A simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation

Anthony Leverrier, Philippe Grangier

Simple proof that Gaussian attacks are optimal among collective attacks against continuous-variable quantum key distribution with a Gaussian modulation

Anthony Leverrier
Institut Telecom/Telecom ParisTech, CNRS LTCI, 46, rue Barrault, F-75634 Paris Cedex 13, France

Philippe Grangier
Laboratoire Charles Fabry, Institut d'Optique, CNRS, University Paris-Sud, Campus Polytechnique, RD 128, F-91127 Palaiseau Cedex, France

(Received 21 December 2009; revised manuscript received 12 March 2010; published 15 June 2010)

In this article, we give a simple proof of the fact that the optimal collective attacks against continuous-variable quantum key distribution with a Gaussian modulation are Gaussian attacks. Our proof, which makes use of symmetry properties of the protocol in phase space, is particularly relevant for the finite-key analysis of the protocol and therefore for practical applications.

DOI: 10.1103/PhysRevA.81.062314 PACS number(s): 03.67.Dd

I. INTRODUCTION

Quantum key distribution (QKD) is a cryptographic primitive allowing two distant parties, traditionally referred to as Alice and Bob, to establish a secret key [1]. This key can later be used to secure sensitive communication thanks to a one-time pad, for instance. QKD has received a lot of attention lately as it is the first application of quantum information science which could be developed on a large scale. For instance, metropolitan networks are certainly compatible with present technology, as was recently demonstrated in Vienna with the SECOQC project [2].

Historically, QKD protocols have used discrete variables, meaning that Alice and Bob exchange information encoded on a finite-dimensional Hilbert space such as the polarization of a single photon. Hence, protocols such as the Bennett-Brassard 1984 protocol (BB84) [3] have been studied for a long time, and their unconditional security is well established today [4], at least in a scenario where side channels are not considered [5].

More recently, it was suggested that one could encode information on continuous variables in phase space to perform QKD [6]. Practical schemes requiring only coherent states together with an homodyne detection were introduced by Grosshans and Grangier in 2002 (GG02), first with direct [7] and then with reverse [8] reconciliation, and later successfully implemented [9,10]. These protocols were proven secure against collective attacks [11,12], which are optimal in the asymptotic limit [13]. Let us recall that the optimal collective attacks are Gaussian attacks, meaning that the eavesdropper operation corresponds to a Gaussian map.

The basic idea of the protocol GG02 is the following: Alice draws two random numbers q_A and p_A with a Gaussian probability distribution and sends the coherent state $|q_A + ip_A\rangle$ to Bob. Bob chooses a random quadrature and performs a homodyne detection for that quadrature: He then obtains the classical variable y, a noisy version of either q_A or p_A. He finally informs Alice of his choice of quadrature. Alice keeps her relevant classical variable, which she denotes as x. Repeating this operation n times, Alice and Bob end up with two correlated vectors $\mathbf{x} = (x_1, \ldots, x_n)$ and $\mathbf{y} = (y_1, \ldots, y_n)$, from which they can distill a secret key by applying the usual classical postprocessing composed of parameter estimation, error reconciliation, and privacy amplification. Note that a small variation of this protocol consists in performing a heterodyne detection on Bob's side instead of a homodyne detection [14]. The security of this variant was investigated in [15,16], where the optimal attack was given.

Other variations of this GG02 protocol consist in replacing the Gaussian modulation with a discrete modulation [17–23] or adding a postselection procedure to the protocol [24–28].

One main advantage of the protocols with a Gaussian modulation but without postselection is that they display a high level of symmetry. In particular, a specific symmetry of these protocols in phase space was recently investigated in [29] and appears to be a good approach in order to improve the known lower bounds of the secret-key rate against arbitrary attacks *in the finite-size regime*. Remember that Ref. [13] proves that collective attacks are optimal in the asymptotic regime thanks to a de Finetti–type theorem, which gives rather conservative bounds when finite-size effects are taken into account. A general framework for the finite-size analysis of QKD was developed in [30], and the first numerical results appear to be rather pessimistic [31], hence giving incentive to improve known bounds, in particular with the help of symmetries. Partial results in this direction, such as a de Finetti–type theorem in phase space, were already obtained in [32]. Whereas in [29], the authors examined the possibility of using the specific symmetries of GG02 to prove the security of the protocol against general attacks, our goal here is more modest, as we show that these symmetries allow one to easily recover known results concerning the optimality of Gaussian attacks among all collective attacks. A difference between our proof and previous techniques [11,12] is that it can be applied in the finite-size scenario.

