301–1350 (2009).
11. G. Brassard, N. Lütkenhaus, T. Mor, and B. C. Sanders, "Limitations on Practical Quantum Cryptography," Phys. Rev. Lett. **85**, 1330–1333 (2000).
12. C. H. Bennett and G. Brassard, "Quantum cryptography: public key distribution and coin tossing," in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (Institute of Electrical and Electronics Engineers, Bangalore, India, 1984), pp. 175–179.
13. X. Ma, C.-H. F. Fung, and H.-K. Lo, "Quantum key distribution with entangled photon sources," Phys. Rev. A **76**, 012307 (2007).
14. I. Marcikic, H. de Riedmatten, W. Tittel, V. Scarani, H. Zbinden, and N. Gisin, "Time-bin entangled qubits for quantum communication created by femtosecond pulses," Phys. Rev. A **66**, 062308 (2002).

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

15. H. de Riedmatten, V. Scarani, I. Marcikic, A. Acín, W. Tittel, H. Zbinden, and N. Gisin, "Two independent photon pairs versus four-photon entangled states in parametric down conversion," J. Mod. Opt. **51**, 1637–1649 (2004).
16. C. H. Bennett, G. Brassard, and N. D. Mermin, "Quantum cryptography without Bell's theorem," Phys. Rev. Lett. **68**, 557–559 (1992).
17. W.-Y. Hwang, "Quantum Key Distribution with High Loss: Toward Global Secure Communication," Phys. Rev. Lett. **91**, 057901 (2003).
18. X.-B. Wang, "Beating the Photon-Number-Splitting Attack in Practical Quantum Cryptography," Phys. Rev. Lett. **94**, 230503 (2005).
19. H.-K. Lo, X. Ma, and K. Chen, "Decoy State Quantum Key Distribution," Phys. Rev. Lett. **94**, 230504 (2005).
20. X. Ma, B. Qi, Y. Zhao, and H.-K. Lo, "Practical decoy state for quantum key distribution," Phys. Rev. A **72**, 012326 (2005).
21. X.-B. Wang, "Decoy-state protocol for quantum cryptography with four different intensities of coherent light," Phys. Rev. A **72**, 012322 (2005).
22. Y. Zhao, B. Qi, X. Ma, H.-K. Lo, and L. Qian, "Experimental Quantum Key Distribution with Decoy States," Phys. Rev. Lett. **96**, 070502 (2006).
23. N. Lütkenhaus, "Security against individual attacks for realistic quantum key distribution," Phys. Rev. A **61**, 052304 (2000).
24. l.-M. Duan, M. D. Lukin, J. I. Cirac, and P. Zoller, "Long-distance quantum communication with atomic ensembles and linear optics," Nature **414**, 413–418, 2001.
25. J. B. Brask and A. S. Sørensen, "Memory imperfections in atomic-ensemble-based quantum repeaters," Phys. Rev. A **78**, 012350 (2008).
26. L. Jiang, J. M. Taylor, and M. D. Lukin, "Fast and robust approach to long-distance quantum communication with atomic ensembles," Phys. Rev. A **76**, 012301 (2007).
27. B. Zhao, Z.-B. Chen, Y.-A. Chen, J. Schmiedmayer, and J.-W. Pan, "Robust creation of entanglement between remote memory qubits," Phys. Rev. Lett. **98**, 240502 (2007).
28. J. B. Brask, L. Jiang, A. V. Gorshkov, V. Vuletic, A. S. Sørensen, and M. D. Lukin "Fast entanglement distribution with atomic ensembles and fluorescent detection," Phys. Rev. A **81**, 020303 (2010).
29. J. Amirloo, M. Razavi, and A. H. Majedi, "Quantum key distribution over probabilistic quantum repeaters," Phys. Rev. A **82**, 032304 (2010).
30. A. J. Miller, S. W. Nam, J. M. Martinis, and A. V. Sergienko, "Demonstration of a low-noise near-infrared photon counter with multiphoton discrimination," Appl. Phys. Lett. **83**, 791–793 (2003).
31. D. Rosenberg, A. E. Lita, A. J. Miller, S. W. Nam, and R. E. Schwall, " Performance of photon-number resolving transition-edge sensors with integrated 1550 nm resonant cavities," IEEE Trans. Appl. Supercond. **15**(2), 575–578 (2005).
32. D. Rosenberg, A. E. Lita, A. J. Miller, and S. W. Nam, "Noise-free high-efficiency photon-number-resolving detectors," Phys. Rev. A **71**, 061803 (2005).
33. G. N. Gol'tsman, O. Okunev, G. Chulkova, A. Lipatov, A. Semenov, K. Smirnov, B. Voronov, A. Dzardanov, C. Williams, and R. Sobolewski, "Picosecond superconducting single-photon optical detector," Appl. Phys. Lett. **79**, 705–707 (2001).
34. K. M. Rosfjord, J. K. W. Yang, E. A. Dauler, A. J. Kerman, V. Anant, B. M. Voronov, G. N. Gol'tsman, and K. K. Berggren, "Nanowire single-photon detector with an integrated optical cavity and anti-reflection coating," Opt. Express **14**, 527–534 (2006).
35. A. J. Kerman, E. A. Dauler, W. E. Keicher, J. K. W. Yang, K. K. Berggren, G. Gol'tsman, and B. Voronov, "Kinetic-inductance-limited reset time of superconducting nanowire photon counters," Appl. Phys. Lett. **88**, 111116 (2006).
36. A. Divochiy, F. Marsili, D. Bitauld, A. Gaggero, R. Leoni, F. Mattioli, A. Korneev, V. Seleznev, N. Kaurova, O. Minaeva, G. Gol'tsman, K. G. Lagoudakis, M. Benkhaoul, F. Lévy, and A. Fiore, "Superconducting nanowire photon-number-resolving detector at telecommunication wavelengths," Nat. Photonics **2**, 302–306 (2008).
37. H. Hübel, M. R. Vanner, T. Lederer, B. Blauensteiner, T. Lorünser, A. Poppe, and A. Zeilinger, "High-fidelity transmission of polarization encoded qubits from an entangled source over 100 km of fiber," Opt. Express **15**, 7853–7862 (2007).
38. R. Ursin, F. Tiefenbacher, T. Schmitt-Manderbach, H. Weier, T. Scheidl, M. Lindenthal, B. Blauensteiner, T. Jennewein, J. Perdigues, P. Trojek, B. Ömer, M. Fürst, M. Meyenburg, J. Rarity, Z. Sodnik, C. Barbieri, H. Weinfurter, and A. Zeilinger, "Entanglement-based quantum communication over 144 km," Nat. Phys. **3**, 481–486 (2007).
39. M. Halder, A. Beveratos, N. Gisin, V. Scarani, C. Simon, and H. Zbinden, " Entangling independent photons by time measurement," Nat. Phys. **3**, 692–695 (2007)
40. E. Saglamyurek, N. Sinclair, J. Jin, J. A. Slater, D. Oblak, F. Bussires, M. George, R. Ricken, W. Sohler, and W. Tittel, "Broadband waveguide quantum memory for entangled photons," Nature, 12 January 2011.
41. G. B. Xavier, G. Vilela de Faria, G. P. Temporão, and J. P. von der Weid, "Full polarization control for fiber optical quantum communication systems using polarization encoding," Opt. Express **16**, 1867–1873 (2008).
42. I. Lucio-Martinez, P. Chan, X. Mo, S. Hosier, and W. Tittel, "Proof-of-concept of real-world quantum key dis-

