PHYSICAL REVIEW A **75**, 050305(R) (2007)

Quantum key distribution with passive decoy state selection

Wolfgang Mauerer* and Christine Silberhorn
*Institute of Optics, Information and Photonics, Max Planck Research Group, University of Erlangen-Nürnberg,
Günther-Scharowsky-Straße 1/Bau 24, 91058 Erlangen, Gernany*

(Received 22 July 2006; published 31 May 2007)

We propose a quantum key distribution scheme which closely matches the performance of a perfect single photon source. It nearly attains the physical upper bound in terms of key generation rate and maximally achievable distance. Our scheme relies on a practical setup based on a parametric downconversion source and present day, nonideal photon-number detection. Arbitrary experimental imperfections which lead to bit errors are included. We select decoy states by classical postprocessing. This allows one to improve the effective signal statistics and achievable distance.

DOI: 10.1103/PhysRevA.75.050305 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.Dv

Quantum key distribution (QKD) allows two parties (Alice and Bob) to communicate securely even in the presence of an arbitrarily powerful eavesdropper (Eve) who tries to listen undetected. To prove unconditional security, Eve must not be restricted by any technological limitations, but must only be bounded by the laws of quantum physics. A multitude of protocols has been suggested in the last decades, where the Bennett-Brassard 1984 (BB84) protocol [1] is the best-known and most-studied protocol. It was shown to be secure both in principle ([2] and references therein) and in the presence of experimental imperfections, e.g., [3]. Unfortunately, the maximum distance and the bit rates over which secure communications can be guaranteed are strongly constricted if experimental imperfections are taken into account: lossy channels, imperfect detectors with finite efficiency, dark counts and misalignment errors, as well as nonideal signal sources—which do not provide the required single photon states [4,5]—degrade the performance of the protocol. Decoy-state QKD, which was recently introduced by [6], analyzed in [7,8], and adapted for practical use in [9,10], could mend this. Still, implementations using coherent-state laser pulses achieve only about 70% of the maximum secure distance imposed by fundamental physics.

In this paper, we show how we can close the gap between practical QKD implemented with state-of-the-art devices and idealized QKD assuming perfect single-photon signals. Our protocol reaches up to a few percent the performance of a single-photon source in terms of distance, while the key generation rate is on par with the best available schemes. In our approach, we utilize a parametric downconversion (PDC) source [11] in conjunction with a photon number resolving detector [12] to substitute an idealized single-photon source. The strict photon-number correlations between the two PDC outputs allow us to infer the complete statistical information about one of them by measuring the photon number distribution of the other. Thus passive decoy-state selection can be accomplished without the need for any active optical elements; our system becomes independent of intensity calibration errors. Furthermore, the passive data analysis enables us to generate optimized effective signal statistics without physical blocking. Otherwise, our scheme—as depicted in Fig. 1—is based on the standard BB84 protocol, where Alice actively encodes her qubits for two different basis sets on the signal states. Note that, contrary to other QKD schemes employing PDC sources, our protocol does not rely on polarization entanglement with passive information coding.

Since our work is based on the decoy state method, we review briefly the underlying basic idea. The security of BB84 with binary detectors rests on single photons. For protocols with active information coding, signals with more than one photon are insecure because Eve can avail herself of a photon-number splitting (PNS) attack, which has been shown to be optimal [13]. For this, Eve performs a quantum nondemolition measurement of the photon number, taps one photon, and delays the measurement until Alice and Bob announce the bases. If Eve replaces the lossy channel with a perfect one and passes on signals mimicking the statistics of a lossy channel for a binary detector, she cannot be detected in a standard BB84 scheme. For a quantum channel with transmission $\eta=10^{\alpha/10l}$ (where α describes the loss parameter and l the fiber length), the probability that at least one photon of an n-photon signal arrives at Bob's side is given by $\eta_n=1-(1-\eta)^n$. This implies that different loss characteristics arise from signals with different photon numbers. The core idea of the decoy method is to exclude a PNS attack by verifying that the signal losses behave as expected for different photon numbers. This can be accomplished if Alice intersperses the stream of signal pulses with decoy states whose intensity differs slightly from the signal states, but share all other characteristics like wavelength and timing. A more detailed description can be found in the work of Lo *et al.* [7].