II. SECURITY PROOF AGAINST COLLECTIVE ATTACKS

The main idea of our proof is to use symmetries of the protocol to simplify the analysis of its security. In general, the security of a usual "prepare and measure" protocol where Alice prepares and sends quantum states to Bob (coherent states with a Gaussian modulation in the case of GG02) is analyzed through an equivalent entangled version of the protocol. For

GG02, this entangled version for Alice consists of preparing two-mode squeezed vacua, measuring one mode of these states with a heterodyne detection, and sending the other mode to Bob through the quantum channel [33].

The security of the entangled protocol is then analyzed through the n-mode bipartite quantum state $\rho_{AB} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ shared by Alice and Bob before they perform their measurements. Here, $\mathcal{H}_A$ and $\mathcal{H}_B$ refer respectively to Alice's and Bob's single-mode Hilbert spaces. Unfortunately, the total Hilbert space $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ is usually too big to allow for a complete analysis.

A solution is therefore to use specific symmetries of the protocol in order to show that only a symmetric subspace of $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ needs to be considered. Indeed, one can show that if a QKD protocol is invariant under a certain class of symmetries, say invariance under permutation of the subsystems of Alice and Bob, then one can safely assume that the quantum state ρ_{AB} displays the same symmetry.

This might look a bit suspicious at first sight as one may object that the eavesdropper is free to break the symmetry of the state, hence invalidating the previous statement. The way to solve this apparent paradox is to recall that, without loss of generality, one can always assume that Eve is given a purification $|\psi\rangle_{ABE}$ of ρ_{AB}. Since the protocol is invariant under the group of symmetry $\mathcal{G}$, Alice and Bob can consider the state $\bar{\rho}_{AB}$, which is obtained by averaging their initial state ρ_{AB} over the group $\mathcal{G}$. As far as Alice and Bob are concerned, applying the QKD protocol (measurements, parameter estimation, reconciliation, and privacy amplification) to the state $\bar{\rho}_{AB}$ is indistinguishable from applying it to the state ρ_{AB}. Now, because the state $\bar{\rho}_{AB}$ is invariant under the action of $\mathcal{G}$, it is possible to find a purification $|\bar{\psi}\rangle_{ABE}$ of this state such that $g|\bar{\psi}\rangle_{ABE} = |\bar{\psi}\rangle_{ABE}$ for all $g \in \mathcal{G}$. This was proven in the case of the symmetric group $\mathcal{S}_n$ in [4] and in the case of locally compact groups in [34]. Then, it is shown in [34] that there exists a completely positive trace-preserving map $\mathcal{T}$ mapping $|\bar{\psi}\rangle_{ABE}$ to $|\psi\rangle_{ABE}$. Hence, the eavesdropper has at least as much information when her state corresponds to the symmetric purification $|\bar{\psi}\rangle_{ABE}$ as when her state corresponds to the (not necessarily symmetric) purification $|\psi\rangle_{ABE}$. This means that considering the state $|\bar{\psi}\rangle_{ABE}$ is sufficient to evaluate the security of the protocol. As a conclusion, Alice and Bob can always assume that their bipartite state displays the same symmetry properties as the QKD protocol.

In addition to using specific symmetries of the protocol, one can simplify the security analysis further by restricting the eavesdropper's action to a certain class of attacks, for instance, *collective attacks*. This means that the bipartite quantum state shared by Alice and Bob is assumed to be independent and identically distributed (i.i.d.), that is, that there exists a probability distribution $p(\sigma_{AB})$ on $\mathcal{H}_A \otimes \mathcal{H}_B$ such that

$$\rho_{AB} = \int \sigma_{AB}^{\otimes n} p(\sigma_{AB}) \mathrm{d}\sigma_{AB}. \tag{1}$$

In the case of protocols such as BB84, which are invariant under permutation of Alice's and Bob's subsystems, it is useless to consider symmetries of the protocol when considering collective attacks since an i.i.d. state is clearly invariant under permutation of its subsystems. The converse property is not true in general. However, the exponential version of the de Finetti theorem [35] and the postselection technique introduced in [34] show that it also holds asymptotically.