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

tribution with quantum frames," N. J. Phys. **11**, 095001 (2009).
43. H. de Riedmatten, I. Marcikic, J. A. W. van Houwelingen, W. Tittel, H. Zbinden and N. Gisin, "Long-distance entanglement swapping with photons from separated sources," Phys. Rev. A **71**, 050302 (2005).
44. J. G. Rarity and P. R. Tapster, "Experimental violation of Bell's inequality based on phase and momentum," Phys. Rev. Lett. **64**, 2495–2498 (1990).
45. P. W. Shor and J. Preskill, "Simple Proof of Security of the BB84 Quantum Key Distribution Protocol," Phys. Rev. Lett. **85**, 441–444 (2000).
46. J. Calsamiglia and N. Lütkenhaus, "Maximum efficiency of a linear-optical Bell-state analyzer," Appl. Phys. B **72**, 67–71 (2001).
47. G. Brassard and L. Salvail, "Secret-Key Reconciliation by Public Discussion," in *Advances in Cryptology – EUROCRYPT '93 (Lecture Notes in Computer Science, Vol.* **765***)* (Springer, Berlin, 1994), pp. 410–423.
48. M. Koashi and J. Preskill, "Secure Quantum Key Distribution with an Uncharacterized Source," Phys. Rev. Lett. **90**, 057902 (2003).
49. N. J. Beaudry, T. Moroder, and N. Lütkenhaus, "Squashing Models for Optical Measurements in Quantum Communication," Phys. Rev. Lett. **101**, 093601 (2008).
50. T. Moroder, O. Gühne, N. J. Beaudry, M. Piani, and N. Lütkenhaus, "Entanglement verification with realistic measurement devices via squashing operations," Phys. Rev. A **81**, 052342 (2010).

1. Introduction

Quantum cryptography technologies have matured to commercial applications [1]. Yet long-distance quantum communication and particularly long-distance quantum key distribution (QKD) are hampered by exponential channel loss of photons with respect to transmission distance. Quantum relays [2, 3, 4, 5, 6] and quantum repeaters [7] could solve these distance limits by exploiting entanglement swapping (ES) [8] between photon pairs as a key building block. However, ES based on present technology is performance-limited due to real-world imperfections.

ES is achieved with two sources of entangled photon pairs (EPPs) and a joint Bell-state measurement (BSM) performed on two of their outputs, specifically one from each source. Realistic EPP sources are probabilistic, and occasionally emit two or more independent EPPs. Spontaneous parametric down-conversion (PDC) in nonlinear crystals is the most common way to produce EPPs. Detectors used to perform BSM are inefficient and suffer from dark counts. Aiming at realistic aspects of ES-based QKD, we have studied the effect of experimental imperfections on ES-generated entangled quantum states (in terms of their fidelity with a target Bell state) via a *non-perturbative* mathematical model for practical ES accounting for detector inefficiencies, detector dark counts and multipair events [9]. Our closed-form solution for realistic ES-generated quantum states determines the " amount" of useful entanglement, which depends on experimental parameters such as dark-count rates and efficiencies of off-the-shelf detectors as well as brightness of PDC sources. This realism makes our model useful for planning long-distance QKD experiments employing ES, which is demonstrated in this paper.

The impact of real-world imperfections on the performance and communication range of QKD has been the objective of numerous recent investigations [10]. In [11] Brassard et al. showed that channel losses, a realistic detection process, and qubit-source imperfections drastically impair the feasibility of QKD over long distances. In particular, it was shown in [11] that unconditional security is difficult to achieve in long-distance QKD based on the BB84 protocol [12] realized by attenuated laser pulses instead of by idealized single-photon on-demand sources; in the same work, a superior performance was obtained for QKD schemes based on a single PDC source. The consequences of using probabilistic EPP sources (realized by PDC) instead of by single-pair on-demand sources for quantum communication including entanglement-based QKD have been investigated [13, 14, 15].

For long distances, the entanglement-based BBM92 QKD protocol [16] with a single PDC source placed midway between the two communicating parties was shown to perform significantly better than BB84-based QKD realized by faint coherent-state pulses under the restric-

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

tion to individual eavesdropping attacks and trusted noisy detectors [3]. Even though faint-pulse BB84 QKD with *decoy states* (decoy-BB84 QKD) [17, 18, 19, 20, 21, 22] permits much larger communication ranges than conventional faint-pulse BB84 QKD without decoy states, PDC-based BBM92 QKD with the source in the middle tolerates higher channel loss and thus enables longer communication distance than decoy-BB84 QKD [13], setting aside the fact that the latter protocol can realize appreciably higher key-distribution rates than the former for medium- and low-loss settings. Moreover, for *ideal* EPP sources, ES-based BBM92 QKD schemes were proven to allow achieving even greater distances at the cost of smaller communication rates [3, 6].

Here we extend our entanglement-swapping model [9] to practical QKD based on distributing entangled photons over extended distances by ES and relying only on existing off-the-shelf technology. The resources we consider are (i) lossy transmission links, such as telecom optical fibers or free space, (ii) spontaneous PDC to produce EPPs and (iii) inefficient, noisy threshold detectors. We show how to employ these resources so as to optimize QKD performance. We determine the QKD figures of merit *quantum bit error rate* (QBER) and *secret key rate* as functions of experimental parameters. Our theory permits constrained optimization of the experimentally tunable detector efficiencies and dark count rates as well as brightness of PDC thereby yielding optimal QKD performance for any distance d between sender Alice and receiver Bob.

Determining optimal source brightness is important for both faint-pulse BB84 QKD and PDC-based BBM92 QKD. Low source brightness implies a low key-generation rate. However, as the source brightness increases, the multiphoton-signal probability for faint-pulse BB84 QKD or multipair probability for PDC-based BBM92 QKD rises. In faint-pulse BB84 QKD, multiphoton signals are vulnerable to photon number splitting (PNS) attacks which jeopardize QKD security. Decoy states [17, 18, 19, 20]) are generally used as a remedy to tackle this problem. Although PNS attacks do not help an eavesdropper in PDC-based BBM92 QKD [2, 6], occasional multipairs cause erroneous heralding events, thus contributing to QBER (see Sec. 2).

The optimal mean photon number per signal for faint-pulse coherent-state QKD can be determined [20, 23] as well as the optimal source brightness for PDC-based BBM92 QKD with a single PDC source placed midway between sender and receiver [13]. Although the effects of transmission losses, detector inefficiencies and dark counts on the performance of quantum relays has been examined [6], the probabilistic nature of realistic EPP sources including occasional multipair events has not yet been incorporated. Our analysis yields optimal PDC-source brightness for PDC-based BBM92 QKD exploiting ES as a crucial tool (PDC-ES-BBM92 QKD) for any channel distance given an empirical constraint between efficiency and dark counts for common off-the-shelf detectors.

