Secure Quantum Key Distribution using Continuous Variables of Single Photons

Lijian Zhang,[1,*] Christine Silberhorn,[2] and Ian A. Walmsley[1]

[1]*Clarendon Laboratory, University of Oxford, Parks Road, Oxford OX1 3PU, United Kingdom*

[2]*Institut für Optik, Information und Photonik, Universität Erlangen-Nürnberg, 91058 Erlangen, Germany*

(Received 25 April 2007; published 18 March 2008)

We analyze the distribution of secure keys using quantum cryptography based on the continuous variable degree of freedom of entangled photon pairs. We derive the information capacity of a scheme based on the spatial entanglement of photons from a realistic source, and show that the standard measures of security known for quadrature-based continuous variable quantum cryptography (CV-QKD) are inadequate. A specific simple eavesdropping attack is analyzed to illuminate how secret information may be distilled well beyond the bounds of the usual CV-QKD measures.

DOI: 10.1103/PhysRevLett.100.110504 PACS numbers: 03.67.Dd, 42.50.Dv, 42.79.Sz

The distribution of secret information via optical channels, e.g., quantum key distribution (QKD), provides an important example of the technological capability of quantum correlations. The QKD protocol proposed by Bennett and Brassard [1] and its large collection of variations [2], including QKDs using nonorthogonal states [3] and entangled photons [4], employ single photons or photon pairs to ensure secure information transfer between the source (Alice) and receiver (Bob). The quantum information associated with the single-photon states in these schemes is encoded as dichotomic variables, e.g., in the polarization or relative phases of single-photon superposition states [5]. Thus, the maximum achievable information transfer rate is intrinsically limited to 1 bit per photon. A newer development of QKD utilizes continuous variable (CV) multiphoton systems [6–8] where the amplitude and phase quadratures of coherent states [9,10] or squeezed states [11,12] serve as the information carriers. CV-QKD systems potentially enable higher key distribution rates. Recently, single-photon CV-QKD employing the position and momentum observables has been suggested as a means to increase the information transfer rate by coding more than 1 bit per photon. Compared to quadrature-based CV-QKD, single-photon CV-QKD eliminates the local oscillators required for homodyne detection and, as we will show, decouples the channel loss from the quantum correlations. Experimental implementations have demonstrated the feasibility of these schemes by utilizing the spatial freedom of single photons [13] or entangled photon pairs generated by parametric down-conversion (PDC) [14,15]. Yet, the security of such schemes has not been analyzed and, as we show here, this is not a trivial extension of either BB84 or the conventional CV-QKD security proofs.

In this Letter, we evaluate the potential of the spatial properties of PDC for QKD by considering a realistic PDC source as well as practical detectors and a lossy quantum channel. The analysis here can also be applied to CV-QKD by employing the correlations of time-frequency entangled photon pairs [16]. Spatial correlations are, however, easier to manipulate with current technology. In our analysis we derive the mutual information of the communicating parties from measurable position-momentum correlations of PDC states and bound the information of a potential eavesdropper (Eve) by analyzing detected photocount statistics. Our results lie in the region between conventional dichotomic and continuous variable QKD and highlight the differences between these alternative approaches in terms of the experimental imperfections corrupting the secrecy of the key exchange. Our security analysis, which is mainly based on an intercept-resend eavesdropping strategy, indicates that single-photon CV-QKD gives increased secure bit rates per photon for intermediate channel losses.

During the process of PDC, the pump photon with wave vector $\boldsymbol{k}_p$ splits into two lower frequency (signal and idler) photons with wave vectors $\boldsymbol{k}_s$ and $\boldsymbol{k}_i$. The spatial and spectral properties of the photon pair are correlated by the material dispersion. In what follows it is assumed that the state is spectrally filtered such that the frequencies of signal and idler photons are restricted to $\omega_{s0} = \omega_{i0} = \omega_p/2$. The resulting two-photon state is

$$|\Psi\rangle \approx |\mathrm{vac}\rangle + \mu \iint d\boldsymbol{k}_s^{\perp} d\boldsymbol{k}_i^{\perp} f(\boldsymbol{k}_s^{\perp};\boldsymbol{k}_i^{\perp}) |\boldsymbol{k}_s^{\perp};\boldsymbol{k}_i^{\perp}\rangle. \quad (1)$$