In the case of continuous-variable QKD protocols, one can consider a specific symmetry in phase space [29] which is not strictly implied by collective attacks. The protocol GG02 is indeed invariant under conjugate passive symplectic operations applied by Alice and Bob. Physically, this invariance means that the protocol is not affected when Alice processes her n modes into any passive linear interferometer while Bob processes his n modes into the passive linear interferometer effecting the conjugate orthogonal transformation in phase space. To see this, it is enough to show that the reconciliation procedure as well as the parameter estimation would perform equally well regardless of whether conjugate passive symplectic operations are applied. Let us consider first the reconciliation procedure, which consists of turning Alice's and Bob's measurement results into identical bitstrings. Such a procedure (see Ref. [36] for a specific example) is designed to work in the case where Alice's classical data follow a Gaussian modulation and the correlation between Alice's and Bob's data is measured by their covariance. Since passive symplectic operations in phase space correspond to orthogonal transformations for Alice's and Bob's measurement results, neither the Gaussian modulation nor the covariance of the data are affected, which guarantees that the reconciliation procedure is transparent to such transformations. Concerning the parameter estimation, which is used in particular to compute Eve's information, it is notable that for the protocol GG02, only the covariance matrix of the state ρ_{AB} should be estimated, and more specifically only the *transmission* and *excess noise* of the quantum channel. Both these quantities are invariant under any orthogonal transformation of the data. This means that the state ρ_{AB} can safely be considered to be invariant under conjugate passive Gaussian operations applied by Alice and Bob.

Using this symmetry together with the assumption of collective attacks leads to a simple proof that the optimal collective attacks are Gaussian. More precisely, if the adversary is restricted to perform a collective attack, Alice and Bob can safely assume that this attack is Gaussian. To show this, it is enough to prove that the state ρ_{AB} can be considered Gaussian. Indeed, at the beginning of the protocol, Alice prepares n two-mode squeezed states, which is a $2n$-mode Gaussian state. If the quantum state shared by Alice and Bob at the end of the protocol is also Gaussian, it means that the quantum channel can be described as a Gaussian map. Our proof is based on the following lemma.

Lemma 1. If a bipartite $2n$-modal quantum state ρ_{AB} (for $n \geqslant 2$) is both i.i.d. and invariant under conjugate passive Gaussian operations, then ρ_{AB} is a Gaussian state.

Proof. Let us first rephrase the lemma in phase-space representation. Any state ρ_{AB} is completely characterized by its Wigner function $W_\rho(x,p,y,q)$ where x,p are n-dimensional vectors corresponding to Alice's phase space and y,q correspond to Bob's phase space. The application of a passive Gaussian operation on Alice's modes and of its conjugate operation on Bob's modes maps the state ρ to the state ρ'. The Wigner function $W_{\rho'}(x,p,y,q)$ of ρ' is equal to $W_\rho(x',p',y',q')$ for the change of coordinates $(x',p',y',q') = S^T(x,p,y,q)$ and

the symplectic map S can be written as

$$S = S(X,Y) \equiv \begin{pmatrix} X & Y & 0 & 0 \\ -Y & X & 0 & 0 \\ 0 & 0 & X^T & -Y^T \\ 0 & 0 & Y^T & X^T \end{pmatrix} \tag{2}$$

where the matrices X and Y are such that [37]

$$X^T X + Y^T Y = X X^T + Y Y^T = 1 \tag{3}$$

$$X^T Y, \quad X Y^T \quad \text{symmetric.} \tag{4}$$

In order to prove the lemma, we observe that if any such map S leaves the Wigner function invariant, then W can only depend on three parameters, which are $||x||^2 + ||p||^2$, $||y||^2 + ||q||^2$, and $x \cdot y - p \cdot q$ (a proof of this fact can be found in Appendix A). This means that there exists a function $f : \mathbb{R}^+ \times \mathbb{R}^+ \times \mathbb{R} \mapsto \mathbb{R}$ such that

$$W_\rho(x,p,y,q) = f(||x||^2 + ||p||^2, ||y||^2 + ||q||^2, x \cdot y - p \cdot q). \tag{5}$$

