Security of Quantum Key Distribution with Coherent States and Homodyne Detection

S. Iblisdir, G. Van Assche, and N. J. Cerf

QUIC, Ecole Polytechnique, CP 165/59, Université Libre de Bruxelles, 1050 Brussels, Belgium

(Received 11 July 2003; published 19 October 2004)

We assess the security of a quantum key distribution protocol relying on the transmission of Gaussian-modulated coherent states and homodyne detection. This protocol is shown to be equivalent to an entanglement purification protocol using CSS codes followed by key extraction, and is thus secure against any eavesdropping strategy.

DOI: 10.1103/PhysRevLett.93.170502 PACS numbers: 03.67.Dd, 03.67.Hk

Quantum key distribution (QKD) uses quantum mechanics to provide two parties (Alice and Bob) with a secret key [1], which they can later use to encrypt confidential information. Unlike classical key distribution, QKD relies, at least in principle, on no computational assumption [1], but only draws its validity from the laws of quantum mechanics. The resources needed for QKD always comprise a source of nonorthogonal quantum states on Alice's side, a quantum channel conveying these states to Bob, a measuring apparatus on Bob's side, and a (public) authenticated classical channel between Alice and Bob. QKD protocols generally consist in two (intertwined) parts. The first part consists in probing the quantum channel to determine whether it is possible to securely transmit the key over it. The second part consists in the explicit distillation of the secret key. It is the use of nonorthogonal quantum states which allows one to reliably probe the quantum channel.

Most interest in QKD has been devoted to protocols involving (an approximation to) a single-photon source on Alice's side and a single-photon detector on Bob's side [1,2]. However, protocols involving quantum continuous variables have lately been considered with an increasing interest [3–6]. Of special importance are "coherent-state" protocols [7,8]. The quantum source at Alice's side then randomly generates coherent states of a light mode with a Gaussian distribution, and Bob's measurements are homodyne measurements. These protocols seem to allow for facilitated implementations and higher secret-key generation rates than the protocols involving single-photon sources [8].

In this Letter, we constructively prove that secure coherent-state protocols exist. Previous security analyses have been carried out, but they were restricted to individual Gaussian [7,8] or finite-size non-Gaussian [9] eavesdropping strategies. We here want to address a more general setting and allow a potential eavesdropper (Eve) to probe the quantum channel between Alice and Bob in any manner she pleases. We want to establish the security of coherent-state protocols against arbitrary coherent attacks (see [10] and references therein). The importance of our result lies in that it shows that no nonclassical feature of light, such as squeezing, is necessary for continuous-variable QKD: coherent states, homodyne detection, and well-chosen communication procedures are sufficient for Alice and Bob to distill a secret key.

The basic ingredient that we shall use in the remaining is the argument used in [10] to prove the security of the BB84 protocol, when classical postprocessing derives from a Calderbank-Shor-Steane (CSS) code. Let us start with a brief review of this argument. It is well known that quantum error-correcting codes provide a means to perform entanglement purification with one-way communication [11]. The situation where Alice and Bob share N noisy entangled qubit pairs is fully equivalent to a situation where Alice would have prepared N pairs, all in the Einstein-Podolski-Rosen (EPR) state

$$|\phi^+\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle), \tag{1}$$

and would have kept half of each pair for herself while sending all other halves to Bob through some noisy quantum channel. The effect of this channel on the state can be modeled as if the state either remains unaltered or undergoes one of the three following "errors": bit-flip, $\phi^+ \to \psi^+$, or phase-flip, $\phi^+ \to \phi^-$, or both, $\phi^+ \to \psi^-$, where $|\phi^-\rangle = \frac{1}{\sqrt{2}}(|00\rangle - |11\rangle)$ and $|\psi^\pm\rangle = \frac{1}{\sqrt{2}}(|01\rangle \pm |10\rangle)$. In the latter situation, Alice and Bob could get pure EPR pairs upon Alice using a quantum error-correcting code (QECC) to protect the halves sent to Bob from the noise effected by the channel. Equivalently, in the former situation, Alice and Bob can get CN pairs in the state (1) ($C \leq 1$) upon Alice and Bob measuring the syndromes (or error patterns) of some QECC, Alice communicating the values of her syndromes to Bob, and Bob performing error correction so as to align the values of his syndromes on those of Alice. Then, C is the rate of the used quantum code. Clearly, secure QKD can be achieved from entanglement purification: Alice and Bob can certainly extract a secret bit from the state (1).