Multi-excitation events, as significant sources of error, have been considered in other recent investigations that elaborate on practical implementations of the DLCZ quantum repeater scheme [24]. The effects of multipair events in PDC, in addition to transmission losses, detector and quantum memory imperfections on quantum repeater performance, have been accounted for perturbatively [25]. The atom-light entangled states produced by Stokes scattering in the DLCZ scheme are similar to the light-light entangled states produced by non-degenerate PDC, as both are two-mode squeezed states. In these works [26, 27, 28] the impact of multi-excitation contributions in such atom-light entangled states has also been taken into account perturbatively. A more thorough analysis of multi-excitation events in atomic-ensemble memories has been provided in [29]. Our theory is based on a substantially different approach, which is non-perturbative and uses the principle of Bayesian inference to account for the presence of experimental imperfections.

Finally, we address the communication range and corresponding key generation rates

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

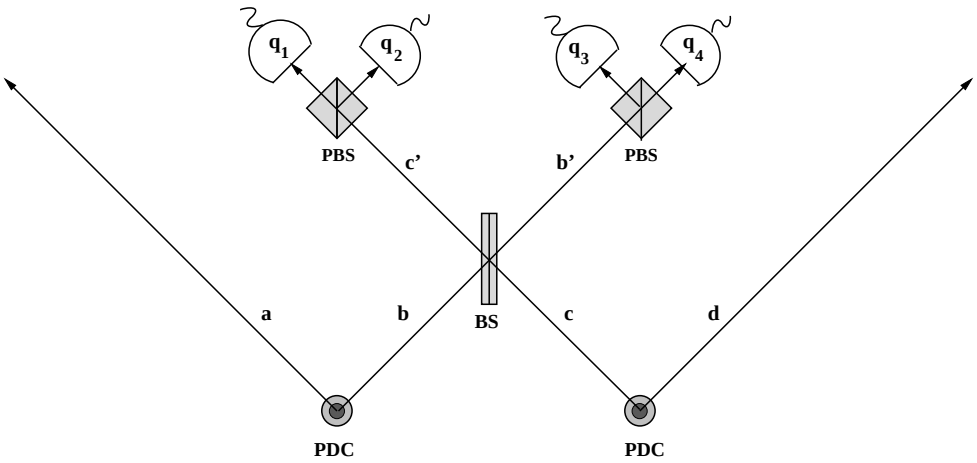

Fig. 1. Entanglement swapping based on two PDC sources and an interferometric BSM. Four spatial modes are involved: a, b, c and d. The modes b and c are combined at a balanced beamsplitter (BS). Outputs b' and c' are directed to polarizing beamsplitters (PBS) and then detected at four photon detectors: one for the H and one for the V polarization of each of the c' and b' modes. The detectors are inefficient and subject to dark counts. Their readout is denoted by $\{q_1, q_2, q_3, q_4\}$. In a QKD experiment (see Fig. 2), the polarization-entangled photons of the remaining modes a and d are distributed between Alice and Bob, respectively, and the BBM92 protocol [16] can be applied to make the secret key.

achieved by PDC-ES-BBM92 QKD compared to decoy-BB84 QKD. In particular, we analyze the conjecture that there is no superiority of PDC-ES-BBM92 QKD over decoy-BB84 QKD with respect to achievable range for detectors with negligible dark counts.

This paper is organized as follows. In Sec. 2 we identify the resources and describe how we incorporate real-world imperfections into our mathematical model. In Sec. 3 we demonstrate how to optimize the performance of PDC-ES-BBM92 QKD with respect to PDC sources and detectors. Sec. 4 provides a comparison between PDC-ES-BBM92 QKD and decoy-BB84 QKD for negligibly small detector dark count rates. We conclude in Sec. 5 with a brief summary and important remarks.

2. Identifying the resources

The photon transmission probability is $10^{-\alpha l/10}$ for α the loss coefficient (in dB/km) and l the distance the light travels. The loss differs depending on whether transmission is via fiber optics or free space. In this analysis we leave the loss coefficient unspecified and normalize the distance between sender and receiver through the product αd. For example, the loss coefficient for light of wavelength 1550 nm propagating through a telecom optical fiber is approximately $\alpha \approx 0.25$ dB km^{-1} [6], so $\alpha d = 10$ (a " 10 dB loss") corresponds to $d \approx 40$ km of fiber.

Basic experimental ES is illustrated in Fig. 1. Two PDC sources emit photon pairs into spatial modes a and b (first PDC) and c and d (second PDC). For ES, a joint BSM is performed on the b and c modes. As a consequence, provided that a certain measurement readout occurs, the photons in outgoing modes a and d emerge entangled despite never having interacted with one another [8]. The entanglement previously contained in the a and b and the c and d photon pairs, respectively, is swapped to the a and d photon pair.

We assume type-I nondegenerate PDC as the generator of *polarization-entangled* quantum

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

states

$$|\chi\rangle_{ab} = \exp[i\chi(\hat{a}_{\mathrm{H}}^{\dagger}\hat{b}_{\mathrm{H}}^{\dagger} + \hat{a}_{\mathrm{H}}\hat{b}_{\mathrm{H}})] \otimes \exp[i\chi(\hat{a}_{\mathrm{V}}^{\dagger}\hat{b}_{\mathrm{V}}^{\dagger} + \hat{a}_{\mathrm{V}}\hat{b}_{\mathrm{V}})]\,|\mathrm{vac}\rangle \tag{1}$$

in two spatial modes a and b, where $|\mathrm{vac}\rangle$ is the multimode vacuum state. Our analysis is straightforward to generalize to other types of entanglement. The parameter $\chi \in \mathbb{R}$ is proportional to the $\chi^{(2)}$ nonlinearity of the crystal, the strength of the pump laser and the interaction time between the pump laser and the medium, which is approximately the laser-pulse duration. The value of χ^2 (the square of χ, not to be confused with the crystal's $\chi^{(2)}$ nonlinearity) is the probability for EPP generation within the time window of a laser pulse. Equivalently, χ^2 can be interpreted as the EPP production rate (brightness) of the PDC source. We assume the same brightness for both PDCs. The quantum state generated by the second PDC source is thus $|\chi\rangle_{cd}$, and the common quantum state prepared by two identical PDC sources is then given by $|\chi\rangle_{abcd} = |\chi\rangle_{ab} \otimes |\chi\rangle_{cd}$. Exceedingly small χ values imply disadvantageously low EPP production rates; however, as χ increases, the probability for harmful multipair events rises, which lead to faulty detection clicks and thus incorrect estimates of entanglement after ES.

We model detector efficiency η ($0 \leq \eta \leq 1$) by preceding a fictitious unit-efficiency, dark-count-exempt photon-counting detector with a virtual beamsplitter of transmittance η. We include dark counts by a fictitious thermal background source of light incident on the second input port of the beamsplitter. Dark counts are incorporated by the dark count probability $\wp_{\mathrm{dc}}$ per time window of the pump laser pulse in the PDC process. In our model transmission losses are included in detector efficiencies according to $\eta = \eta_0 10^{-\alpha l/10}$, where η_0 denotes the intrinsic detector efficiency.