Then, since ρ_{AB} is an i.i.d. state, the same must be true for f, meaning in particular that

$$f\left(\sum_{i=1}^n x_i^2 + p_i^2, \sum_{i=1}^n y_i^2 + q_i^2, \sum_{i=1}^n x_i y_i - p_i q_i\right) \propto \prod_{i=1}^n f\left(x_i^2 + p_i^2, y_i^2 + q_i^2, x_i y_i - p_i q_i\right), \tag{6}$$

which is exactly the characterization of the exponential function. Hence, f and also W are exponential in $||x||^2 + ||p||^2$, $||y||^2 + ||q||^2$, and $x \cdot y - p \cdot q$, which means that the state ρ_{AB} is a Gaussian state. This concludes our proof. ∎

The protocol GG02 is invariant under conjugate passive symplectic operations applied by Alice and Bob. Hence, Alice and Bob can safely assume that their state ρ_{AB} displays the same symmetry. Restricting the analysis to collective attacks, one can use Lemma 1 to conclude that the state ρ_{AB} can be considered to be Gaussian. Since the initial state produced by Alice, a (Gaussian) two-mode squeezed vacuum, is transformed through the quantum channel into another Gaussian state, this means that the action of the channel (i.e., of the attack) can be safely considered to be Gaussian, which gives a simple proof that Gaussian attacks are optimal among collective attacks.

III. CONCLUSION AND PERSPECTIVES

In this article, we gave an alternative proof that Gaussian attacks are optimal against GG02 among all collective attacks. This proof makes use of symmetries of the protocol in phase space and does not require considering specific properties of the entropy, as in previous proofs [11,12]. A natural question is whether this technique can be exploited for variants of the GG02 protocol.

Let us consider first protocols with a discrete modulation, such as [22]. In this case, our proof cannot be applied directly because protocols with a discrete modulation are less symmetric than protocols with a Gaussian modulation. Indeed, not all rotations in phase space leave the protocol invariant: Only the orthogonal transformations leaving the modulation unchanged, that is, transformations belonging to the symmetry group of the hypercube, are relevant in this case. This group, however, is much smaller that the group considered here, and one cannot conclude directly that the state ρ_{AB} can be safely considered to be Gaussian. Note that this is still true but has to be proven with a different approach [22,23] based on the extremality of Gaussian states [38].

The second class of protocols one could consider is protocols with a postselection procedure [24–28]. These protocols have not yet been proven secure against general collective attacks because it is not known whether Gaussian attacks are optimal among collective attacks. The technique presented in this article cannot be used for protocols displaying a postselection step as this postselection explicitly breaks the symmetry of the protocol in phase space.

In addition to its simplicity, our proof turns out to be particularly useful for the finite-size analysis of the security of continuous-variable QKD protocols. Indeed, a specificity of the finite-size analysis is that Alice and Bob cannot assume to perfectly know the quantum state they share. For continuous-variable protocols in general, this is in fact theoretically impossible, as their state belongs to an infinite-dimensional Hilbert space and therefore requires an infinite number of parameters to be fully described. Fortunately, for protocols such as GG02 where the state can safely be considered to be Gaussian, Alice and Bob only need to know their covariance matrix, which depends on three parameters: the modulation variance, which is chosen by Alice, as well as the transmission and the excess noise of the quantum channel. These parameters are estimated by revealing part of Alice's and Bob's data. In order to proceed with this estimation, one needs a statistical model, and choosing a normal model seems quite natural. However, previous proofs of Gaussian optimality presented in [11,12] assume that the covariance matrix is known from Alice and Bob and cannot justify the use of a normal statistical model for its estimation. The proof presented here, on the contrary, allows for such a justification (see Appendix B for details).