For the practical PDC source, the down-converted modes are usually close to the longitudinal axis with the transverse vectors $|\boldsymbol{k}_s^{\perp}| \ll k_s$ and $|\boldsymbol{k}_i^{\perp}| \ll k_i$ ($k_{s/i} = |\boldsymbol{k}_{s/i}|$). For a pump beam with a Gaussian profile the biphoton amplitude $f(\boldsymbol{k}_s^{\perp};\boldsymbol{k}_i^{\perp})$ can be approximated by

$$\begin{aligned} f(\boldsymbol{k}_s^{\perp};\boldsymbol{k}_i^{\perp}) &= \alpha(\boldsymbol{k}_s^{\perp} + \boldsymbol{k}_i^{\perp}) \phi_L(\boldsymbol{k}_s^{\perp} - \boldsymbol{k}_i^{\perp}) \\ &= C \exp\left[-\frac{w_0^2}{4} |\boldsymbol{k}_s^{\perp} + \boldsymbol{k}_i^{\perp}|^2 \right] \frac{\exp(i\Delta k_z L) - 1}{i\Delta k_z L}, \\ \text{with} \quad \Delta k_z &\approx 2K - k_p - \frac{|\boldsymbol{k}_s^{\perp} - \boldsymbol{k}_i^{\perp}|^2}{4K} \end{aligned} \quad (2)$$

and where $\alpha(\boldsymbol{k}_s^{\perp} + \boldsymbol{k}_i^{\perp})$ originates from the pump envelope and transverse phase-matching function, while $\phi_L(\boldsymbol{k}_s^{\perp} - \boldsymbol{k}_i^{\perp})$ is the longitudinal phase-matching function. C is the constant for normalization, $K = k_s = k_i$, w_0 is the beam

waist of the pump, and L denotes the length of the nonlinear crystal in the z direction [17]. Retaining the longitudinal phase-matching function $\phi_L(\boldsymbol{k}_s^\perp - \boldsymbol{k}_i^\perp)$ is critical to bounding the shared information from above [19].

The joint probability distribution of $\boldsymbol{k}_s^\perp$ and $\boldsymbol{k}_i^\perp$ is given by $p(\boldsymbol{k}_s^\perp;\boldsymbol{k}_i^\perp) = |f(\boldsymbol{k}_s^\perp;\boldsymbol{k}_i^\perp)|^2$. The mutual information between $\boldsymbol{k}_s^\perp$ and $\boldsymbol{k}_i^\perp$ can be calculated from [20]

$$I(\boldsymbol{k}_s^\perp;\boldsymbol{k}_i^\perp) = H(\boldsymbol{k}_i^\perp) - H(\boldsymbol{k}_i^\perp \mid \boldsymbol{k}_s^\perp), \tag{3}$$

where $H(\boldsymbol{k}_i^\perp)$ and $H(\boldsymbol{k}_i^\perp \mid \boldsymbol{k}_s^\perp)$ denote the entropy and conditional entropy, respectively. Similarly, the Fourier transform of Eq. (2) determines the mutual information $I(\boldsymbol{r}_s^\perp;\boldsymbol{r}_i^\perp)$ between the transverse positions of the two photons. We model our practical source of entangled photon pairs by considering degenerate Type-I PDC in a β-BaB_2O_4 (BBO) crystal with a phase-matching angle of 3°, pumped at 400 nm. Figure 1 shows the calculated maximum mutual information that Alice and Bob can extract if they measure with equal probabilities the position and momentum of the photons. The graph illustrates the information transfer gain for CV single-photon systems. This should be compared with binary coding, for which a maximal value of one is obtained. For a fixed pump power, the amount of shared information between PDC photons may be increased by increasing the pump waist w_0 and decreasing the crystal length L, though the penalty is a reduced efficiency of photon-pair generation. The entanglement of the two-photon state in our analysis can be characterized by considering the mutual information for direct measurements of a pair of conjugate continuous variables, namely, the position and momentum of the photons. Alternatively, one may quantify the entanglement contained in this degree of freedom by decomposing the state into its Schmidt modes [21] and evaluating the corresponding concurrence. We verified that this approach yields the same asymptotic behavior, which confirms the consistency of our results with more general entanglement measures. QKD further requires that the measurements of