The security analysis in [7] proves that a lower bound on the secure key generation rate is given by

$$S \geqslant \max(0,q\{-Q_{\bar{N}}f(E_{\bar{N}})H_2(E_{\bar{N}})+Q_1[1-H_2(e_1)]\}). \quad (1)$$

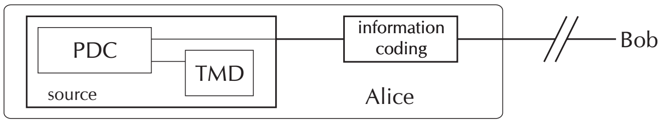

FIG. 1. Setup of the proposed QKD scheme. The PDC source emits photon number correlated bipartite states; the time-multiplexed detector (TMD) records photon statistics.

*Electronic address: wolfgang.mauerer@ioip.mpg.de

In Eq. (1) the overall *gain* $Q_{\bar{N}}$ depends on the mean photon number $\bar{N}$ of the signal pulses and denotes the ratio of Bob's detection events to Alice's number of submitted signals after sifting. The *yield* Y_n is defined as the conditional probability that Bob receives a signal if Alice has sent an n-photon signal. The parameter $E_{\bar{N}}$ describes the overall, and e_n the photon number resolved quantum bit error rate (QBER), i.e., the fraction of signals which contribute false key bits although a signal was received. The quantities are related as follows:

$$Q_{\bar{N}} \equiv \sum_{n=0}^{\infty} Q_n = \sum_{n=0}^{\infty} Y_n p(n), \tag{2}$$

$$E_{\bar{N}} Q_{\bar{N}} \equiv \sum_{n=0}^{\infty} Y_n p(n) e_n. \tag{3}$$

The function f in Eq. (1) accounts for nonideal practical error correction which does not reach the Shannon limit, and H_2 is the binary Shannon entropy. The sifting factor q corrects incompatible bases, i.e., for standard BB84 $q=1/2$. In the asymptotic limit of a large number of transmitted signals, it is possible to reach values of $q \approx 1$ [5], which is used in the remainder of the paper. Conventional QKD schemes employ binary detectors. Thus, only the gain $Q_{\bar{N}}$ and QBER $E_{\bar{N}}$ can be measured during transmission. Source characterization guarantees that the probability $p(n)$ of an n-photon signal is known. The decoy state idea exploits that the linear system of Eqs. (2) and (3) can be solved for Y_n and e_n, if states with different mean intensities $\bar{N}$ are employed. While Y_n and e_n are identical for the signal and all decoy states in case of a regular quantum channel, it is proven that any PNS attack will modify these quantities, i.e., Eve's attempt of a PNS attack will be detected [7].

The original security proof for BB84 given in [14] utilized local operations and one-way classical communication (1-LOCC). While many security analyses retain with 1-LOCC, enhanced security proofs employing 2-LOCC [2] have been elaborated recently and adapted to the decoy method in [15]. In two-way postprocessing, Alice and Bob compare parities for random bit pairs of their key. If the parities match, they keep the first bit, otherwise they discard both. One iteration of this procedure is called a B-step; repeating it for several rounds is possible and allows to increase the maximum secure distance. For comparison we consider both cases, 1-LOCC and 2-LOCC.

Consider the setup in Fig. 1. In the source, we use a standard PDC process to obtain the photon-number correlated state

$$|\psi\rangle = \frac{1}{\mathcal{N}} \sum_{n=0}^{\infty} \lambda_n |n,n\rangle, \tag{4}$$

where λ and the normalization factor $\mathcal{N}$ depend on the physical boundary conditions [16]. The distribution exhibits Poissonian ($\lambda_n = \frac{\lambda^n}{\sqrt{n!}}$, $\mathcal{N} = e^{-\lambda^2}$) or thermal ($\lambda_n = \tanh^{2n} \bar{N}$, $\mathcal{N} = \cosh^2 \bar{N}$) statistics in the extremal cases, so we will consider both possibilities. Since Eve has no phase reference, the phase can be assumed to be totally randomized, and an effective mixture of photon number eigenstates with density operator $\varrho = \sum_n |\lambda_n / \mathcal{N}|^2 \varrho_n$ is transmitted.

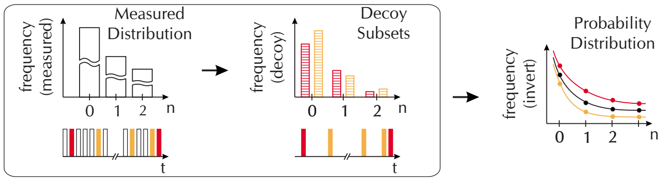

FIG. 2. (Color online) Passive decoy state selection. Apt subsets of the recorded TMD measurements are selected and inverted to form the decoy states which are similar to the signal state (see text).