The fact that our proof applies to finite-size analysis is crucial as our ultimate goal is clearly to assess the security of practical implementations, which are necessary finite. A general finite-size analysis of continuous-variable protocols will be the subject of future work.

ACKNOWLEDGMENTS

We thank Frédéric Grosshans for helpful remarks on a previous version of this work. We acknowledge support from Agence Nationale de la Recherche under projects PROSPIQ (ANR-06-NANO-041-05) and SEQURE (ANR-07-SESU-011-01).

APPENDIX A: COMPLETE PROOF OF LEMMA 1

Before considering the general case of Wigner functions, let us first consider the case of a probability distribution $p(x,y)$, which is invariant under orthogonal transformations applied to both x and y. In other words, for any $R \in O(n)$, one has $p(Rx,Ry) = p(x,y)$. Such a symmetry property clearly

implies that $p(x,y)$ can only depend on three parameters, namely $||x||$, $||y||$, and $x \cdot y$. With Wigner functions, the argument is more subtle and is detailed here.

We show that any function $W : \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}$, such that $W(x,p,y,q) = W(S^T(x,p,y,q))$ for any symplectic transformation S of the form given by Eq. (2), only depends on the following three parameters: $||x||^2 + ||p||^2$, $||y||^2 + ||q||^2$, and $x \cdot y - p \cdot q$.

Our goal is therefore to prove the following: for any pair of quadruples (x,p,y,q) and (x',p',y',q') such that

$$\begin{cases} ||x||^2 + ||p||^2 = ||x'||^2 + ||p'||^2 \\ ||y||^2 + ||q||^2 = ||y'||^2 + ||q'||^2 \\ x \cdot y - p \cdot q = x' \cdot y' - p' \cdot q' \end{cases}, \tag{A1}$$

one has $W(x,p,y,q) = W(x',p',y',q')$.

Let us introduce the following vectors:

$$a = x + ip, \quad a' = x' + ip' \tag{A2}$$

$$b = y - iq, \quad b' = y' - iq'. \tag{A3}$$

The condition (A1) can be rewritten as

$$\begin{cases} ||a||^2 = ||a'||^2 \\ ||b||^2 = ||b'||^2 \\ \mathrm{Re}\langle a|b\rangle = \mathrm{Re}\langle a'|b'\rangle \end{cases}, \tag{A4}$$

where $\mathrm{Re}(x)$ refers to the real part of x. It is sufficient to prove that there exists an unitary transformation $U \in U(n)$ such that $Ua = a'$ and $Ub = b'$. Indeed, one can split U into real and imaginary parts ($U = X - iY$), and it is easy to check that $S(X,Y)$ gives the correct change of coordinates. Since W is invariant under this change of coordinates, one concludes that $W(x,p,y,q) = W(x',p',y',q')$.

Let us introduce the following notations: $A \equiv ||a||^2 = ||a'||^2$, $B \equiv ||b||^2 = ||b'||^2$, and $C \equiv \mathrm{Re}\langle a|b\rangle = \mathrm{Re}\langle a'|b'\rangle$.

Consider first the case where a and b are colinear. This means that $b = C/Aa$ and $C = \pm\sqrt{AB}$. Use the Cauchy-Schwarz inequality, $|C| = |a' \cdot b'| \leqslant ||a'|| \cdot ||b'|| = \sqrt{AB}$ with equality if and only if a' and b' are colinear. This means that a' and b' are colinear and that $b' = (C/A)\,a'$. Because $||a|| = ||a'||$, the reflexion U across the mediator hyperplane of a and a' is a unitary transformation that maps a to a'. This reflexion also maps b to b'. This ends the proof in the case where a and b are colinear.