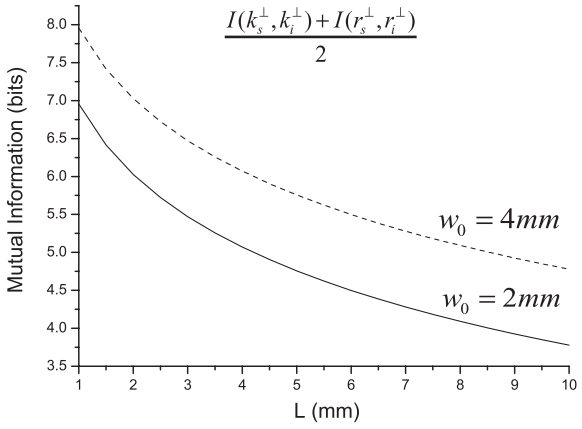

FIG. 1. Mutual information for entangled photon pairs generated by type-I PDC in BBO crystal.

noncorresponding variables do not exhibit correlations; our calculations show that the mutual information between momentum and position $[I(\boldsymbol{k}_s^\perp;\boldsymbol{r}_i^\perp)$ and $I(\boldsymbol{r}_s^\perp;\boldsymbol{k}_i^\perp)]$ is negligible.

To analyze the security of a single-photon CV-QKD system, we choose a specific protocol. Pairs of entangled photons are generated in the nonlinear crystal and transmitted to Alice and Bob separately via a quantum channel. The two parties choose randomly to detect either the position ($\boldsymbol{r}^\perp$) or momentum ($\boldsymbol{k}^\perp$) of each photon they receive. Then Alice and Bob announce by an authenticated public channel the variables that they measured for each photon and drop the bits where they used different variables; the remaining bits constitute the sifted raw key. To accomplish a successful quantum key distribution, the system must allow Alice and Bob to distill a secret key from the sifted raw key that is inaccessible to the adversary, Eve. With forward reconciliation [22] and privacy amplification [23], the achievable secret key rate in momentum is bounded below by

$$\Delta I = I_{AB} - I_{AE} = H(\boldsymbol{k}_A \mid E) - H(\boldsymbol{k}_A \mid \boldsymbol{k}_B), \tag{4}$$

where E is the result of Eve's measurement on her ancilla. For individual attacks, it has been shown that there exists the entropic uncertainty relation [24]

$$H(\boldsymbol{k}_A \mid E) + H(\boldsymbol{r}_A \mid \boldsymbol{r}_B) \geq \log_2 \pi e, \tag{5}$$

The conditional entropy is bounded by [25]

$$H(\boldsymbol{x}_A \mid \boldsymbol{x}_B) \leq \tfrac{1}{2}\log_2[2\pi e \Delta^2(\boldsymbol{x}_A \mid \boldsymbol{x}_B)], \tag{6}$$

where $\boldsymbol{x}$ stands for $\boldsymbol{k}$ or $\boldsymbol{r}$, while Δ^2 denotes the variance. So that by combining Eqs. (4)–(6), we find

$$\Delta I \geq \frac{1}{2}\log_2\left(\frac{1}{4}\frac{1}{\Delta^2(\boldsymbol{r}_A \mid \boldsymbol{r}_B)\Delta^2(\boldsymbol{k}_A \mid \boldsymbol{k}_B)}\right). \tag{7}$$

It follows that a sufficient condition for $\Delta I \geq 0$ is

$$\Delta^2(\boldsymbol{r}_A \mid \boldsymbol{r}_B)\Delta^2(\boldsymbol{k}_A \mid \boldsymbol{k}_B) \leq \tfrac{1}{4}. \tag{8}$$

This result also applies for the security analysis in position. For high entanglement, this condition coincides with the EPR criterion [26]. It is easy to prove from Eq. (2) that the states generated by PDC satisfy this condition, as demonstrated recently [14,15,27]. Note, however, almost all of these experiments employ one detector to scan through the momentum or position values, so in principle the outcome of each measurement is binary: either the photon hits the detector or not. Therefore this setup is not suitable for single-photon CV-QKD. To realize the full potential of continuous variables without complex encoding, a sufficiently large array of detectors [avalanche photodiodes (APDs), pixels of a CCD camera, etc.] is needed to ensure that binning and truncating do not significantly diminish the information transfer rate [28]. This implies that the dark count of the detectors will have a much higher impact on the error rate than in standard BB84, though the proba-

bility that Eve can guess the correct result also decreases with the increased number of detectors.