In our protocol, Alice and Bob follow the standard BB84 protocol [4] for the encoding and analysis of the transmitted information. The qubits can be represented by polarization, time, or any other suitable coding. The analysis is not affected by any particular choice. Additionally, Alice performs a photon number resolved detection on one conjugate PDC mode to obtain additional information about the signal photon statistics. Note that Alice will run the PDC source always with constant pump intensity without any active optical manipulation. There are several methods to perform photon number resolved detection, but we focus on time multiplexed detection (TMD) [12] since it is cost effective and easy to handle experimentally. The measured TMD statistics can be related to the impinging photon number statistics by

$$\vec{p}_{\text{source}} = \mathbf{L}^{-1} \cdot \mathbf{C}^{-1} \cdot \vec{p}_{\text{meas}} \equiv \mathcal{R}(\vec{p}_{\text{meas}}), \tag{5}$$

where the matrix $\mathbf{L}$ accounts for photon loss in the detection, and the convolution matrix $\mathbf{C}$ models the effect of a finite number of detected modes in the TMD design (for details: see [12]). In Eq. (5), $\vec{p}_{\text{source}}$ and $\vec{p}_{\text{meas}}$ describe the original photon number distribution of the source and the measured statistics. The matrix $\mathbf{C} \cdot \mathbf{L}$ with its entries $p_\eta(m|n)$ can be determined by measurement, or calculated analytically as given in [17]. It represents the probability to obtain an m-photon detection outcome conditioned on n photons entering the detector with total loss η. Using Eq. (5), the TMD measurement can be inverted such that the real statistics of the source are reconstructed with high fidelity [18]. Note that this inversion is only possible for an ensemble of states but not for a single signal; hence Alice needs to record the measurement results of the TMD for every time slot.

The essential step of our passive decoy state selection follows after the data transmission with a sufficiently large number of signals is completed. Alice utilizes the measured photon statistics to separate signal from decoy states. Figure 2 provides an overview about the process: The measured probabilities $\vec{p}_{\text{meas}}$= are given by $p_{\text{meas}}(n) = \frac{\#n_{\text{tot}}}{N_{\text{tot}}}$, where $\#n_{\text{tot}}$ denotes the number of n-photon measurement outcomes from the TMD. This distribution can be inverted by Eq. (5); the strict photon number correlations of the PDC states ensure that Alice's measurements coincide with the signal statistics. The decoy state protocol employs signal states of different intensities, such that the linear system of Eqs. (2) and (3) can be solved.

Assume that we start with a random selection of a set containing $M \ll N_{\text{tot}}$ signals to construct decoy states, which

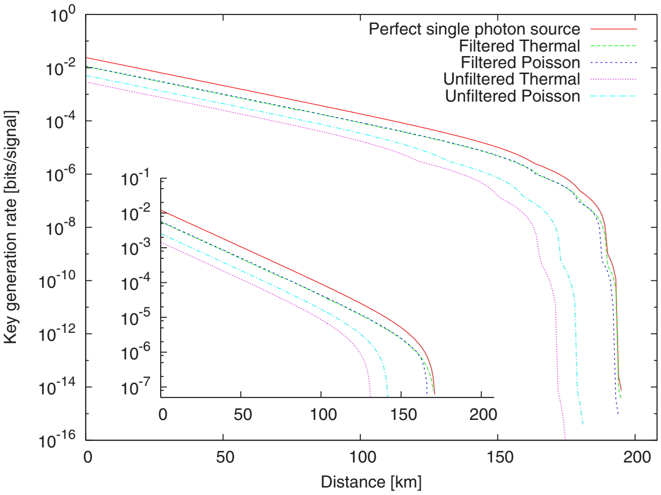

FIG. 3. (Color online) Simulation results for two-way and one-way (inset) classical communication. Both graphs were obtained by a numerical evaluation of Eq. (1); the optimal values for $\bar{N}$ and the number of B steps which maximize the key generation rate have been used for all distances. The right border represents the principal upper bound at 208 km given by the intercept-resend attack.

have exactly the same statistics as the remaining signal states. Alice then additionally picks δ_n slots with an n-photon measurement result such that

$$\#n_{\text{decoy}} = \# n_{\text{tot}} \frac{M}{N_{\text{tot}}} + \delta_n, \tag{6}$$

where δ_n is a small positive or negative offset which results in a photon number distribution of the decoy subset differing slightly from the distribution in the signal. The decoy subset can be inverted to obtain the proper probability distribution $\vec{p}_{\text{decoy}}$. Different distributions of δ_n for different subsets ensure that the generated decoy signals are sufficiently distinct from each other as required to solve the system of linear equations (2) and (3). We would like to stress that our passive method for "generating" decoys provides distinct advantages: during signal transmission it is still undecided which states will become signal or decoy states. Therefore a distinction between signal and decoy states by Eve is impossible, even in principle. Furthermore, our decoy selection mechanism inherently eliminates many experimental challenges (e.g., different spectra for signal and decoys which introduce distinguishing side information for Eve) which arise in proposals with the same hardware, but a different analysis procedure ([19,20]), which do not draw maximum use of the TMD's capabilities. The remainder of the protocol is identical to a standard decoy scheme: Alice and Bob check e_n and Y_n as described above. Error correction and privacy amplification need to be performed to generate a final secure key. The inset in Fig. 3 presents our simulation results (for details see below). The key generation rate and maximum secure distance closely match a perfect single photon source.

