PHYSICAL REVIEW A **86**, 060302(R) (2012)

Gaussian postselection and virtual noiseless amplification in continuous-variable quantum key distribution

Jaromír Fiurášek[1] and Nicolas J. Cerf[2]
[1]*Department of Optics, Palacký University, 17. listopadu 12, 77146 Olomouc, Czech Republic*
[2]*QuIC, Ecole Polytechnique de Bruxelles, Université Libre de Bruxelles, 1050 Brussels, Belgium*
(Received 7 June 2012; revised manuscript received 18 September 2012; published 26 December 2012)

Noiseless amplification or attenuation are two heralded filtering operations that enable amplifying or de-amplifying a quantum state of light with no added noise, at the cost of a small success probability. We show that inserting such noiseless operations in a transmission line improves the performances of continuous-variable quantum key distribution over this line. Remarkably, these noiseless operations do not need to be physically implemented but can simply be simulated in the classical data postprocessing stage. Hence, *virtual* noiseless amplification or attenuation amounts to performing a *Gaussian postselection*, which enhances the secure range or tolerable excess noise while keeping the benefits of Gaussian security proofs.

DOI: 10.1103/PhysRevA.86.060302 PACS number(s): 03.67.Dd, 03.67.Hk, 42.50.−p

I. INTRODUCTION

Continuous-variable quantum key distribution (CV QKD) based on Gaussian states and homodyne or heterodyne detection can achieve very high secret key rates; see, e.g., [1] for a review. Moreover, its practical implementation does not require single-photon detectors and can be made to be compatible with telecommunication optical networks [2]. However, although theory predicts that a secure key can be generated for a pure loss channel over an arbitrary large distance [3], the practical range of CV QKD is currently limited to several tens of kilometers by noise and imperfect classical data processing [4,5].

In contrast to classical optical networks, losses in quantum communication channels cannot be compensated for by usual phase-insensitive amplifiers, as the latter inevitably add noise [6], making the channel insecure. Recently, however, the concept of heralded noiseless quantum amplification has emerged as a novel tool [7], which enables one to probabilistically increase the amplitude of a coherent state without adding any extra noise, $|\alpha\rangle \rightarrow |g\alpha\rangle$ with gain $g > 1$. Of course, a natural question arises whether this noiseless amplifier may improve the performance of QKD, particularly whether it can enhance its secure range. In Ref. [8], it was indeed argued that (a double version of) the noiseless amplifier can be beneficial for device-independent quantum cryptography with single photons.

Here, we investigate this question in more general terms. We start from the observation that any physical realization of the noiseless amplifier turns out to be very demanding. Even the proof-of-principle experimental noiseless amplification of weak coherent states requires state-of-the art technology, such as single-photon addition and subtraction, or an auxiliary source of single photons and multiphoton interference [9–13]. Moreover, the actual success rate of these experiments is much lower than the theoretical predictions due to various experimental limitations, and, furthermore, the noiseless transformation can only be implemented approximately. Such an approach seems rather impractical in the context of CV QKD, where the system should be reasonably simple and robust in order to allow for field deployment.

In this paper, we show that the physical implementation of the noiseless amplifier can be substituted with suitable data processing, so that the amplification is performed only virtually. Just as *virtual* entanglement is used to analyze the security of prepare-and-measure CV QKD protocols [14], it appears that *virtual* noiseless amplification may simulate the associated quantum filter and be beneficial. We also turn our attention to a dual quantum filter called noiseless attenuation, which is analogous to noiseless amplification but with a gain lower than 1 [15]. It probabilistically transforms $|\alpha\rangle \rightarrow |\nu\alpha\rangle$ with gain $\nu < 1$, so it is akin to a beam splitter although it effects a similar de-amplification on any state without adding noise. We prove that noiseless attenuation can be faithfully emulated by classical postprocessing of experimental data with a moderate overhead. Noiseless amplification can, in principle, also be emulated arbitrarily well, but an exact emulation is, in contrast, only possible in the limit of a low success probability. In both cases, the emulation amounts to applying what we call a *Gaussian postselection* of the classical data.