Let us now consider the general case where a and b are not colinear. It is clear that a' and b' cannot be colinear either. We take two bases, $(a,b,f_3,\ldots,f_n)$ and $(a',b',f'_3,\ldots,f'_n)$, of $\mathbb{C}^n$ and use the Gram-Schmidt process to obtain two orthonormal bases, $\mathcal{B} = (e_1,\ldots,e_n)$ and $\mathcal{B}' = (e'_1,\ldots,e'_n)$. Note that vectors e_1, e_2, e'_1, and e'_2 are given by

$$e_1 = \frac{a}{\sqrt{A}}, \quad e_2 = \frac{b - \langle e_1|b\rangle e_1}{||b - \langle e_1|b\rangle e_1||} \tag{A5}$$

$$e'_1 = \frac{a'}{\sqrt{A}}, \quad e'_2 = \frac{b' - \langle e'_1|b'\rangle e'_1}{||b' - \langle e'_1|b\rangle e'_1||}. \tag{A6}$$

Let us call U the unitary operator mapping $\mathcal{B}$ to $\mathcal{B}'$. It is easy to see that U maps a and b to a' and b', respectively. This concludes our proof.

APPENDIX B: NORMAL STATISTICAL MODEL

In this section, we discuss briefly the problem of parameter estimation in continuous-variable protocols with a Gaussian modulation. This question is particularly relevant when one is concerned with a finite-size analysis of the security of the protocol (a more detailed presentation can be found in [39,40]).

One of the main differences between the asymptotic and the finite-size study of a protocol lies in the parameter estimation. In the former case, one typically assumes that the quantum state ρ_{AB} is known from Alice and Bob, while in the latter case, this state needs being estimated.

For continuous-variable protocols with a Gaussian modulation, it is known that Gaussian attacks are optimal (among collective attacks) and therefore that the secret-key rate only depends on the covariance matrix of ρ_{AB}. This means that only this covariance matrix, that is, a finite number of parameters, needs to be estimated in practice. Moreover, using the symmetries described in this article, one can see that three parameters are in fact sufficient, namely Alice's and Bob's variances and their covariance. More precisely, the covariance matrix Γ_{AB} of the state ρ_{AB} can be assumed to have the following form:

$$\Gamma_{AB} = \begin{pmatrix} X\mathbb{1}_{2n} & Z\sigma_z \\ Z\sigma_z & Y\mathbb{1}_{2n} \end{pmatrix}, \tag{B1}$$

with $\sigma_z = \mathrm{diag}(1,-1,1,-1,\ldots,1,-1)$.

Furthermore, in a "prepare and measure" implementation of the protocol, X simply corresponds to Alice's modulation variance, which is *a priori* known from Alice and Bob. Hence, only two paramters remain to be estimated in practice. Asymptotically, this is not a problem since one can assume that the parameter estimation is done perfectly. However, for a finite-size analysis, which is eventually required to prove the security of a practical scheme, it is crucial to have an upper bound on the error in the parameter estimation. Indeed, in an adversarial scenario such as QKD, the legitimate parties should always consider the *worst* covariance matrix compatible with their data except with some small probability ϵ.

This can be easily done once a statistical model is given for the data $\mathbf{x} = (x_1,\ldots,x_n)$ and $\mathbf{y} = (y_1,\ldots,y_n)$ observed by Alice and Bob, respectively.

Whereas this could be done even without a model in the case of bounded parameters such as the quantum bit error rate for discrete-variable QKD protocols, this is much more complicated for *a priori* unbounded parameters, such as the excess noise in the GG02 protocol.

Then the demonstration given previously that the state ρ_{AB} can be considered Gaussian has a crucial consequence: Since the classical data $\mathbf{x}$ and $\mathbf{y}$ are obtained by performing Gaussian measurements (either homodyne or heterodyne detection), the joint distribution of $(\mathbf{x},\mathbf{y})$ corresponds to some marginal of a Gaussian Wigner function, and therefore it is also Gaussian. As a consequence, the variables x_i and y_i (for $i \in \{1,\ldots,n\}$) are related through

$$y_i = \alpha x_i + z_i, \tag{B2}$$

where α is a constant and z_i is a Gaussian random variable:

$z_i \sim \mathcal{N}(0,\sigma^2)$, which is independent of x_i. This is the definition of a normal statistical model, where one tries to estimate the values of α and σ^2. For such a model, one can bound the errors made in the estimation of both α and σ^2 and therefore on Y and Z (since these are simple functions of α and σ^2). Finally, and this is a crucial step in finite-key analysis, one can compute the worst key rate compatible with the data, except with probability ϵ.