A (binary) CSS code is a 2^k-dimensional subspace of the Hilbert space of n qubits ($k \leq n$) [12,13]. Such a code belongs to the class of so-called stabilizer codes; i.e., they are defined as the eigenspace of a set of mutually commuting operators $\{\mathcal{O}_1, \ldots, \mathcal{O}_A\}$, the stabilizer generators.

The essential feature of a CSS code is that all stabilizer generators are either of the form $X^{s_1} \otimes \ldots \otimes X^{s_n}$ or of the form $Z^{s_1} \otimes \ldots \otimes Z^{s_n}$, where $X|i\rangle = |i \oplus 1\rangle$, $Z|i\rangle = (-)^i|i\rangle$, and where $(s_1, \ldots, s_n) \in \{0, 1\}^n$. Because of this feature, it is possible to prove that entanglement purification using a CSS code followed by key extraction is fully equivalent to a quantum cryptographic protocol using BB84 as a physical part, supplemented with suitable error correction and privacy amplification [10]. The postprocessing works as follows. Let the binary vectors $\mathcal{K}$ and $\mathcal{K}'$ denote, respectively, Alice's and Bob's raw key bits, and let $C_2 \subset C_1$ denote two embedded n-bit classical linear codes, with parity check matrices, respectively, H_1 and H_2 [14]. Alice announces the syndrome $H_1\mathcal{K}$. Bob corrects $\mathcal{K}'$ to the nearest vector $\mathcal{K}''$ such that $H_1\mathcal{K}'' = H_1\mathcal{K}$ (error correction). With high probability, $\mathcal{K}'' = \mathcal{K}$. The key is then reduced to $H_2\mathcal{K}$ (privacy amplification).

Entanglement purification is (asymptotically) achievable using a CSS code as long as the bit-flip probability e_b and the phase-flip probability e_p satisfy

$$C \equiv 1 - h(e_b) - h(e_p) > 0, \tag{2}$$

where $h(x) = -\log_2 x^x (1 - x)^{(1-x)}$ denotes the binary Shannon entropy [10]. Equivalently, the BB84 protocol allows Alice and Bob to distill a secret key using the above error correction and privacy amplification schemes if the error rates for two conjugate bases satisfy (2).

From QKD schemes based on entanglement purification for qubits, it is possible to derive a secure QKD scheme using squeezed states and homodyne detection, which is in spirit very close to the BB84 protocol [4]. Let us present this scheme in a slightly modified form. Let $\hat{x}$ and $\hat{p}$ denote two conjugate quadratures of a single mode of the electromagnetic field ($[\hat{x}, \hat{p}] = i$). Alice creates (about) $4N$ quantum oscillators in a squeezed state as follows. She draws a $4N$-bit string b to decide for each of the $4N$ oscillators whether it will be prepared in an x-squeezed state or in a p-squeezed state. For each oscillator, she draws a real value x [or p] according to a probability distribution $P_{\text{pos}}(x)$ [or $P_{\text{mom}}(p)$], and sends Bob an x-squeezed [or p-squeezed] state centered on $(x, 0)$ [or $(0, p)$]. Bob receives the states and decides at random to measure each of them either in the x basis or in the p basis. By public discussion, Alice and Bob discard the oscillators for which Alice's choice of preparation and Bob's choice of measurement mismatch. Alice and Bob should now have a list of (about) $2N$ correlated real values $(x_1, x'_1), \ldots, (x_{2N}, x'_{2N})$ from which they wish to extract bits. To do so, Alice decomposes each real value, x, as $x = [S(x) + \bar{S}(x)]\sqrt{\pi}$, where $S(x)$ is an integer, and reveals $\bar{S}(x)$ to Bob. Alice's bit is the parity of $S(x)$. Bob subtracts $\bar{S}(x)\sqrt{\pi}$ from his corresponding real value, x', and adjusts his result $x' - \bar{S}(x)\sqrt{\pi}$ to the nearest integer multiple of $\sqrt{\pi}$. The key bit will be 0 if this integer is even, and 1 otherwise. At this point, Alice and Bob agree on a subset of size (about) N of their key elements that they use for verification. A bit error (phase error) occurs when Alice sends an x-squeezed state (a p-squeezed state), and Alice's bit and Bob's bit mismatch. If the estimates of the error rates e_b and e_p satisfy Eq. (2), Alice and Bob further proceed with error correction and privacy amplification to distill a secret key out of the N remaining key elements exactly as in the BB84 protocol.