Detector quality is important for long-distance QKD. On the one hand, detectors should be as efficient as possible to achieve fast key rates and high efficiency for ES operation. On the other hand, dark count noise should be low to make the QBER small. In experiments these two aims compete: η_0 and $\wp_{\mathrm{dc}}$ counteract for typical off-the-shelf detectors. Avalanche photodiodes (APDs) are the most used photon detectors in long-distance quantum communication experiments over telecom optical fibres, with InGaAs/InP diodes being the most common. The trade-off between efficiency and dark counts for high quality InGaAs APD detectors at optical telecom wavelength 1550 nm can be characterized by the empirical relation

$$\wp_{\mathrm{dc}} = A\exp(B\eta_0) \tag{2}$$

with typical values $A = 6.1 \times 10^{-7}$ and $B = 17$ [6]. For simplicity, we assume the same efficiency η_0 and dark count probability $\wp_{\mathrm{dc}}$, respectively, for all detectors employed in the here considered QKD scheme, subject to the empirical constraint (2).

In fact single-photon detectors other than APDs have been prototyped. Most notable are superconducting transition-edge sensors (TES), which are photon-number-resolving with up to 88% detection efficiency at 1550 nm and benefit from negligible dark count rates [30, 31, 32]. A further type with a demonstrated photon-number-resolving functionality is given by superconducting nanowire single-photon detectors (SNSPDs) [33, 34, 35, 36], which combine a high infrared detection efficiency (up to 57% at 1550 nm [34]) with an ultra-low dark count rate and a high counting frequency [36]. Such detectors (TES or SNSPDs) substantially increase the range, security and bit rate for QKD. However, a severe drawback of both TES and SNSPDs is the fact that they must be operated at cryogenic temperatures, which makes them impractical for off-the-shelf QKD technology.

Transmission of polarization-encoded qubits naturally suffers from depolarization, i.e., environment-induced randomization of photon polarization. The amount of this depolarization depends on the properties of the quantum channel, i.e., on the specific fiber used for photon transmission or atmospheric conditions in the case of free-space QKD, as well as on the spectral band-width of the individual photons. Nevertheless, modern fibers affect the polarization

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

far less than previously thought. High-fidelity transmission of polarization-encoded qubits from EPP sources is possible and was successfully demonstrated over 100 km of fiber [37] and in free space even up to 144 km [38]. Such high-fidelity transmission can be extended to even greater distances by spectral filtering of the down-converted photons [39, 40]. Moreover, various implementations have demonstrated how to remedy birefringence-caused, time-varying unitary polarization transformations during photon transmission. Promising proposals include, e.g., real-time polarization control employing two nonorthogonal reference signals multiplexed in either time or wavelength with the data signal [41] as well as stabilization of unwanted qubit transformation in the quantum channel using quantum frames [42]. Hence, for distances up to 100 km, and probably beyond this range, the degree of observed quantum correlations is limited mainly by detector dark counts and multi-pair emissions rather than by depolarization, which we neglect in the present analysis.

Previously we derived a nonperturbative, closed-form solution for the quantum states $\hat{\rho}^{\{q_\nu\}}(\chi,\{\eta_\nu\},\{\wp_{\mathrm{dc}\,\nu}\})$ prepared by a realistic ES, given a recorded readout $\{q_\nu\}$ (e.g. $\{q_1,q_2,q_3,q_4\}$ in Fig. 1) of a BSM with faulty detectors characterized by efficiencies $\{\eta_\nu\}$ and dark count probabilities $\{\wp_{\mathrm{dc}\,\nu}\}$ (ν is a label for different detectors involved in the BSM), as a density-operator valued function of χ, $\{\eta_\nu\}$ and $\{\wp_{\mathrm{dc}\,\nu}\}$ [9]. Using this closed-form solution, we can simulate a four-fold coincidence experiment. A direct measure for entanglement quantification after ES is the visibility $V := (\mathrm{MAX}-\mathrm{MIN})/(\mathrm{MAX}+\mathrm{MIN})$, where "MAX" and "MIN" denote the maximum and minimum values of the four-fold coincidence rate as a function of polarization angle. Provided that click events are observed in both the a and d modes, and restricting ourselves to the corresponding post-selected quantum states $\hat{\rho}^{\{q_\nu\}}_{\mathrm{postsel}}$, the visibility is directly connected to the fidelity $F = \langle\psi^T|\,\hat{\rho}^{\{q_\nu\}}_{\mathrm{postsel}}\,|\psi^T\rangle$ with respect to a target Bell state $|\psi^T\rangle$ via the relation $V = (4F-1)/3$ [43]. The relation between visibility and correlation coefficient S_{CHSH} of the CHSH Bell inequality is $S_{\mathrm{CHSH}} = 2\sqrt{2}V$, cf. [44]. Our predictions [9] agree with experimental results [43]: our theory predicts $V_{\mathrm{theory}} = 77.7\%$, and the observed visibility in experiment was $V_{\mathrm{exp}} = (80\pm4)\%$.

3. Optimizing QKD performance

We numerically simulate the effect of real-world imperfections on the two common QKD figures of merit, quantum bit error rate (QBER) and secret key rate R_{sec}, for an entanglement-based QKD experiment in which the long-distance quantum channel (with distance d) between sender Alice and a receiver Bob is split into shorter segments with two PDC sources placed $1/4$ and $3/4$ of the way along the channel and a BSM performed halfway (Fig. 2). Due to ES, the photons distributed between Alice and Bob are entangled, so the BBM92 protocol can be applied to produce the key.

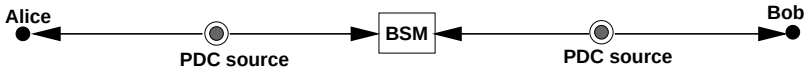

Fig. 2. Illustration of ES-based QKD. The quantum channel between Alice and Bob is split into shorter segments, with two PDC sources placed $1/4$ and $3/4$ of the way along the channel and a joint BSM performed halfway. Given a successful BSM (with success probability equal to $\frac{1}{2}\eta_0^2$), the photons arriving at Alice and Bob are entangled despite never having interacted with one another, and the BBM92 protocol can be used to create the secret key.

The QBER, defined as the ratio of wrong bits to the total number of bits exchanged between Alice and Bob, is directly related to the visibility V of four-fold coincidence measurements via the relation $\mathrm{QBER} = (1-V)/2$ [2]. Hence, it can be computed nonperturbatively using our

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

closed-form solution [9]. For compactness, the procedure for computation of V is not repeated in the present paper.