We also demonstrate that (virtual) noiseless amplification or attenuation can extend the range of CV QKD over noisy channels. A simple picture, which provides a good—though not rigorous—intuition of this effect, is as follows. The emitter (Alice) preprocesses her signal states by noiselessly attenuating them, thereby making them strongly indistinguishable to an eavesdropper (Eve) as they all approach vacuum. At the other end of the line, the receiver (Bob) "revives" the signal states by noiselessly amplifying them. Somehow, Eve cannot bias the pre- and postselection filters, and the above "compaction" of the signal states in the channel can only be detrimental to her. In practice, preselection is not needed (it amounts to reducing the modulation variance), while postselection associated with noiseless amplification can be applied virtually on the experimental data.

The usefulness of postselection in CV QKD is well known [16], but it also comes with a strong limitation on the resulting security [17]. Here, we replace this classical filter (i.e., postselection conditionally on some measurement outcome) with a quantum filter (i.e., noiseless amplification or attenuation), which, although it is simulated classically, can be viewed as an entanglement distillation protocol. Thus, our

protocol with postselection is completely equivalent to the following entanglement-based scheme: Alice sends one part of an entangled two-mode squeezed vacuum state through the channel to Bob, who applies a quantum filter in order to distill the entanglement. The successfully distilled entangled states are then used in an ordinary deterministic CV QKD protocol where both Alice and Bob perform Gaussian measurements on their parts of the shared states. Due to this equivalence with an effective deterministic Gaussian protocol, all security proofs and corresponding secret key rates that have been obtained based on the optimality of Gaussian attacks [18–20] fully apply to the protocol discussed here.

II. CV QKD PROTOCOLS

Gaussian protocols, to which we restrict ourselves here, are based on the Gaussian modulation of Gaussian (coherent or squeezed) states of light and Gaussian (homodyne or heterodyne) measurements, which gives four possibilities. In the first two protocols, Bob performs homodyne detection, measuring at random the x or p quadrature, while Alice emits a Gaussian-modulated coherent [21] or squeezed [22] state. In the next two, Bob performs heterodyne detection, measuring the x and p quadratures simultaneously, while Alice emits again a coherent [23] or squeezed [24] state. Note the existence of a fifth protocol, where Alice sends (mixed) thermal states instead of pure states [25].

In what follows, we focus on the most symmetric protocol [23], where Alice emits coherent states $|\alpha\rangle$ and Bob projects onto coherent states $|\beta\rangle$ (heterodyne detection), as illustrated in Fig. 1(a). Alice draws a complex amplitude α from a bivariate Gaussian distribution of variance V, and sends $|\alpha\rangle$ to Bob through a quantum channel $\mathcal{L}$ which is controlled by Eve. Then, Bob makes a projective measurement onto coherent states and obtains the complex outcome β. After N repetitions of these steps, Alice and Bob extract a secret key from the accumulated classical data. From Eve's point of view, this prepare-and-measure protocol is indistinguishable from an entanglement-based scheme where Alice prepares an entangled two-mode squeezed vacuum state,

$$|\Psi_{\rm EPR}\rangle = \sqrt{1-\lambda^2}\sum_{n=0}^{\infty}\lambda^n|n,n\rangle, \qquad (1)$$

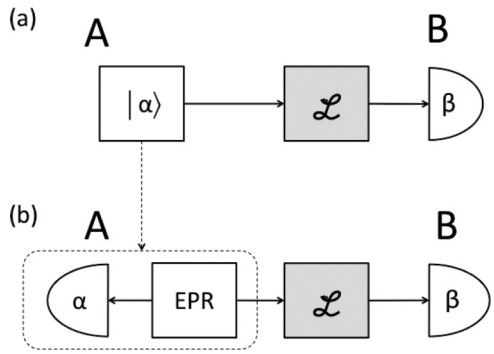

FIG. 1. (a) Prepare-and-measure CV QKD protocol with coherent states and heterodyne detection. (b) Equivalent virtual entanglement-based protocol, with heterodyne detection on both sides.