The bit error rate e_b is bounded by the probability that, when Alice sends an x-squeezed state centered on the value x_0, $|\text{sq}(x_0)\rangle$, and Bob performs an $\hat{x}$ homodyne measurement, Bob gets an outcome whose value differs from x_0 by a magnitude greater than $\sqrt{\pi}/2$. The phase-error rate, e_p, can be bounded similarly. Therefore, even in the absence of eavesdropping, e_b and e_p will be nonzero due to finite squeezing. As a consequence, it can be proven that a minimum of 2.51 dB of squeezing is necessary for the protocol to work [4].

We now want to convert the above squeezed-state protocol to a coherent-state protocol. For that, we first observe that three modifications can be brought to it without weakening its security. First [4], the above protocol is equivalent to an asymmetric protocol where Alice decomposes her real values as $x = [S(x) + \bar{S}(x)]\alpha\sqrt{\pi}$ when using the x quadrature, and $p = [S(p) + \bar{S}(p)]\sqrt{\pi}/\alpha$ when using the p quadrature, where $S(x)$ [$S(p)$] is an integer and α is some positive real parameter. Such an asymmetric protocol allows Alice to squeeze unequally the x and p quadratures. The squeezing should only be such that Eq. (2) is obeyed. In particular, Alice can use coherent states when encoding in the x quadrature if, when encoding in the p quadrature, she uses states exhibiting at least 3.37 dB of squeezing. Our second modification concerns the method used by Alice for encoding. When she chooses to encode in the x quadrature, she draws the value of x from the probability distribution $P_{\text{pos}}(x)$ and prepares a coherent state centered on $(x, 0)$. However, the decision to prepare states centered on $(x, 0)$ relies on an arbitrary convention between Alice and Bob about the position of the x axis. Instead of sending a state centered on $(x, 0)$, Alice could as well send a state centered on (x, p), where the value p, drawn from some probability distribution $P'_{\text{pos}}(p)$, may in principle be publicly disclosed to allow Bob to displace the state back on the x axis. Of course, a similar remark applies when Alice encodes information using the p quadrature. As a third modification, we note that there is no loss of security if Alice and Bob decide that the key is encoded in the coherent states and never in the squeezed states. They can decide that about two-thirds of the time Alice will send coherent states to transmit the key and to estimate e_b, while about a third of the time Alice will send p-squeezed states to estimate e_p. (Note that this fact holds for BB84 as well: one can decide that the key is encoded only in the Z eigenstates, while the X eigenstates are sent only to determine the phase-error rate.)

In summary, the following is a secure squeezed-state protocol.