[1] V. Scarani, H. Bechmann-Pasquinucci, N. J. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
[2] M. Peev *et al.*, New J. Phys. **11**, 075001 (2009).
[3] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems, and Signal Processing, Bangalore, India* (IEEE, New York, 1984), p. 175.
[4] R. Renner, Ph.D. thesis, ETH Zurich, 2005, e-print arXiv:quant-ph/0512258.
[5] V. Scarani and C. Kurtsiefer, e-print arXiv:0906.4547.
[6] T. C. Ralph, Phys. Rev. A **61**, 010303(R) (1999).
[7] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[8] F. Grosshans and P. Grangier, e-print arXiv:quant-ph/0204127.
[9] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. Cerf, and P. Grangier, Nature **421**, 238 (2003).
[10] S. Fossier, E. Diamanti, T. Debuisschert, A. Villing, R. Tualle-Brouri, and P. Grangier, New J. Phys. **11**, 045023 (2009).
[11] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
[12] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
[13] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
[14] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
[15] J. Lodewyck and P. Grangier, Phys. Rev. A **76**, 022332 (2007).
[16] J. Sudjana, L. Magnin, R. García-Patrón, and N. J. Cerf, Phys. Rev. A **76**, 052301 (2007).
[17] R. Namiki and T. Hirano, Phys. Rev. A **67**, 022308 (2003).
[18] R. Namiki and T. Hirano, Phys. Rev. Lett. **92**, 117901 (2004).
[19] M. Heid and N. Lütkenhaus, Phys. Rev. A **73**, 052316 (2006).
[20] Y.-B. Zhao, M. Heid, J. Rigas, and N. Lütkenhaus, Phys. Rev. A **79**, 012307 (2009).
[21] D. Sych and G. Leuchs, AIP Conf. Proc. **1110**, 347 (2009).
[22] A. Leverrier and P. Grangier, Phys. Rev. Lett. **102**, 180504 (2009).
[23] A. Leverrier and P. Grangier, e-print arXiv:1002.4083.
[24] C. Silberhorn, T. C. Ralph, N. Lütkenhaus, and G. Leuchs, Phys. Rev. Lett. **89**, 167901 (2002).
[25] A. M. Lance, T. Symul, V. Sharma, C. Weedbrook, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **95**, 180503 (2005).
[26] R. Namiki and T. Hirano, Phys. Rev. A **72**, 024301 (2005).
[27] R. Namiki and T. Hirano, Phys. Rev. A **74**, 032302 (2006).
[28] M. Heid and N. Lütkenhaus, Phys. Rev. A **76**, 022313 (2007).
[29] A. Leverrier, E. Karpov, P. Grangier, and N. Cerf, New J. Phys. **11**, 115009 (2009).
[30] V. Scarani and R. Renner, Phys. Rev. Lett. **100**, 200501 (2008).
[31] R. Y. Q. Cai and V. Scarani, New J. Phys. **11**, 045024 (2009).
[32] A. Leverrier and N. J. Cerf, Phys. Rev. A **80**, 010102(R) (2009).
[33] F. Grosshans, N. J. Cerf, J. Wenger, R. Tualle-Brouri, and P. Grangier, Quantum Inf. Comput. **3**, 535 (2003).
[34] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
[35] R. Renner, Nature Phys. **3**, 645 (2007).
[36] A. Leverrier, R. Alléaume, J. Boutros, G. Zémor, and P. Grangier, Phys. Rev. A **77**, 042325 (2008).
[37] B. D. Arvind, N. Mukunda, and R. Simon, Pramana **45**, 471 (1995).
[38] M. M. Wolf, G. Giedke, and J. I. Cirac, Phys. Rev. Lett. **96**, 080502 (2006).
[39] A. Leverrier, Ph.D. thesis, Ecole Nationale Supérieure des Télécommunications, 2009, [http://tel.archives-ouvertes.fr/tel-00451021].
[40] A. Leverrier, F. Grosshans, and P. Grangier, e-print arXiv:1005.0339.