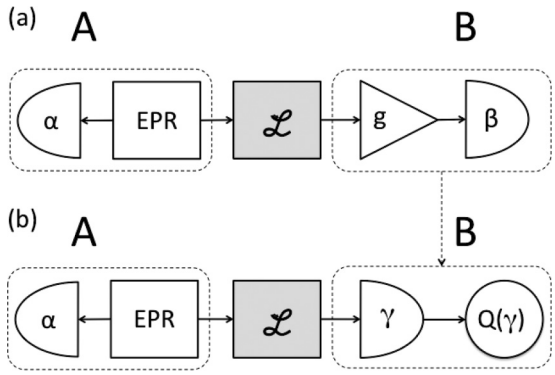

FIG. 2. (a) CV QKD with coherent states and heterodyne detection augmented with noiseless amplification of the received signal. (b) Equivalent protocol where noiseless amplification is emulated by postprocessing Bob's measurement data.

with $\lambda^2 = 2V/(2V+1)$, and performs heterodyne measurement on one mode; see Fig. 1(b).

This virtual entanglement picture [14] is very useful for analyzing the security and understanding the benefit of noiseless amplification. Suppose that $\mathcal{L}$ is a pure loss channel with transmittance T. As shown in Ref. [26], an entangled state (1) can be faithfully distributed over $\mathcal{L}$ if Alice sends one mode of a weakly entangled state ($\lambda \ll 1$) to Bob, who noiselessly amplifies his mode. In the considered CV QKD protocol, this would correspond to weak modulation on Alice's side ($V \ll 1$) combined with noiseless amplification on Bob's side; see Fig. 2(a).

III. VIRTUAL NOISELESS AMPLIFICATION

The noiseless amplifier is described by the nonunitary operator $g^{\hat{n}}$, where $\hat{n}$ denotes the photon number operator. Although it is probabilistic, this filter is Gaussian in the sense that it converts a Gaussian state into another Gaussian state. This filter can be viewed as distilling the virtual entanglement between Alice and Bob, hence effectively converting the channel $\mathcal{L}$ into another channel with presumably higher associated performances. Unfortunately, $g^{\hat{n}}$ is an unbounded operator for $g > 1$, so it cannot be implemented exactly, and, furthermore, its optical implementation is very challenging. Remarkably, these obstacles can be overcome by emulating the noiseless amplifier, which is possible as it is immediately followed by heterodyne measurement. Note that we can formally consider the noiseless amplifier $g^{\hat{n}}$ at the output of channel $\mathcal{L}$ to be part of the detection process; see Fig. 2(a). Denoting by $\hat{\rho}$ the mixed state at the output of $\mathcal{L}$, Bob obtains (after amplification) the measurement outcome β with relative (unnormalized) probability

$$P_g(\beta) = \frac{1}{\pi}\,\langle\beta|g^{\hat{n}}\hat{\rho}\,g^{\hat{n}}|\beta\rangle. \qquad (2)$$

Using the identity $g^{\hat{n}}|\beta\rangle = e^{(g^2-1)|\beta|^2/2}|g\beta\rangle$, we can write

$$P_g(\beta) = \frac{1}{\pi}\,e^{(g^2-1)|\beta|^2}\langle g\beta|\hat{\rho}|g\beta\rangle. \qquad (3)$$

If Bob directly measures $\hat{\rho}$ without prior amplification, he gets the outcome γ with probability $P(\gamma) = \frac{1}{\pi}\langle\gamma|\hat{\rho}|\gamma\rangle$. By

comparing this probability with Eq. (3), we see that Bob can emulate the noiseless amplifier by properly rescaling each measurement outcome γ as $\beta = \gamma/g$, while assigning to it a relative weight $Q(\gamma) = e^{(1-g^{-2})|\gamma|^2}$; see Fig. 2(b).