(1) Alice prepares the state

$$S = S_{\text{key}}^{\text{coh}} \otimes S_{\text{ck}}^{\text{coh}} \otimes S_{\text{ck}}^{\text{sq}},$$

where $S_{\text{key}}^{\text{coh}} = \gamma_1 \otimes \ldots \gamma_N$ and $S_{\text{ck}}^{\text{coh}} = \gamma_1^c \otimes \ldots \gamma_N^c$ are tensor products of N coherent states, drawn from some probability distribution $P_{\text{pos}}(x)P'_{\text{pos}}(p)$, and $S_{\text{ck}}^{\text{sq}} = \sigma_1 \otimes \ldots \sigma_N$ is a tensor product of N p-squeezed states drawn from some probability distribution $P'_{\text{mom}}(x) \times P_{\text{mom}}(p)$. These probability distributions are chosen such that the ensemble formed by the coherent states is identical to the ensemble formed by the squeezed states:

$$\begin{aligned}\rho_{\text{ens}} &= \int dx dp\, P_{\text{pos}}(x)P'_{\text{pos}}(p)\gamma(x, p) \\ &= \int dx dp\, P'_{\text{mom}}(x)P_{\text{mom}}(p)\sigma(x, p), \end{aligned} \tag{3}$$

where $\gamma(x, p) = |\text{coh}(x, p)\rangle\langle\text{coh}(x, p)|$ [$\sigma(x, p) = |\text{sq}(x, p)\rangle\langle\text{sq}(x, p)|$] denotes a coherent state [a p-squeezed state] centered on (x, p).

(2) Alice picks a random permutation of $3N$ elements, π, and sends the state $\pi S \pi^*$ to Bob.

(2′) Let the CP map $T{:}\mathcal{B}(\mathcal{H}^{\otimes 3N}) \rightarrow \mathcal{B}(\mathcal{H}^{\otimes 3N})$ denote the quantum channel between Alice and Bob, where $\mathcal{H}$ denotes the Hilbert space of a quantum oscillator, and where $\mathcal{B}(\mathcal{H}^{\otimes 3N})$ denotes the space of bounded operators over $\mathcal{H}^{\otimes 3N}$. Thus, T represents the (possibly collective) eavesdropping strategy used by Eve.

(3) After Bob acknowledges receipt of the oscillators, Alice reveals the permutation π, which Bob undoes: $T(\pi S \pi^*) \rightarrow T^\pi(S) = \pi^* T(\pi S \pi^*)\pi$. For each $\gamma_j^c \in S_{\text{ck}}^{\text{coh}}$, Alice publicly discloses the values $x_j = \text{tr}\,\hat{x}\gamma_j^c$, and for each $\sigma_j \in S_{\text{ck}}^{\text{sq}}$, she discloses the values $p_j = \text{tr}\,\hat{p}\sigma_j$.

(4) For each $\gamma_j^c \in S_{\text{ck}}^{\text{coh}}$, Bob measures the binary effect $X(x_j) = \int_{\alpha\sqrt{\pi}/2+x_j}^{+\infty} dx|x\rangle\langle x| + \int_{-\infty}^{-\alpha\sqrt{\pi}/2+x_j} dx|x\rangle\langle x|$. The corresponding outcome $e_{b,j}$ equals 1 if $X(x_j)$ is measured and $e_{b,j} = 0$ otherwise. Similarly, for each $\sigma_j \in S_{\text{ck}}^{\text{sq}}$, Bob measures the effect $P(p_j) = \int_{\sqrt{\pi}/2\alpha+p_j}^{+\infty} dp|p\rangle\langle p| + \int_{-\infty}^{-\sqrt{\pi}/2\alpha+p_j} dp|p\rangle\langle p|$ and gets an outcome $e_{p,j}$.

(5) If the estimates for the bit error rate, $e_b = \frac{1}{N}\sum_j e_{b,j}$, and the phase-error rate, $e_p = \frac{1}{N}\sum_j e_{p,j}$, satisfy the CSS rate inequality (2), Alice and Bob extract bits from the remaining oscillators, $S_{\text{key}}^{\text{coh}}$, and proceed further with error correction and privacy amplification to distill a secret key.