For one-way communication, which we analyze here, according to Shor and Preskill's security proof the secret key yield is [45]

$$R_{\rm sec} = R_{\rm sift}\left[1 - \kappa H_2(\mathrm{QBER}) - H_2(\mathrm{QBER})\right]. \tag{3}$$

The first factor, $R_{\rm sift}$, is the *sifted key* rate; it is the number of all coincidental detection events (per second) for which Alice and Bob made by chance compatible choices of bases in which they measured the received photons. Hence, the sifted key rate is only half that of the *raw key* rate, which consists of the overall number of qubits exchanged between Alice and Bob. The raw key rate is obtained as a product of the following probabilities per attempt of ES: (i) the probability that both PDCs emit EPPs, which is the product of their photon-pair production rates χ^2, respectively, (ii) the probability that the generated photons arrive at the analyzers of both Alice and Bob as well as at the BSM device, (iii) the probabilities that the photons that arrive at Alice's and Bob's sites are also detected, and (iv) the probability that the BSM is successful, which is equal to $\frac{1}{2}\eta_0^2$ and thus bounded by its maximum value $1/2$ [46]. Hence, for the QKD scheme considered here, under our assumptions,

$$R_{\rm sift} = \frac{1}{2}\chi^2\chi^2(10^{-\alpha d/40})^4\eta_0^2(\frac{1}{2}\eta_0^2) = \frac{1}{4}\chi^4\eta_0^4 \times 10^{-\alpha d/10}. \tag{4}$$

The second factor of Eq. (3) describes the effect of privacy amplification. The two subtracted terms $\kappa H_2(\mathrm{QBER})$ and $H_2(\mathrm{QBER})$, where

$$H_2(x) \equiv -x\log_2(x) - (1-x)\log_2(1-x) \quad \text{for} \quad x \in [0,1] \tag{5}$$

is the binary Shannon entropy function, represent the reduction of the key rate due to error correction and eavesdropping on the quantum transmission, respectively, with $\kappa = 1.22$ characterizing the efficiency of error correction algorithm compared to the Shannon limit [47].

We remark that the Shor-Preskill lower bound for the ratio between the number of secure key bits and the number of sifted key bits, as given by Eq. (3), was derived under the assumption of perfect sources and detectors; i.e., it was assumed that any source or detector imperfections can be absorbed into eavesdropper Eve's attack. The same bound was achieved by Koashi and Preskill in their QKD security proof for an arbitrary (possibly faulty) source with the only restriction that the source must not reveal any information to Eve about the basis chosen by Alice and Bob for their measurements [48]. This feature is naturally satisfied for our entanglement-based PDC-ES-BBM92 QKD. The Koashi-Preskill security proof indicates that source defects are efficiently detected by the QKD protocol — in our case the BBM92 protocol rather than BB84. This means that Alice and Bob cannot be fooled into accepting a part of the secret key that Eve got to know by exploiting source imperfections.

Both Shor-Preskill [45] and Koashi-Preskill [48] security proofs rely on the crucial assumption that Alice's and Bob's measurements are performed on qubits. This assumption is certainly not valid for real-world QKD. In our PDC-ES-BBM92 QKD scheme, polarization measurements are implemented by means of polarization rotators (quarter- and half-wave plates), PBSs and threshold detectors acting on multiphoton states in spatio-temporal optical modes. The corresponding detection events are theoretically described by POVMs over the *infinite*-dimensional Fock space. Yet, by using squashing techniques [49, 50], which are directly applicable to our setup, all detection events of our QKD scheme can indeed be reduced to a statistically equivalent two-dimensional qubit-based description. The existence of a squashing model permits employing the Shor-Preskill lower bound (3) for our QKD scheme. It also ensures validity of

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

our entanglement verification via four-fold coincidence measurements with (realistic) threshold detectors (see [50]).

Our results are illustrated in Figs. 3–7. Fig. 3 displays the dependence of the QBER on the parameter χ for various fixed values of the product αd, whereas Fig. 4 shows the QBER's dependence on αd for various fixed χ values. In both figures, η_0 and $\wp_{\rm dc}$ are fixed and interrelated by constraint (2). As expected, for a fixed distance, the QBER is large for exceedingly small as well as for notably large χ values. This dependence can be understood as follows. In the case of excessively low photon-pair PDC production rates (exceedingly small χ values), most detection events arise due to detector dark counts, which contribute noise, thus implying an increase of the QBER. As the photon-pair production rate increases, the constant detector noise level becomes less relevant so that most detector clicks are due to correctly detecting single photons stemming from PDC sources, thereby entailing a low QBER value. On the other hand, excessively high photon-pair production rates (large χ values) are counterproductive as they involve a higher probability of multipair events in the PDC process, thereby making the QBER grow. As we observe in Fig. 3, our theory predicts the value of χ that minimizes the QBER for given channel length and loss coefficient. Conversely, given fixed χ, we know how the QBER scales with distance d. We also find that, as far as QBER is concerned, lower detector efficiency is preferable, given the constraint (2). Note that, to achieve non-vanishing secret key rates the QBER must not exceed the value 0.094 if $\kappa = 1.22$. (0.11 if $\kappa = 1.0$).

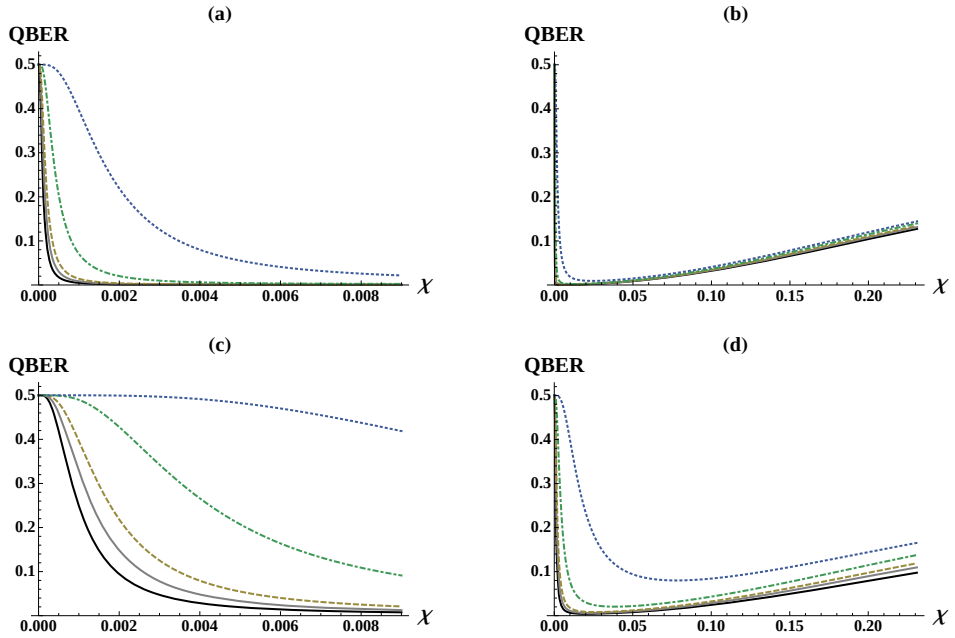

Fig. 3. QBER as a function of χ for various values of the normalized distance αd and fixed η_0 and $\wp_{\rm dc}$. The function is plotted for $\alpha d = 0, 5, 10, 25$ and 50, corresponding, respectively, to the curves of lowest- to highest-QBER values in all diagrams, and $\eta_0 = 0.1$ & $\wp_{\rm dc} \approx 3 \times 10^{-6}$ in figures (a) and (b), or $\eta_0 = 0.3$ & $\wp_{\rm dc} \approx 10^{-4}$ in figures (c) and (d). The values of η_0 and $\wp_{\rm dc}$ are related to one another by constraint (2). Figures (a) and (c) display a higher resolution for very small χ values in both cases. To have $R_{\rm sec} > 0$ the QBER must assume values less than approx. 0.094 if $\kappa = 1.22$ (0.11 if $\kappa = 1.0$).