This relative weight can be simulated by postselection, accepting each piece of data γ with a probability $P_{\rm acc}(\gamma)$ that is proportional to $Q(\gamma)$. After each measurement, Bob publicly announces whether the result is kept or rejected, which is equivalent to establishing the success or failure of entanglement distillation in the virtual entanglement picture. A difficulty arises here because $Q(\gamma)$ diverges for large $|\gamma|$, which reflects the impossibility of implementing a perfect noiseless amplifier. If Alice's modulation V is weak enough, $P(\gamma)$ could be sufficiently narrow so that $\lim_{|\gamma|\to\infty} P(\gamma)Q(\gamma) = 0$. Then, for a finite number N of data points γ_j, one can accept each one with probability

$$P_{\rm acc}(\gamma) = e^{(1-g^{-2})(|\gamma|^2-|\gamma_M|^2)} \leqslant 1, \tag{4}$$

where $|\gamma_M| = \max_j |\gamma_j|$. Unfortunately, the resulting number of accepted data points $N_{\rm acc}$ grows sublinearly with the size N, so that the rejection rate increases with N and the procedure becomes inefficient (see the Supplemental Material [27]). Alternatively, one can fix $|\gamma_M|$ independently of N. For instance, if $P(\gamma)Q(\gamma)$ is expected to exhibit a distribution with variance V_γ, then one can choose $|\gamma_M|$ equal to a few standard deviations $\sqrt{V_\gamma}$ and set $P_{\rm acc}(\gamma) = 1$ if $|\gamma| > |\gamma_M|$. Assuming a Gaussian distribution of variance V_B for Bob's measurement outcomes γ, we find that $N_{\rm acc}$ scales linearly with N in this case (see the Supplemental Material [27]), namely

$$\frac{N_{\rm acc}}{N} \approx \frac{g^2}{g^2 + 2V_B(1-g^2)}\left[e^{-(1-g^{-2})|\gamma_M|^2} - e^{-\frac{|\gamma_M|^2}{2V_B}}\right]. \tag{5}$$

Note that this only works if $2V_B < g^2/(g^2-1)$. Given its linear scaling, this second method is more practical than the first one, although the data processing does not emulate the exact Gaussian filter because of the finite cutoff, which might complicate the security analysis.

IV. VIRTUAL NOISELESS ATTENUATION

We also consider a reverse situation in which the noiseless amplifier is on Alice's side (replaced, in fact, by a larger modulation variance V), while the noiseless attenuator is on Bob's side (replaced by its virtualization). Noiseless attenuation $\nu^{\hat{n}}$ with $\nu < 1$ is a physical operation which can be implemented by sending the state through a beam splitter of transmittance ν^2 and projecting the auxiliary output port of the beam splitter onto a vacuum state. Although the efficiency of common single-photon detectors is too low to implement this latter projection with high fidelity, one can faithfully emulate noiseless attenuation with a moderate overhead. The principle is the same as before. Denoting by $\hat{\rho}$ the state emerging from $\mathcal{L}$, the relative (unnormalized) probability of the measurement outcome β after attenuation can be expressed as

$$P_\nu(\beta) = \frac{1}{\pi}\langle\beta|\nu^{\hat{n}}\hat{\rho}\,\nu^{\hat{n}}|\beta\rangle = \frac{1}{\pi}e^{-(1-\nu^2)|\beta|^2}\langle\nu\beta|\hat{\rho}|\nu\beta\rangle. \tag{6}$$

Since $\nu < 1$, we have $e^{-(1-\nu^2)|\beta|^2} \leqslant 1$, hence no divergence problem. Therefore, we can emulate noiseless attenuation by rescaling the measurement outcome γ as $\beta = \gamma/\nu$ and accepting the data point with probability $Q(\gamma) = e^{-(\nu^{-2}-1)|\gamma|^2} < 1$. In this way, we postselect a subset of the original data that corresponds to a protocol where the signal would be noiselessly attenuated before heterodyne detection. This emulation is efficient as the number of accepted data points is proportional to the original size (see the Supplemental Material [27]),

$$\frac{N_{\rm acc}}{N} = \frac{\nu^2}{\nu^2 + 2V_B(1-\nu^2)}. \tag{7}$$

V. CV QKD WITH GAUSSIAN POSTSELECTION

Exploiting that the (Gaussian) quantum filter effected by the noiseless amplifier or attenuator can be emulated in the postprocessing stage, we now investigate the benefit of the resulting Gaussian postselection for CV QKD. We consider a Gaussian lossy channel with excess noise, which is described by the linear canonical transformation