To see this, assume that the entangled photon pair is generated from the pump pulse with probability P_{PDC} and sent to Alice and Bob through two quantum channels with throughputs t_A and t_B. To measure the continuous variables $\boldsymbol{r}^{\perp}$ or $\boldsymbol{k}^{\perp}$, each party maps the distribution to n identical detectors. We denote the probability of recording a dark count within the detection time window for each detector as P_{dark} and its efficiency as η. Alice and Bob keep the results when one and only one detector clicks. There are three cases to consider: (1) both parties have a dark count; (2) one party detects a photon and the other has a dark count; (3) both parties detect a photon. The probabilities for each case are:

$$P_1 = [1 - P_{\mathrm{PDC}} + P_{\mathrm{PDC}}(1 - \eta t_A) \times (1 - \eta t_B)]n^2 P_{\mathrm{dark}}^2 (1 - P_{\mathrm{dark}})^{2n-2}, \quad (9a)$$

$$P_2 = P_{\mathrm{PDC}}[\eta t_A(1 - \eta t_B) + (1 - \eta t_A)\eta t_B]nP_{\mathrm{dark}}(1 - P_{\mathrm{dark}})^{2n-1}, \quad (9b)$$

$$P_3 = P_{\mathrm{PDC}}\eta^2 t_A t_B (1 - P_{\mathrm{dark}})^{2n}, \quad (9c)$$

respectively. The probability that the photon and a dark count arise at the same detector simultaneously is negligible. Among all the cases, only P_3 will reveal the quantum correlations. This probability decreases as the channel loss and number of detectors increase. Some typical values for the realistic system with APDs as detectors and nanosecond time gating are $P_{\mathrm{PDC}} = 0.01$, $\eta = 0.6$, and $P_{\mathrm{dark}} = 10^{-6}$. We fix the length of the BBO crystal at 2 mm and assume a 2 mm pump waist (FWHM). The source is taken to be at Alice's station, so that $t_A \approx 1$ and $t_B = t$, where t is the transmission of the channel between Alice and Bob. Taking into account the dark count contribution according to Eq. (9), Eq. (8) is satisfied for channel throughput above $t = 36\%$ (68%) [4.4 dB (1.7 dB) channel loss] assuming a detector array with $n = 128$ (256) pixels. For free space transmission the extinction coefficient varies over a large range [29]. Here we assume it is 1 dB/km, so the corresponding distance is 4.4 km and 1.7 km, respectively. At these distances the probability of uncorrelated events $P_1 + P_2$ is less than 1%, which means that the noise level is still extremely low.

Analysis of the variance product seems to suggest that this QKD scheme is not suitable for long-distance use. But note that Eq. (8) is tight bound for the general CV-QKD schemes and it is possible to loosen the bound when considering the special characteristics of the experimental imperfections in the single-photon CV-QKD protocol. Reconsidering Eqs. (4)–(8), note that the equality in Eq. (7) can be achieved only when Eve's attacks satisfy certain strict conditions. The most important condition is that the distribution of Bob's measurement outcomes conditioned on Alice's results should be Gaussian [25]. A Gaussian attack is well known to be optimal for conventional CV-QKD using the quadratures of multiphoton states since in these systems experimental imperfections—mainly the loss of the channel—will preserve the Gaussian character of the transmitted state, broadening Bob's distribution. By replacing the channel with a lossless one and applying a Gaussian attack, Eve can hide in the channel noise. The normal way for Alice and Bob to detect Eve is to monitor the covariance matrix of their results. In contrast, for single-photon dichotomic-variable QKD, the experimental imperfections (loss, noise, etc.) yield uncorrelated detection events between Alice and Bob, which are typically interpreted as background noise. In single-photon CV-QKD the experimental imperfections play a similar role to those in standard dichotomic single-photon QKD. The events registered by each party are either from the PDC photons or from the detector noise, and the latter has a uniform distribution. Hence Alice and Bob expect unbroadened Gaussian joint probability distributions from the quantum correlation measurements interspersed with uncorrelated flat background events, which in total represents a non-Gaussian distribution. In order to stay undetected Eve must mimic this distribution; therefore, she only has limited options and the optimal attack for multiphoton CV-QKD is prohibited here. Moreover, for non-Gaussian distributions, the left side of Eq. (7) can be much bigger than the right side, which means even when the EPR condition is violated, it is still possible for Alice and Bob to draw the secret key.