To convert this protocol to a secure coherent-state protocol, all we need to prove is that the phase-error rate, e_p, can be estimated upon Alice sending only coherent states instead of squeezed states and Bob performing only homodyne measurements. Therefore, consider a situation where, instead of sending the state $S = S_{\text{key}}^{\text{coh}} \otimes S_{\text{ck}}^{\text{coh}} \otimes S_{\text{ck}}^{\text{sq}}$, Alice was preparing the state

$$R = S_{\text{key}}^{\text{coh}} \otimes S_{\text{ck}}^{\text{coh}} \otimes S_{\text{ck}}^{\text{p}},$$

where $S_{\text{key}}^{\text{coh}}$ and $S_{\text{ck}}^{\text{coh}}$ are again used to distill the key and estimate the bit error rate, respectively, and where $S_{\text{ck}}^{\text{p}} = \gamma_1^{\otimes M} \otimes \ldots \otimes \gamma_K^{\otimes M}$ denotes a tensor product of $KM = N'$ coherent states. If Alice and Bob were able to get a reliable estimate of the phase-error rate e_p from S_{ck}^{p}, then a QKD protocol where Alice and Bob use the state R would be as secure as a protocol where they use the state S.

Now observe that, as far as the estimation of e_p is concerned, since Bob performs *individual* measurements on his oscillators, the action of Eve is the same as if she were acting on each oscillator with individual maps $\tau_i : \rho \rightarrow \tau_i(\rho)$, $i = 1, \ldots, 2N + N'$, where τ_i denotes the map obtained by restricting the whole map $T^\pi(R)$ to the ith oscillator and replacing the ith state appearing in the tensor product R with ρ. Next, let M denote a sufficiently large integer and suppose that Alice and Bob had a means to estimate the quantities $\phi_j = \frac{1}{M}[\text{tr}P(p_j)\tau_{2N+1}(\sigma_j) + \ldots + \text{tr}P(p_j)\tau_{2N+M}(\sigma_j)]$, then the quantity

$$\Phi = \frac{1}{N}\sum_{j=1}^{N} \phi_j \tag{4}$$

would be as reliable an estimator for e_p as the one Alice and Bob would have obtained if they had used the state S.

Upon performing p-quadrature homodyne measurements, Bob can determine the NK quantities

$$F_{jk} \equiv \frac{1}{M}[\text{tr}\,P(p_j)\tau_{i_1(k)}(\gamma_k) + \ldots + \text{tr}\,P(p_j)\tau_{i_M(k)}(\gamma_k)],$$

where $I_k = \{i_1(k), \ldots, i_M(k)\}$ is some subset of $\{2N + 1, \ldots, 2N + N'\}$. Because of the random permutation π, we can be statistically confident that, for M sufficiently large, the quantity F_{jk} does not depend on the particular set I_k. In particular, we can be confident that F_{jk} tends to $\frac{1}{M}[\text{tr}\,P(p_j)\tau_{2N+1}(\gamma_k) + \ldots + \text{tr}\,P(p_j)\tau_{2N+M}(\gamma_k)]$ with arbitrarily high accuracy (taking M sufficiently large).

To conclude our conversion from a squeezed-state protocol to a coherent-state protocol, it remains to prove only that the ϕ_j's can be inferred from the F_{jk}, when the coherent states γ_k are correctly chosen. First, in order to simplify notations in the subsequent discussion, we define an operator E_j (which depends on the τ_i's) by

$$\text{tr}\,E_j\rho = \frac{1}{M}[\text{tr}\,P(p_j)\tau_{2N+1}(\rho) + \ldots + \text{tr}\,P(p_j)\tau_{2N+M}(\rho)].$$