$$\hat{a}_{\rm out} = \sqrt{T}\,\hat{a}_{\rm in} + \sqrt{1-T}\,\hat{c}, \tag{8}$$

where $\hat{a}$ and $\hat{c}$ denote the annihilation operators of the signal and ancilla modes, respectively, and T is the channel transmittance. A channel which is not quantum-noise-limited is modeled by assuming that the ancilla mode is initially prepared in a thermal state with mean photon number $\langle c^\dagger c\rangle = \bar{n}_{\rm th}/(1-T)$, where $\bar{n}_{\rm th}$ is the mean number of excess thermal photons at the output of the channel. Sending one part of the entangled state (1) through this channel yields a mixed two-mode Gaussian state with covariance matrix

$$\gamma_{AB} = \begin{pmatrix} a\,I & c\,\sigma_z \\ c\,\sigma_z & b\,I \end{pmatrix}, \tag{9}$$

where $a = \cosh(2r)$, $b = T\cosh(2r) + 1 - T + 2\bar{n}_{\rm th}$, $c = \sqrt{T}\sinh(2r)$, and $r = \tanh^{-1}(\lambda)$. Here, I stands for the 2×2

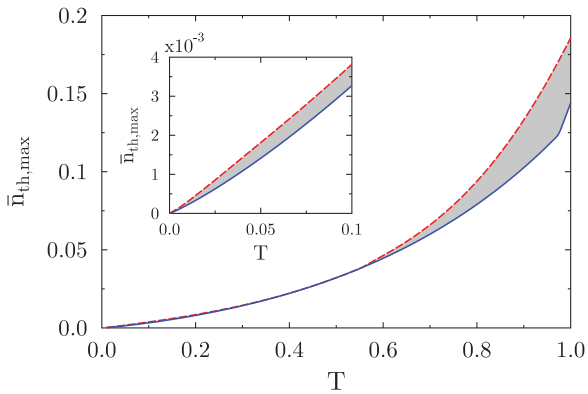

FIG. 3. (Color online) CV QKD over a lossy channel of transmittance T and output excess thermal noise $\bar{n}_{\rm th}$. The maximum tolerable noise $\bar{n}_{\rm th,max}$ decreases for decreasing T. A secret key can be generated if $\bar{n}_{\rm th} < \bar{n}_{\rm th,max}$, shown with the blue solid line (standard protocol) or red dashed line (protocol augmented with virtual noiseless amplification). The gray area indicates the class of channels for which noiseless amplification is beneficial. We optimize over Alice's modulation variance V and Bob's amplification gain g, and we assume the reconciliation efficiency $\eta = 0.9$. The inset shows a zoom-in of the region of high losses, $T \leqslant 0.1$.

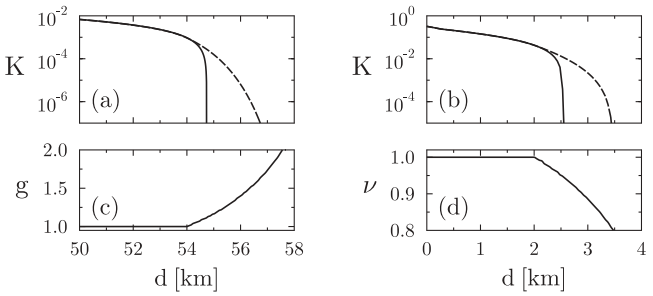

FIG. 4. Achievable secret key rate K in CV QKD over a lossy channel with 0.2 dB losses per km. (a) Comparison of the protocol without Gaussian postselection (solid line) and with optimal noiseless amplification (dashed line), $n_{\rm th} = 2.5 \times 10^{-3}$, $\gamma_M = 3\sqrt{V_\gamma}$. (b) Comparison of the protocol without Gaussian postselection (solid line) and with optimal noiseless attenuation (dashed line), $n_{\rm th} = 0.1$. We assume $\eta = 0.9$, and the parameters V, g, and ν were optimized for each d so as to maximize K. The resulting optimal g and ν are plotted in panels (c) and (d), respectively.