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

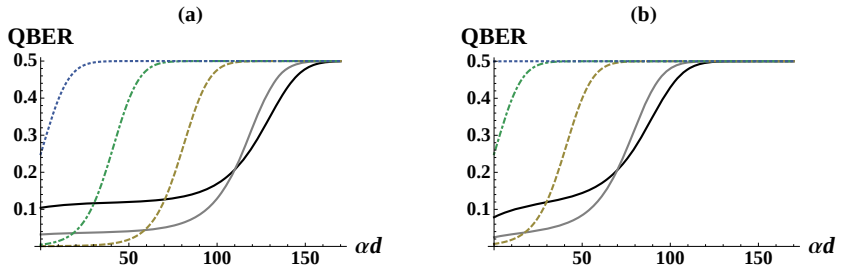

Fig. 4. QBER vs αd for various χ values and fixed η_0 and $\wp_{dc}$. The function is plotted for $\chi = 10^{-4}$, 10^{-3}, 10^{-2}, 0.1, and 0.2, corresponding to the dotted, dot-dashed, dashed, gray solid and dark solid curves, respectively, in both diagrams, and (a) $\eta_0 = 0.1$ & $\wp_{dc} \approx 3\times 10^{-6}$ or (b) $\eta_0 = 0.3$ & $\wp_{dc} \approx 10^{-4}$. The values of η_0 and $\wp_{dc}$ are related to one another by constraint (2).

However, optimal brightness for QKD is not given by the value of χ that minimizes the QBER because two effects contribute to R_{sec}'s dependence on χ. The first contribution is via the sifted key rate, which increases proportionally with χ^4. The second contribution is via the QBER in a nontrivial way (see the second factor in Eq. (3)). For the highest possible R_{sec}, an optimal trade-off between the production rate of final EPPs and the amount of entanglement after the ES operation has to be achieved.

For QKD the relevant quantity to be optimized is the secret key rate R_{sec}, whose dependence on χ and η_0 is displayed in Figs. 5 and 6 for various values of αd. Our model reveals the optimal χ and η_0 that maximize the secret key rate for given channel length. We have performed a constrained optimization, both with respect to χ and η_0, assuming constraint (2) between the detector efficiencies and dark counts for APD detectors. The result is presented in Fig. 7.

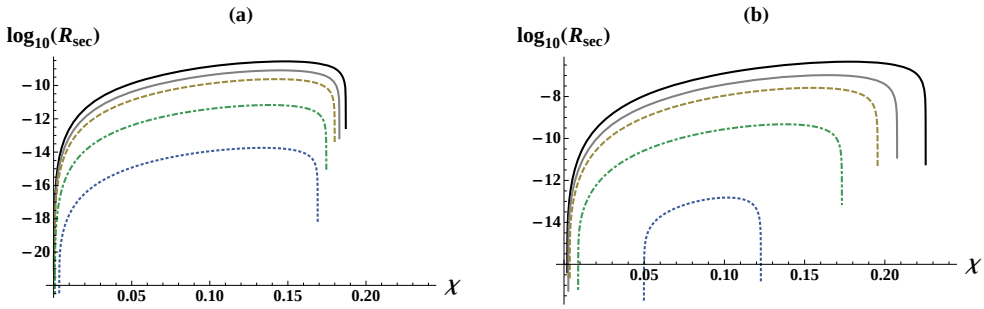

Fig. 5. $\log R_{sec}$ as a function of χ for various values of the product αd, and fixed η_0 and $\wp_{dc}$. Plots are displayed for $\alpha d = 0, 5, 10, 25$, and 50, corresponding, respectively, to the dark solid, gray solid, dashed, dot-dashed and dotted curves in both diagrams, and (a) $\eta_0 = 0.1$ & $\wp_{dc} \approx 3\times 10^{-6}$ or (b) $\eta_0 = 0.3$ & $\wp_{dc} \approx 10^{-4}$. Dark count probabilities are related to the values of η_0 by constraint (2). The value of R_{sec} is the number of secure bits created per single pump-laser pulse.

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

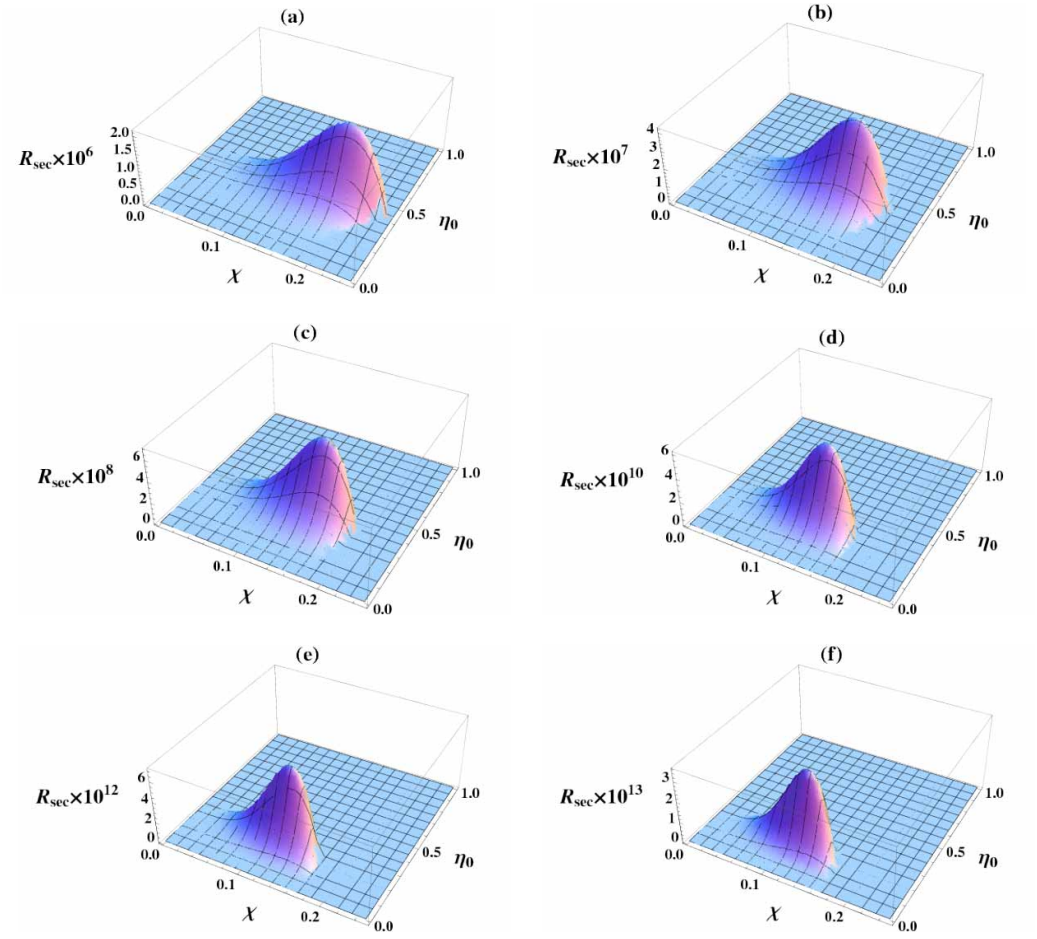

Fig. 6. Secret key rate R_{sec} as a function of χ and η_0 for various exemplary values of the product αd. From left to right: (a) $\alpha d = 1$, (b) $\alpha d = 5$, (c) $\alpha d = 10$, (d) $\alpha d = 25$, (e) $\alpha d = 40$ and (f) $\alpha d = 50$. Dark count probabilities are related to the values of η_0 by constraint (2), respectively. Here R_{sec} is given in terms of the number of secure bits created per single pump-laser pulse (precisely: for each attempt of ES, which requires two laser pulses, specifically with one per crystal).