A possible eavesdropping strategy that satisfies the above conditions is an intercept-resend attack: Eve intercepts the photon sent to Bob, measures it in the randomly chosen variable (momentum or position), and resends a photon in the eigenstate based on her measurement result. If, by chance, she has chosen the same measurement basis as Alice and Bob, her operation will appear as an undisturbed channel between these two parties. Otherwise, by measuring the conjugate variable Eve introduces a flat background noise, which cannot be distinguished from the dark noise of the detector array. Therefore by adjusting the loss of the channel, Eve can hide her disturbance behind the experimental imperfections. We define an intercept-resend ratio λ as

$$\lambda = \frac{\text{number of photons intercepted by Eve}}{\text{total number of photons Alice sends to Bob}}.$$

By balancing the disturbance introduced by Eve with the background noise, which originates from the experimental imperfections, we find an allowed maximum intercept-resend ratio for Eve is

$$\lambda_{\max} \approx \min\left\{\frac{2n}{(\frac{1}{l} - 1)(\frac{1}{P_{\mathrm{dark}}} - 1) + n}, 1\right\}, \quad (10)$$

where l is the channel loss and n is the number of detectors. For a lossless channel ($l = 0$) or noiseless detectors ($P_{\mathrm{dark}} = 0$), $\lambda_{\max} = 0$; i.e., no eavesdropping is possible,

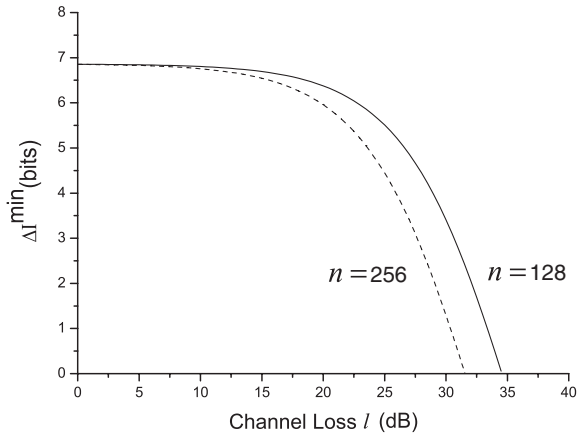

FIG. 2. The minimum secret information per recorded photon pair ($\Delta I^{\min}$) is estimated numerically from $\lambda_{\max}$. The corresponding channel loss l is calculated from Eq. (10). The initial entangled photons are generated by a 2 mm-long BBO crystal and a pump at 400 nm with 2 mm beam waist.

while for fixed l and P_{dark}, $\lambda_{\max}$ increases with n. Equation (10) clearly shows how the experimental imperfections open loopholes for Eve to attack. Moreover, the minimum secret information that Alice and Bob are able to distill ($\Delta I^{\min} = I_{AB}^{\min} - I_{AE}^{\max}$) can be directly estimated from $\lambda_{\max}$. The relation between $\Delta I^{\min}$ and the channel transmission loss is shown in Fig. 2. Comparing this result with the variance product analysis, it is evident that the secure loss level (35 dB for $n = 128$) is significantly improved for this eavesdropping strategy.

An important question in quantum cryptography is the relationship between entanglement and security. It has been proved that distributed entanglement between Alice and Bob is a necessary precondition for secret key distribution [30]. Also the connection between quantum and secret correlations has been established [31]. Nevertheless, it is still not clear how to draw a secure key from the distributed entanglement. For classical privacy amplification (forward or reverse reconciliation), the security limit is usually a stronger condition than the entanglement threshold [32]. In the intercept-resend attack for our protocol, the logarithm negativity as a function of the intercept fraction λ shows that Alice and Bob remain entangled until $\lambda = 1$, while as Fig. 2 and Eq. (10) show, the classical privacy amplification requires $\lambda < 75\%$ (where $\Delta I^{\min} = 0$) to draw the secret key. Hence for a practical QKD scheme, the detection of entanglement may not be enough for secret key distillation.