Thus we have $F_{jk} = \text{tr}\,E_j\gamma_k$ and $\phi_j = \text{tr}\,E_j\sigma_j$. Next, let $\sigma_j = |\psi_j\rangle\langle\psi_j|$ and let $\sum_n \psi_n^j|n\rangle$ denote the expansion of $|\psi_j\rangle$ in photon-number basis. Since $\sum_n |\psi_n^j|^2 = 1$, we have $\forall\ \epsilon > 0, \exists\ N_j$ such that $\sum_{n=N_j+1}^{\infty} |\psi_n^j|^2 < \epsilon$. Let $N^* = \max_j N_j$ and let us denote $|\psi_{N^*}^j\rangle = \sum_{n=0}^{N^*} \psi_n^j|n\rangle$ and $|\psi_{N^*}^{j,c}\rangle = |\psi_j\rangle - |\psi_{N^*}^j\rangle$. We have $|\langle\psi^j|E_j|\psi^j\rangle - \langle\psi_{N^*}^j|E_j|\psi_{N^*}^j\rangle| < \epsilon + 2\sqrt{\epsilon}$. Indeed, $0 \le E_j \le \mathbf{1}$ and the Cauchy-Schwarz inequality imply that $\langle\psi_{N^*}^{j,c}|E_j|\psi_{N^*}^{j,c}\rangle \le ||\psi_{N^*}^{j,c}||^2 < \epsilon$ and that

$\langle\psi^j_{N^*}|E_j|\psi^{j,c}_{N^*}\rangle \leq \sqrt{\epsilon}$. Thus the knowledge of $\langle\psi^j_{N^*}|E_j|\psi^j_{N^*}\rangle$ brings (in arbitrarily good approximation) the knowledge of $\langle\psi^j|E_j|\psi^j\rangle$. Also, the quantities $\langle\psi^j_{N^*}|E_j|\psi^j_{N^*}\rangle$ can be inferred from the $(N^*+1)^2$ quantities $\langle k_1|E_j|k_2\rangle$, $0 \leq k_1, k_2 \leq N^*$. It thus remains to show only that these quantities can be estimated with coherent states. Therefore, consider the *pseudomixture* of coherent states

$$\Gamma^{(n)}(r) = \int \frac{d\theta}{2\pi} e^{in\theta} |re^{i\theta}\rangle\langle re^{i\theta}|.$$

Using the number state expansion of coherent state $|re^{i\theta}\rangle$ [15], one immediately checks that

$$\Gamma^{(n)}(r) = e^{-r^2} \sum_{l=0}^{\infty} \frac{r^{2l+n}}{\sqrt{l!\,(l+n)!}} |l\rangle\langle l+n|.$$

If a sufficiently large subset, $\mathcal{A}(r)$, of states of $\{\gamma_1, \ldots, \gamma_K\}$ are randomly distributed on a circle of radius r in phase space, then the quantities

$$\mathrm{tr}\,\Gamma^{(n)}(r)E_j = e^{-r^2} \sum_{l=0}^{\infty} \frac{r^{2l+n}}{\sqrt{l!\,(l+n)!}} \langle l+n|E_j|l\rangle \qquad (5)$$

can be estimated from the quantities F_{jk}, $\gamma_k \in \mathcal{A}(r)$, with arbitrarily high accuracy when M and the size of $\mathcal{A}(r)$ are sufficiently large. From Eq. (5), we find that

$$\langle L+n|E_j|L\rangle = \frac{e^{r^2}\mathrm{tr}\,\Gamma^{(n)}(r)E_j - \sum_{l=0}^{L-1} \frac{r^{2l+n}}{\sqrt{l!\,(l+n)!}} \langle l+n|E_j|l\rangle}{r^{2L+n}} \times \sqrt{L!\,(L+n)!} + \mathrm{O}(r^2). \qquad (6)$$

That is, if the quantities $\langle l+n|E_j|l\rangle$, $0 \leq l \leq L-1$, are known with high accuracy, then the quantity $\langle L+n|E_j|L\rangle$ can also be known, with accuracy $O(r^2)$. Thus considering some sufficiently small value r_0, the quantity $\langle 0+n|E_j|0\rangle$ can be inferred. Then considering $r_1 > r_0$, one determines $\langle 1+n|E_j|1\rangle, \ldots$, considering $r_L > \ldots > r_0$, one determines $\langle L+n|E_j|L\rangle$. Of course, taking increasing values of L, the errors will accumulate and the choice of $r_0, \ldots, r_L$ is a delicate problem. But since we always consider a situation where L is *finite,* it should be possible to choose the values of $r_0, \ldots, r_L$ so as to *control* the accumulated errors. It should be noted that the coherent states used to estimate e_p must be drawn from ρ_{ens}, so that Eve has no information on whether a coherent state was used for the key or to estimate e_p. This can, in principle, be achieved by combining several distributions such as those needed in the above estimation procedure, and averaging the resulting e_p's.