The TMD results cannot only be used to generate decoy states, but also provide improved effective signal statistics. While the error rates e_n for $n \geq 1$ are the order of 10^{-2}, the contribution by vacuum signals is $e_0 = 1/2$ [25]. Thus, it is desirable to remove such events as well as possible. We would like to emphasize that this is not possible with present day technology when a weak coherent laser is employed as source since only a single signal copy is available in this case.

TABLE I. Comparison of the obtainable distances for different signal sources and postprocessing methods with the limits set by a perfect single photon source and the principal physical upper bound. A perfect single photon source achieves 170.9 km for 1-LOCC and 195.2 km for 2-LOCC. $\Delta_{1,\text{f}}$ denotes the difference to this distance. $\Delta_{2,\text{f}}$ denotes the the difference to the principal intercept-resend upper bound. Both refer to the effectively filtered source. At most, 4 B steps were used.

Source	Distance unf./filt.	$\Delta_{1,\text{f}}$	$\Delta_{2,\text{f}}$
Thermal (one way)	130.8/169.7	0.7%	18.3%
Thermal (two way)	174.5/194.5	0.4%	6.3%
Poissonian (one way)	141.2/166.0	2.9%	20.0%
Poissonian (two way)	180.8/193.8	0.7%	6.6%

Decreasing the dark count rate on Bob's side is hard because it requires refinement of the detectors, while fine-grained time triggering can be used on Alice's side to reduce the dark count probability in the TMD to a negligible level, i.e., $p(n|m)=0$ for $n>m$ [12]. Note that due to losses and imperfect detection, filtering multiphoton contributions does not work perfectly and results in comparatively small rate improvements [19]. The benefits are negligible in contrast to filtering zero photon contributions. Alice has recorded the TMD measurement for every signal. Hence, she can easily discard all zero events in the postprocessing phase which leads to a better effective probability distribution given by

$$p_{f,\text{meas}}(n) = \begin{cases} 0, & n=0, \\ \dfrac{1}{N_{\text{tot}} - \sum\limits_{n=1}^{\infty} \# n} \dfrac{\# n}{N_{\text{tot}}}, & n \geq 0, \end{cases} \tag{7}$$

where $p_{f,\text{meas}}$ denotes the measured, filtered distribution; the effectively sent distribution is $\vec{p} = \mathcal{R}(\vec{p}_{f,\text{meas}})$. Since $p(0|n) \neq 0$ for $n>0$, some usable signal states are also removed from the distribution, but this does not endanger the total positive effect of the filtering. To implement the operation, Alice and Bob need to discard all slots in the postprocessing stage where the TMD result was zero and use the inverted probability distribution in the rate calculations. Since this type of filtering is applied in the postprocessing phase, it does not modify the actual signal transmission and no physical blocking is required.

Figure 3 and Table I present the results of the numerical evaluation for all cases discussed above. In order to demonstrate the influence of our different postselection methods we consider four cases: signals with and *without* filtering empty pulses for both 1- and 2-LOCC. In our analysis, we apply an optimization for both, the best value for $\bar{N}$ and the ideal number of B steps for every distance. To allow comparison with other proposals, we use the set of experimental parameters given in [21] (the same data are used for the idler detection which is not part of the referenced scheme). The upper bound on the secure distance caused by the undetectable intercept-resend attack at a QBER of more than 25% [5] lies at 208 km, i.e., the right border of the graph. The *lower* bound on our rate closely approaches this *upper* limit, and reaches the single photon performance. One also needs to keep in mind that this upper bound is not even tight but can be replaced by smaller ones (e.g., [22]).