identity matrix and σ_z stands for the third Pauli matrix. The covariance matrix of the Gaussian state obtained conditionally on the success of $g^{\hat{n}}$ (or $\nu^{\hat{n}}$) can be conveniently calculated (see the Supplemental Material [27]) by exploiting a connection between covariance matrix elements and density matrix elements in the Fock basis [28]. The secret key rate against collective attacks is calculated according to

$$K = \max(\eta I_{AB} - \chi_{AE}, \eta I_{AB} - \chi_{BE}), \tag{10}$$

where the first (second) term corresponds to direct (reverse) reconciliation, so we choose the protocol that yields the highest secret key rate (η is the reconciliation efficiency). Here, I_{AB} is Shannon mutual information between Alice and Bob, while χ_{AE} (χ_{BE}) is the Holevo quantity between Alice and Eve (Bob and Eve). Since we know the postselected virtual Gaussian entangled state shared by Alice and Bob, all these quantities can be calculated using standard methods (see the Supplemental Material [27]).

Figure 3 illustrates that the CV QKD protocol tolerates more excess thermal noise $\bar{n}_{\rm th}$ for a fixed T when it is augmented with virtual noiseless amplification. A clear improvement is obtained even for very high losses; see the inset of Fig. 3. This effect may be connected to the improvement brought about by inserting an optical amplifier in front of Bob's detector in CV QKD [29], although here the amplification is noiseless and pushed at the classical postprocessing level, so it suffers basically no imperfection. The benefit is also clear in Fig. 4, where we exhibit the dependence of the achievable secret key rate K on the channel length d, assuming 0.2 dB losses per km. We can see that the postselection becomes useful and increases the key rate as soon as d exceeds a certain threshold depending on the channel parameters. The plotted key rates include the effect of the rejection due to postselection, as specified by Eqs. (5) and (7), but they neglect the slight non-Gaussianity induced by the postselection cutoff γ_M. While Fig. 4(a) illustrates the improvement due to noiseless amplification, we see in Fig. 4(b) that noiseless attenuation also helps to increase the key rate and secure range of the protocol in the high-noise low-loss regime. This unexpected benefit of noiseless attenuation is actually more understandable if we consider an amplifying channel instead of a lossy channel (see the Supplemental Material [27], where it is shown that noiseless attenuation increases the maximum tolerable noise of an amplifying channel, which is an effect dual to that depicted in Fig. 3). Note finally that in Figs. 3 and 4, we have taken a realistic value $\eta = 0.9$ for the efficiency of the classical data reconciliation [4,5]. The gain of virtual noiseless amplification in Fig. 4(a) would be even stronger for larger efficiencies, which are becoming reachable nowadays with sophisticated error-correcting codes [30].

VI. CONCLUSION

We have demonstrated the improved performance (enhanced secure range or tolerable excess noise) of a CV QKD protocol with coherent states, heterodyne detection, and *virtual* noiseless amplification or attenuation. The latter two quantum filters do not need to be physically implemented, which would be experimentally quite challenging, but they may be simulated by classical postprocessing (Gaussian postselection) of the measured data, making this proposal immediately applicable in practical CV QKD. Furthermore, since the postselected data can be treated as emerging from an effective deterministic Gaussian protocol, the standard security proofs based on Gaussian extremality still hold.

One may also consider virtual operations in protocols where Bob performs homodyne detection. A noiseless attenuation followed by the projection onto squeezed displaced states can be interpreted as a projection onto a squeezed displaced state with lower squeezing and rescaled displacements. Thus, to simulate noiseless attenuation, we would need to change the detection scheme so that it performs projections onto finitely squeezed states. This could be achieved by employing an eight-port homodyne detection with an unbalanced central beam splitter. In view of all this, we anticipate that Gaussian postselection may become a tool of practical importance in quantum communication.

Note added. Recently, the usefulness of noiseless amplification in CV QKD has been independently demonstrated in [31] and [32].