In summary, we have studied the security of Gaussian-modulated coherent-state protocols. We have shown how to extend the protocol of [4] to remove the need of squeezing for estimating the phase-error rate. This quantity can be estimated using coherent states modulated in *two* conjugate quadratures, homodyne measurements, and appropriate classical postprocessing. The equivalence between the derived coherent-state QKD protocol and an EPR purification with CSS codes assesses the security against any attack, going beyond individual Gaussian or finite-size non-Gaussian attacks [7–9]. An interesting question is the following: how robust is this coherent-state protocol in a practical situation such as an attenuation channel? Answering it amounts to estimating how e_b and e_p vary with loss and with the amount of (virtual) squeezing involved in the protocol. Duplicating the analysis carried in [4], one finds that a key can be distilled if losses are below 0.4 dB. This value should not be considered as a security threshold though, because it is strongly related to the periodic encoding scheme used here and in [4] to assign a bit value to a real number. Methods to get more efficient coherent state protocols will be presented in a forthcoming paper [16].

We thank P. Grangier, F. Grosshans, N. Lütkenhaus, and J. Preskill for fruitful discussions. We acknowledge financial support from the Communauté Française de Belgique under Grant No. ARC 00/05-251, from the IUAP programme of the Belgian government under Grant No. V-18 and from the EU under project projects RESQ, SECOQC, and COVAQIAL. S. I. acknowledges support from the Belgian FRIA foundation.

[1] N. Gisin, G. Ribordy, W. Tittel, and H. Zbinden, Rev. Mod. Phys. **74**, 145 (2002).
[2] A. Beveratos, R. Brouri, T. Gacoin, A. Villing, J.-P. Poizat, and P. Grangier, Phys. Rev. Lett. **89**, 187901 (2002).
[3] M. Hillery, Phys. Rev. A **61**, 022309 (2000).
[4] D. Gottesman and J. Preskill, Phys. Rev. A **63**, 022309 (2001).
[5] N. J. Cerf, M. Lévy, and G. Van Assche, Phys. Rev. A **63**, 052311 (2001).
[6] C. Silberhorn, N. Korolkova, and G. Leuchs, Phys. Rev. Lett. **88**, 167902 (2002).
[7] F. Grosshans and P. Grangier, Phys. Rev. Lett. **88**, 057902 (2002).
[8] F. Grosshans, G. Van Assche, J. Wenger, R. Brouri, N. J. Cerf, and P. Grangier, Nature (London) **421**, 238 (2003).
[9] F. Grosshans and N. J. Cerf, Phys. Rev. Lett. **92**, 047905 (2004).
[10] P. W. Shor and J. Preskill, Phys. Rev. Lett. **85**, 441 (2000).
[11] C. H. Bennett, D. P. DiVincenzo, J. A. Smolin, and W. K. Wootters, Phys. Rev. A **54**, 3824 (1996).
[12] A. R. Calderbank and P. W. Shor, Phys. Rev. A **54**, 1098 (1996).
[13] A. Steane, Proc. R. Soc. London A **452**, 2551 (1996).
[14] T. M. Cover and J. A. Thomas, *Elements of Information Theory* (Wiley & Sons, New York, 1991).
[15] D. F. Walls and G. J. Milburn, *Quantum Optics* (Springer-Verlag, Berlin, 1994).
[16] G. Van Assche, S. Iblisdir, and N. J. Cerf, quant-ph/0410031.