The filtering transformation in Eq. (7) modifies the effective signal distribution so that a different rate is obtained although the sent statistics remain unmodified. Thus, a penalty factor $p_{\text{pen}}=1-\Sigma_{n=0}^{\infty}p(0|n)p_s(n)$ needs to be introduced into Eq. (1). To find the optimal value of $\bar{N}$, the quantity $p_{\text{pen}}S$ must be maximized. The optimal values for $\bar{N}$ depend on the simulation parameters and the source statistics; a comprehensive set of results for different combinations can be found elsewhere [23]. We would like to mention that the optimization yields values for $\bar{N}$ in the range (0,0.5), which can well be realized with current PDC sources [24]. Existing sources provide better performance than actually required.

As explained above, two-way processing with B steps can increase the achievable distances. Ma *et al.* [15] calculated that after performing a B step, a lower bound on the secure key generation rate is given by $S'=\max[0,qQ_{\bar{N}}(\frac{1}{2}s_{n\neq1}\times\{-f(E'_{\bar{N}})H_2(E'_{\bar{N}})+\Omega'[1-H_2(e'_{1,p})]\})]$. The primed quantities represent the error rate, etc., after the B steps have been performed. A detailed derivation of the formula is beyond the scope of this paper, but can be found in Refs. [15,23]. Multiple rounds of B steps apply the transformation multiple times. The difference between the lower bound on the maximum secure distance and the principal limit shrinks to about 6.5% with 4 B steps as shown in Table. I.

In summary, we have shown how to use the photon number correlations of a PDC source to implement a BB84 scheme which nearly reaches the performance of a single photon scheme. This removes the predominant imperfection from real-world QKD implementations. Since the lower bound on the key generation rate coincides up to a few percent with the principal upper bounds, further improvements need either come from new protocols or improved hardware. Refinements of security proofs will likely be unfruitful by comparison.

We acknowledge helpful comments by N. Lütkenhaus, H.-K. Lo, and J. Lundeen.

[1] C. H. Bennet and G. Brassard, in *Proceedings of the IEEE International Conference on Computer, Systems, and Signals* (IEEE, Los Alamitos, CA, 1984), pp. 175–179.

[2] D. Gottesman and H.-K. Lo, IEEE Trans. Inf. Theory **49**, 457 (2003).

[3] D. Gottesman, H.-K. Lo, N. Lütkenhaus, and J. Preskill, Quantum Inf. Comput. **4**, 325 (2004).

[4] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).

[5] M. Dušek, N. Lütkenhaus, and M. Hendrych, Prog. Opt. (to be published).

[6] W.-Y. Hwang, Phys. Rev. Lett. **91**, 057901 (2003).

[7] H.-K. Lo, X. Ma, and K. Chen, Phys. Rev. Lett. **94**, 230504 (2005).

[8] X. B. Wang, Phys. Rev. Lett. **94**, 230503 (2005).

[9] J. W. Harrington, J. M. Ettinger, R. J. Hughes, and J. E. Nordholt, e-print arXiv:quant-ph/0503002.

[10] X. B. Wang, Phys. Rev. A **72**, 049908(E) (2005).

[11] L. Mandel and E. Wolf, *Optical Coherence and Quantum Optics* (Springer, Berlin, 1995).

[12] D. Achilles, C. Silberhorn, C. Sliwa, K. Banaszek, and I. A. Walmsley, Opt. Lett. **28**, 2387 (2003).

[13] N. Lütkenhaus and M. Jahma, New J. Phys. **4**, 44.1 (2002).

[14] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).

[15] X. Ma, C.-H. F. Fung, F. Dupuis, K. Chen, K. Tamaki, and H.-K. Lo, Phys. Rev. A **74**, 032330 (2006).

[16] J. Perina Jr, O. Haderka, and M. Hamar, e-print arXiv:quant-ph/0310065.

[17] M. J. Fitch, B. C. Jacobs, T. B. Pittman, and J. D. Franson, Phys. Rev. A **68**, 043814 (2003).

[18] D. Achilles, C. Silberhorn, and I. A. Walmsley, Phys. Rev. Lett. **97**, 043602 (2006).

[19] T. Horikiri and T. Kobayashi, Phys. Rev. A **73**, 032331 (2006).

[20] Q. Y. Cai and Y. G. Tan, Phys. Rev. A **73**, 032305 (2006).

[21] D. Gobby, Z. Yuan, and A. Shields, Appl. Phys. Lett. **84**, 19 (2004).

[22] T. Moroder, M. Curty, and N. Lütkenhaus, Phys. Rev. A **73**, 012311 (2006).

[23] W. Mauerer and C. Silberhorn (unpublished).

[24] A. B. U'Ren, C. Silberhorn, K. Banaszek, and I. A. Walmsley, Phys. Rev. Lett. **93**, 093601 (2004).

[25] If a vacuum pulse is sent and a dark count causes one detector to click, it is the wrong one with 50% chance.