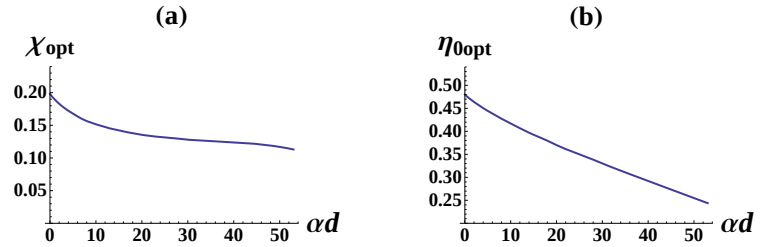

Fig. 7. (a) Optimal χ and (b) optimal η_0 values for QKD as a function of the product αd. The dark count parameter $\wp_{\mathrm{dc}}$ is related to $\eta_{0\mathrm{opt}}$ by constraint (2).

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

4. Comparison: PDC-ES-BBM92 QKD vs Decoy-BB84 QKD

Decoy-BB84 QKD, invented to combat QKD vulnerability due to PNS attacks, was shown to enable achieving much greater distances than conventional faint-pulse BB84 QKD without decoy states [19, 22]. Furthermore, decoy-BB84 QKD realizes substantially higher key distribution rates than PDC-based BBM92 QKD for medium- and low-loss settings (i.e. short distances), while the latter tolerates higher channel losses, hence permitting longer communication distance than the former [13]. Additional range extensions are possible by means of ES at cost of low communication rates; this fact has been demonstrated for ES based on *ideal* EPP sources in [3, 6]. Here we compare PDC-ES-BBM92 QKD and decoy-BB84 QKD with respect to achievable distance. In particular, we analyze the issue whether the advantage of ES-based BBM92 QKD with regard to range limits is due to a better scaling with respect to dark counts rather than due to a higher tolerance of losses and thus would vanish for promising future detectors with negligible dark count rates. In the discussion below, the detector efficiency and dark counts are assumed not to be constrained.

For decoy-BB84 QKD, the key generation rate is given by the formula [20]

$$R_{\mathrm{sec}}^{\mathrm{decoy}} \geq \frac{1}{2}\left\{-Q_\mu f(E_\mu) H_2\left(E_\mu\right) + Q_1\left[1 - H_2\left(e_1\right)\right]\right\}, \tag{6}$$

where μ denotes the intensity (photon number expectation value) of signal states sent by Alice to Bob, Q_μ is the gain of signal states, E_μ is the overall QBER of signal states, Q_1 is the gain of single-photon states in signal states, e_1 is the error rate of single-photon states in signal states, and $f(x)$ is the error correction efficiency function. While Q_μ and E_μ can be measured directly from the experiment, Q_1 and e_1 have to be estimated.

Here we employ the practical vacuum & weak-decoy state method, i.e., a two-decoy-state protocol with expected photon numbers $\nu_1 = 0$ and $\nu_2 = \nu \ll 1$, which has been shown to asymptotically approach the theoretical limit of the most general type of decoy state protocol (with an infinite number of decoy states) [20]. See also [21] for an efficient and feasible three-decoy-state protocol (using vacuum and two decoy states). The weak decoy state method allows to lower-bound Q_1 and upper-bound e_1. Here we use the corresponding bounds derived in [20] as well as definitions of E_μ and Q_μ provided therein. We choose the same error correction efficiency as for PDC-ES-BBM92 QKD in Eq. (3), $f(E_\mu) = \kappa = 1.22$ [47]. Furthermore, for a fair comparison, we assume that only dark counts and other background events contribute to E_μ, while we neglect erroneous detection events due to alignment and stability imperfections of the optical system, which have not been accounted for in our model for PDC-ES-BBM92 QKD either. The optimal choice of ν, which depends on the transmission distance, has also been analyzed in [20]; the optimal ν is fairly small (~ 0.1) for all distances. Here we choose the fixed value $\nu = 0.1$, which is reasonable as shown in [20].

We have computed the secret-key rate as a function of αd for both PDC-ES-BBM92 QKD (using Eq. (3)) and decoy-BB84 QKD (using Eq. (6) with lower and upper bounds for Q_1 and e_1 from Ref. [20]) for detectors with the fixed efficiency $\eta_0 = 0.2$ and diminishing dark count noise, see Fig. 8. Optimal source brightness (i.e., optimal values of χ and μ, respectively) has been chosen for each value of αd, respectively, so as to achieve highest QKD performance at each distance. As demonstrated in Fig. 8, decoy-BB84 QKD permits significantly higher key distribution rates for short distances up to the crossover point at which $R_{\mathrm{sec}}^{\mathrm{decoy}}$ rapidly drops to zero causing a steep slope of $\log R_{\mathrm{sec}}^{\mathrm{decoy}}$, while PDC-ES-BBM92 QKD enables much longer range. As $\wp_{\mathrm{dc}}$ decreases, the range of both decoy-BB84 QKD and PDC-ES-BBM92 QKD increases and the crossover point moves to larger distances. As a consequence, the advantage of PDC-ES-BBM92 over decoy-BB84 QKD with respect to range diminishes because the communication rate of the former beyond the crossover point becomes gradually prohibitively low.

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

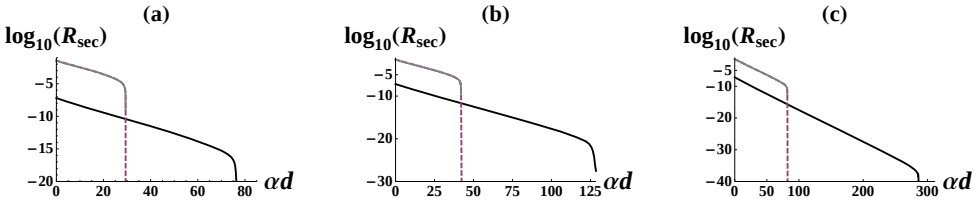

Fig. 8. Comparison between decoy-BB84 and PDC-ES-BBM92 QKD performance for decreasing dark count noise. All three diagrams display the logarithm of $R_{\rm sec}$ vs αd for decoy-BB84 QKD (gray curve) and for PDC-ES-BBM92 QKD (dark curve), with optimal choice of source brightness for every value of αd, respectively, and the fixed detector efficiency $\eta_0 = 0.2$. The detector dark count probabilities are (a) $\wp_{\rm dc} = 1.8 \times 10^{-5}$ (complying with constraint (2)), (b) $\wp_{\rm dc} = 10^{-6}$ and (c) $\wp_{\rm dc} = 10^{-10}$ (ignoring constraint (2) in (b) and (c)).