To conclude, we have shown the potential to transfer more than 1 bit of information per photon using the spatial degrees of freedom of the entangled photon pairs. Because of the special non-Gaussian distributions of Alice and Bob's measurement results, the options for eavesdropping are severely limited. A detailed security analysis on a plausible attack, intercept-resend, is given. Whether Eve gains by means of more powerful attacks requires further study. In particular, a more detailed analysis of the impact of binning the information is required for a practical QKD system using a limited number of detectors.

This work was supported by the EPSRC and the EC under the Integrated Project QAP funded by the IST directorate as Contract No. 015848.

*l.zhang1@physics.ox.ac.uk

[1] C. H. Bennett and G. Brassard, in *Proceedings of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India* (IEEE, New York, 1984), pp. 175–179.
[2] N. Gisin *et al.*, Rev. Mod. Phys. **74**, 145 (2002).
[3] C. H. Bennett, Phys. Rev. Lett. **68**, 3121 (1992).
[4] A. K. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
[5] W. Tittel *et al.*, Phys. Rev. Lett. **84**, 4737 (2000).
[6] T. C. Ralph, Phys. Rev. A **61**, 010303 (1999).
[7] M. D. Reid, Phys. Rev. A **62**, 062308 (2000).
[8] Ch. Silberhorn *et al.*, Phys. Rev. Lett. **88**, 167902 (2002).
[9] F. Grosshans *et al.*, Phys. Rev. Lett. **88**, 057902 (2002).
[10] F. Grosshans *et al.*, Nature (London) **421**, 238 (2003).
[11] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[12] N. J. Cerf *et al.*, Phys. Rev. A **63**, 052311 (2001).
[13] S. P. Walborn *et al.*, Phys. Rev. Lett. **96**, 090501 (2006).
[14] L. Neves *et al.*, Phys. Rev. Lett. **94**, 100501 (2005); M. N. O'Sullivan-Hale *et al.*, Phys. Rev. Lett. **94**, 220501 (2005).
[15] M. P. Almeida *et al.*, Phys. Rev. A **72**, 022313 (2005).
[16] I. Ali-Khan *et al.*, Phys. Rev. Lett. **98**, 060503 (2007).
[17] For the collinear phase-matching situation, where $K = k_p/2$, Eq. (2) becomes Eq. (3) in [18].
[18] S. P. Walborn *et al.*, Phys. Rev. Lett. **90**, 143601 (2003).
[19] In previous treatments of this problem, $\phi_L(\boldsymbol{k}_s^{\perp} - \boldsymbol{k}_i^{\perp})$ has been ignored. See, for example, [15].
[20] C. E. Shannon, Bell Syst. Tech. J. **27**, 379 (1948).
[21] C. K. Law *et al.*, Phys. Rev. Lett. **92**, 127903 (2004).
[22] I. Csiszár and J. Körner, IEEE Trans. Inf. Theory **24**, 339 (1978); G. Brassard *et al.*, Lect. Notes Comput. Sci. **765**, 410 (1994); W. T. Buttler *et al.*, Phys. Rev. A **67**, 052303 (2003); M. Bloch *et al.*, arXiv:cs.IT/0509041.
[23] C. H. Bennett *et al.*, IEEE Trans. Inf. Theory **41**, 1915 (1995).
[24] F. Grosshans *et al.*, Phys. Rev. Lett. **92**, 047905 (2004).
[25] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (John Wiley & Sons, New York, 1991).
[26] M. D. Reid and P. D. Drummond, Phys. Rev. Lett. **60**, 2731 (1988); M. D. Reid, Phys. Rev. A **40**, 913 (1989).
[27] J. C. Howell *et al.*, Phys. Rev. Lett. **92**, 210403 (2004).
[28] The number of detectors should satisfy $n \geq 2^{I_{AB}}$.
[29] C. Kurtsiefer *et al.*, Nature (London) **419**, 450 (2002); R. Ursin *et al.*, Nature Phys. **3**, 481 (2007); J. H. Shapiro, Phys. Rev. A **67**, 022309 (2003).
[30] M. Curty *et al.*, Phys. Rev. Lett. **92**, 217903 (2004).
[31] A. Acín and N. Gisin, Phys. Rev. Lett. **94**, 020501 (2005).
[32] F. Grosshans and N. J. Cerf, arXiv:quant-ph/0306141.