ACKNOWLEDGMENTS

J.F. acknowledges support from the Czech Science Foundation (P205/12/0577). N.J.C. acknowledges support from the F.R.S.-FNRS under project HIPERCOM.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).

[2] J. Lodewyck, M. Bloch, R. Garcia-Patron, S. Fossier, E. Karpov, E. Diamanti, T. Debuisschert, N. J. Cerf, R. Tualle-Brouri, S. W. McLaughlin, and P. Grangier, Phys. Rev. A **76**, 042305 (2007).

[3] F. Grosshans, G. Van Assche, J. Wenger R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).

[4] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).

[5] P. Jouguet, S. Kunz-Jacques, T. Debuisschert, S. Fossier, E. Diamanti, R. Allaume, R. Tualle-Brouri, P. Grangier, A. Leverrier, P. Pache, and P. Painchault, Opt. Express **20**, 14030 (2012); P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, arXiv:1210.6216.

[6] C. M. Caves, Phys. Rev. D **26**, 1817 (1982).

[7] T. C. Ralph and A. P. Lund, in *Quantum Communication Measurement and Computing*, Proceedings of the 9th International Conference, edited by A. Lvovsky (AIP, New York 2009), pp. 155–160.

[8] N. Gisin, S. Pironio, and N. Sangouard, Phys. Rev. Lett. **105**, 070501 (2010).

[9] G. Y. Xiang, T. C. Ralph, A. P. Lund, N. Walk, and G. J. Pryde, Nat. Phot. **4**, 316 (2010).

[10] F. Ferreyrol, M. Barbieri, R. Blandino, S. Fossier, R. Tualle-Brouri, and P. Grangier, Phys. Rev. Lett. **104**, 123603 (2010).

[11] M. A. Usuga, C. R. Muller, C. Wittmann, P. Marek, R. Filip, C. Marquardt, G. Leuchs, and U. L. Andersen, Nat. Phys. **6**, 767 (2010).

[12] A. Zavatta, J. Fiurášek, and M. Bellini, Nat. Phot. **5**, 52 (2011).

[13] C. I. Osorio, N. Bruno, N. Sangouard, H. Zbinden, N. Gisin, and R. T. Thew, Phys. Rev. A **86**, 023815 (2012).

[14] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).

[15] M. Mičuda, I. Straka, M. Miková, M. Dušek, N. J. Cerf, J. Fiurášek, and M. Ježek, Phys. Rev. Lett. **109**, 180503 (2012).

[16] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).

[17] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006); **76**, 022313 (2007).

[18] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).

[19] M. Navascués, F. Grosshans, and A. Acin, Phys. Rev. Lett. **97**, 190502 (2006).

[20] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).

[21] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).

[22] N. J. Cerf, M. Levy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).

[23] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004); S. Lorenz, N. Korolkova, and G. Leuchs, Appl. Phys. B **79**, 273 (2004).

[24] R. Garcia-Patron and N. J. Cerf, Phys. Rev. Lett. **102**, 130501 (2009).

[25] C. Weedbrook, S. Pirandola, S. Lloyd, and T. C. Ralph, Phys. Rev. Lett. **105**, 110501 (2010).

[26] T. C. Ralph, Phys. Rev. A **84**, 022339 (2011).

[27] See Supplemental Material at http://link.aps.org/supplemental/10.1103/PhysRevA.86.060302 for details on Gaussian postselection, the determination of covariance matrices, and the calculation of secret key rates.

[28] J. Eisert, D. E. Browne, S. Scheel, and M. B. Plenio, Ann. Phys. (NY) **311**, 431 (2004).

[29] S. Fossier, E. Diamanti, T. Debuisschert, R. Tualle-Brouri, and P. Grangier, J. Phys. B **42**, 114014 (2009).

[30] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).

[31] R. Blandino, A. Leverrier, M. Barbieri, J. Etesse, P. Grangier, and R. Tualle-Brouri, Phys. Rev. A **86**, 012327 (2012).

[32] N. Walk, T. Symul, P. K. Lam, and T. C. Ralph, arXiv:1206.0936.