There is no crossover of the curves (corresponding to $\log R_{\rm sec}^{\rm decoy}$ and $\log R_{\rm sec}^{\rm ES}$ vs αd) for $\wp_{\rm dc} = 0$. Whereas, in this limit, $\log R_{\rm sec}^{\rm decoy}$ keeps decreasing linearly for all αd, $\log R_{\rm sec}^{\rm ES}$ eventually drops exponentially. Intuitively this is obvious. Under our assumptions, in decoy-BB84 QKD the overall QBER, E_μ, and the error rate of single-photon states, e_1, are caused only by dark count noise; for $\wp_{\rm dc} = 0$ both $E_\mu = 0$ and $e_1 = 0$, implying, according to Eq. (6), $R_{\rm sec}^{\rm decoy} \geq Q_1/2$, which decreases exponentially without range limit. In PDC-ES-BBM92 QKD, in addition to dark counts, multipair events of PDC sources contribute to the overall quantum bit error rate, so $\wp_{\rm dc} = 0$ does not imply a vanishing QBER. It is of no practical interest to determine the point at which the range of decoy-BB84 QKD outdistances the range achieved in PDC-ES-BBM92 QKD, because the corresponding key rates become extremely small, thus useless.

As illustrated in Fig. 9(a), the achievable range in PDC-ES-BBM92 QKD is quite sensitive to the choice of PDC source brightness, whereas in decoy-BB84 QKD the key rate and distance are fairly stable against a variation of μ. Hence, particularly for PDC-ES-BBM92 QKD, it is necessary to optimize the source brightness for each given distance. Furthermore, for negligible dark counts, increasing the detector efficiency yields a higher key rate as well as a longer distribution range. The impact of detector efficiency increase on QKD performance is more significant for PDC-ES-BBM92 QKD than for decoy-BB84 QKD, as shown in Fig. 9(b). This is easily understandable. In decoy-BB84 QKD photon detections take place only at Bob's site, whereas, in ES-based BBM92 QKD, additional detectors are employed at Alice's site as well as to perform a BSM.

5. Conclusions

ES is a fundamental building block in entanglement-based quantum communication schemes over long distances. We propose a nonperturbative theory for *practical* QKD based on ES. After identifying and characterizing the resources for QKD, we perform constrained optimization of QKD performance with respect to PDC sources and detectors for any distance d between sender and receiver and for arbitrary loss coefficients. For QKD schemes via a single ES operation, the PDC brightness and the detector efficiencies should be tuned so that $0.12 < \chi < 0.19$ and $0.25 < \eta_0 < 0.48$ depending on αd and the empirical constraint (2) between the detector efficiency and dark counts. Our theory assumes only existing technology. Even though we have elaborated on PDC sources and APD detectors, our model can straightforwardly be applied to other types of realistic EPP sources and detectors. With respect to eavesdropping, we assume that the eavesdropper (Eve) exploits all experimental imperfections. Our predictions provide useful upper bounds on the ES-based long-distance QKD performance. Although the advantage

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

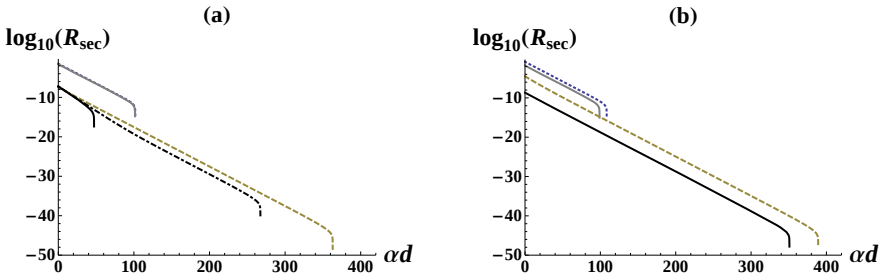

Fig. 9. (a) Effect of source brightness variation on key generation rate and distribution range for fixed $\eta_0 = 0.2$ and negligible dark counts, $\wp_{\rm dc} = 10^{-12}$. In decoy-BB84 QKD, the key rate and range are fairly stable against a change of μ (as already pointed out in [20]): the curves corresponding to $\mu = 0.8$ (dotted) and $\mu = 0.4$ (gray solid) coincide. In PDC-ES-BBM92 QKD, the key rate and achievable range depend drastically on source brightness, as demonstrated by the curves corresponding to $\chi = 0.174$ (dark solid), $\chi = 0.172$ (dot-dashed) and $\chi = 0.12$ (dashed), respectively. (b) Effect of detector efficiency variation on key generation rate and distribution range for fixed $\wp_{\rm dc} = 10^{-12}$ and fixed source brightness, $\mu = 0.7$ and $\chi = 0.120$, respectively. Predictions for two different η_0 values are shown. For $\eta_0 = 0.9$ yielding the dotted curve for decoy-BB84 and the dashed curve for PDC-ES-BBM92 QKD, higher key rates and longer distances are achieved than for $\eta_0 = 0.1$ yielding the gray solid curve for decoy-BB84 and dark solid curve for PDC-ES-BBM92 QKD. The effect is substantially greater for PDC-ES-BBM92 than for decoy-BB84 QKD.

of ES-based QKD over faint-pulse decoy-BB84 QKD, with respect to achievable distances, diminishes for detectors with negligibly small dark count rates, ES-based QKD is also important as an enabler for quantum repeater-based QKD.

Our analysis could be further improved by accounting for temporal-mode overlap imperfections on a beam-splitter as well as spectral-mode mismatch. Moreover, we conjecture that the optimal PDC brightness could be shifted to higher values by employing (realistic) photon-counting detectors instead of threshold detectors. Our closed-form solution for the actual entangled quantum states prepared by practical ES [9] allows for inefficient, noisy photon-number discriminating detectors for the BSM. The intuition affirms this conjecture and is easily understood as follows.

Let us consider the events where a coincidence detection by two threshold detectors for modes *b* and *c* (in Fig. 1) is interpreted as a projection onto a Bell state. For threshold detectors, a fraction of these cases originates from two (or more) photons impinging on one detector and (at least) one photon impinging on the other detector, whenever at least one PDC source has a multipair excitation. These harmful erroneous heralding events, which are not identifiable by threshold detectors, may result in a failure of the ES operation and thus increase of the QBER. On the other hand, unit-efficiency photon-number discriminating detectors would allow to identify and discard these undesired events, which yields a lower QBER for equal-source brightness or, conversely, allows increasing brightness while keeping the QBER constant. Even imperfect photon-number discriminating detectors could reveal and thus enable to eliminate the erroneous heralding events to some extent. Hence, optimum brightness for maximal QKD performance could be chosen higher than in the case of threshold detectors, and one would achieve higher secret-key production rates due to increasing values of the raw-key rate. This conjecture is worth examining in view of promising technological advancements with photon-number-resolving detectors [31, 32, 36].

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011

Acknowledgements

This project has been supported by NSERC, *i*CORE (now part of Alberta Innovates - Technology Futures), MITACS and General Dynamics Canada. BCS is a CIFAR Fellow. The authors thank Norbert Lütkenhaus, Eleni Diamanti, Romain Alléaume, Ben Fortescue and Patrick Ming-yin Leung for helpful discussions.

#140334 - $15.00 USD Received 4 Jan 2011; revised 26 Jan 2011; accepted 26 Jan 2011; published 1 Feb 2011